Firjan SENAI SESI IEL CIRJ

Integridade Conectada: ética, governança e inovação responsável.

Nova agenda para estimular ética e valor nas empresas e na sociedade

NOV. 2026

Juntos pela Integridade

Ficha Catalográfica

I61 Integridade conectada: ética, governança e inovação responsável / Firjan. – Rio de Janeiro: [s.n.], 2026.
348 p. : il., color.

ISBN: 978-85-98246-19-2
Referências ao final de cada artigo.

1. Ética empresarial. 2. Governança corporativa. 3. Integridade organizacional. 4. Compliance. 5. Inteligência artificial — Aspectos éticos. I. Firjan

CDD 658.4

Daisy Margareth Alcáçova de Sá Pimentel – CRB-7 nº 4217

Firjan SENAI SESI IEL CIRJ

Expediente

Firjan – Federação das Indústrias do Estado do Rio de Janeiro

Presidente
Luiz Cesio Caetano

1º Vice-Presidente Firjan
Carlos Erane de Aguiar

2º Vice-Presidente Firjan
Henrique Antônio Nora Oliveira Lima Junior

1º Vice-Presidente CIRJ
Isadora Landau Remy

2º Vice-Presidente CIRJ
Antonio Carlos Vilela

Diretor Executivo Operacional do Sistema Firjan e
Diretor Executivo SESI SENAI
Alexandre Reis

Diretor de Operações e Negócios
Carlos Magno Lucas do Nascimento

Diretor de Relacionamento Industrial
Cesar Kayat Bedran

Diretora de Compliance, Jurídico e Relações Governamentais
Gisela Pimenta Gadelha

Diretora de Desenvolvimento Industrial e Econômico
Luciana Costa Marques de Sá

Diretora de Serviços Corporativos
Luciana Costa Marques de Sá (Interina)

Diretor de Educação e Cultura
Vinícius Cardoso

GERÊNCIA DE INTEGRIDADE CORPORATIVA

Gerente de Integridade Corporativa
Januária Sá Barreto Lopes

Consultora de Integridade Corporativa
Ana Carla Coutinho Torres

Analista de Integridade Corporativa
Luiz Claudio Cabral Coelho

PROJETO GRÁFICO
GERÊNCIA GERAL DE REPUTAÇÃO E COMUNICAÇÃO

Gerente-Geral de Reputação e Comunicação
Luiz Phillipe Steenhagen Blower

Gerente de Comunicação Estratégica e Consultoria
Amanda Zarife

Gerente de Marca e Comunicação
Fernanda Marino

Coordenador de Marca e Soluções de Comunicação
Fábio Neves

Equipe Técnica
Amanda Martins
Clara Marques
Matheus Dames

NOV. 2026

www.firjan.com.br
Av. Graça Aranha, 1, 8º andar
Centro, Rio de Janeiro

Luiz Cesio Caetano

Presidente da Firjan CIRJ

Mensagem do Presidente

A integridade é um dos pilares fundamentais para o desenvolvimento sustentável das organizações, o fortalecimento da confiança e a construção de um ambiente de negócios ético, transparente e competitivo. Em um cenário de constantes transformações econômicas, tecnológicas e sociais, incorporar esses valores à estratégia e à cultura organizacional é um compromisso essencial para a indústria e para toda a sociedade.

Para a Federação das Indústrias do Estado do Rio de Janeiro (Firjan), promover a integridade significa contribuir para o fortalecimento da competitividade empresarial, estimulando práticas responsáveis de governança, inovação e gestão. Mais do que atender a requisitos legais e regulatórios, trata-se de consolidar uma atuação pautada pela ética, pela responsabilidade e pela coerência entre valores e decisões.

É com essa perspectiva que a Firjan, por meio de sua Câmara de Governança, vinculada ao Conselho de ESG, promove o diálogo e o compartilhamento de conhecimentos e experiências sobre temas estratégicos para as organizações. Esta obra reúne contribuições de profissionais e especialistas que, a partir de diferentes perspectivas, refletem sobre os desafios contemporâneos da integridade e suas interfaces com a governança, a tecnologia e a inovação.

Acreditamos que a cooperação entre empresas, instituições e profissionais é fundamental para disseminar boas práticas e transformar conhecimento em soluções aplicáveis à realidade empresarial. Ao estimular esse intercâmbio, reafirmamos nosso compromisso com o desenvolvimento de uma indústria cada vez mais preparada para os desafios do presente e as oportunidades do futuro.

Que esta publicação inspire novas reflexões, fortaleça a cultura de integridade nas organizações e contribua para a construção de um ambiente de negócios baseado na confiança, na responsabilidade e na geração de valor para a sociedade.

Boa leitura!

Claudia Guimarães

Claudia Guimarães é engenheira eletricista com MBAs em Marketing, Gestão Empresarial e Gerenciamento de Projetos, com ampla experiência no setor de energia. Atualmente é Head de Sustentabilidade das distribuidoras da Enel Brasil, Presidente do Conselho ESG da Firjan e atua como voluntária em instituições sociais com foco em diversidade de gênero e educação.

Mensagem da Presidente do Conselho ESG

A agenda de governança tem assumido papel central na forma como as organizações estruturam suas decisões, gerenciam riscos e constroem valor no longo prazo. Mais do que um conjunto de práticas, configura-se como eixo estratégico e transversal que conecta integridade, transparência, desempenho e capacidade de adaptação em um ambiente caracterizado por transformações regulatórias, tecnológicas, climáticas e sociais.

A criação da Câmara de Governança está diretamente associada à instituição do Conselho Empresarial de ESG da Firjan, constituindo desdobramento de uma agenda que reconhece a governança como elemento integrador das dimensões econômica, social e ambiental. O Conselho consolida-se como espaço estratégico de articulação entre lideranças empresariais, contribuindo para a qualificação do debate, a antecipação de tendências e o direcionamento de decisões em temas críticos para o desenvolvimento sustentável dos negócios e da sociedade. Nesse contexto, a indústria fluminense assume papel relevante, tanto por sua contribuição econômica quanto por sua capacidade de liderar agendas estruturantes e influenciar positivamente cadeias produtivas.

As pautas socioambientais passam a ocupar posição central na estratégia empresarial. Temas como mudanças climáticas, uso eficiente de recursos, inclusão produtiva e diversidade configuram-se como fatores determinantes para a competitividade, a gestão de riscos e a legitimidade das organizações. Nesse cenário, a governança atua como mecanismo estruturante, assegurando coerência entre compromissos assumidos e práticas implementadas, bem como a definição de métricas e a mensuração de resultados.

Ao longo desse período, a Câmara de Governança consolida-se como espaço estratégico de articulação e construção coletiva, reunindo representantes das maiores empresas do estado, especialistas e lideranças institucionais em torno de temas como compliance e proteção de dados pessoais. Essa ampla participação fortalece o compartilhamento de experiências, o aprimoramento contínuo das práticas organizacionais e a compreensão de que a governança efetiva constitui condição essencial para a sustentabilidade dos negócios e para o fortalecimento das relações de confiança com a sociedade.

A transversalidade da governança manifesta-se na sua capacidade de integrar estratégia, operação, riscos e oportunidades, promovendo maior alinhamento institucional, consistência na tomada de decisão e fortalecimento das relações de confiança. Nesse contexto, a presente publicação reflete o amadurecimento dessa agenda ao reunir boas práticas e experiências de empresas participantes e convidados, consolidando aprendizados e reafirmando a governança como fundamento para o desenvolvimento responsável e sustentável dos negócios, especialmente no contexto estratégico da indústria fluminense.

Andreia Marques

Andreia Marques é profissional com formação multidisciplinar em Ciências da Computação e Direito, complementada por especializações em Logística, Compliance, Proteção de Dados e Inteligência Artificial. Possui 33 anos de experiência profissional, sendo quase 15 anos dedicados à área jurídica, com atuação estratégica em Tecnologia da Informação, Recursos Humanos, Jurídico, Compliance e Proteção de Dados.

Ao longo da carreira, liderou projetos internacionais na América do Sul e desenvolveu expertise em contratos, Direito do Trabalho, Previdenciário, Ambiental e governança corporativa. Atualmente, responde pelas áreas de Compliance, Gestão da Linha Ética e Proteção de Dados (DPO) da Michelin na América do Sul, conduzindo iniciativas voltadas a ética, ESG, combate à corrupção, direitos humanos, privacidade de dados e sustentabilidade corporativa. Além disso, atua como Coordenadora da Câmara de Governança da Firjan, contribuindo para o fortalecimento das melhores práticas de governança e integridade corporativa.

Mensagem da Coordenadora da Câmara de Governança

A evolução da agenda de governança nas indústrias do Estado do Rio de Janeiro ganha expressão concreta a partir da atuação coordenada entre a Firjan e as empresas fluminenses, que vêm transformando diretrizes em práticas estruturadas e aplicáveis ao dia a dia corporativo. Nesse cenário, a Câmara Técnica de Governança Corporativa do Conselho ESG da Firjan, destacou-se como um fórum estratégico de diálogo qualificado, troca de experiências e construção de diretrizes práticas voltadas ao aprimoramento das estruturas de governança, compliance e privacidade, em consonância com referências nacionais e internacionais.

Ao longo deste primeiro ciclo, a Câmara concentrou esforços em temas essenciais para a maturidade das organizações, como transparência, integridade, criação e fortalecimento de políticas corporativas, além da gestão de riscos e da adequação à Lei Geral de Proteção de Dados (LGPD). Também foram aprofundadas discussões sobre resposta a incidentes de segurança, o papel estratégico do compliance nos processos decisórios, ética empresarial e mecanismos de mensuração de desempenho em governança. Tais iniciativas convergem para a incorporação efetiva dos princípios ESG na estratégia das empresas, promovendo resiliência, competitividade e geração de valor sustentável.

Este livro materializa um ciclo de aprendizado coletivo e de avanços consistentes, evidenciando o comprometimento das empresas com a melhoria contínua de suas práticas responsáveis, inovadoras e aderentes aos desafios contemporâneos. Mais do que registrar resultados, trata-se de um convite à continuidade dessa jornada, baseada na colaboração, no aprendizado contínuo e na transformação positiva do ambiente empresarial fluminense.

Bruno Bioni

Bruno Bioni é Doutor em Direito Comercial e Mestre em Direito Civil pela Faculdade de Direito da Universidade de São Paulo (USP); Autor dos livros "Proteção de Dados Pessoais: a função e os limites do consentimento" e "Regulação e Proteção de Dados: o princípio da *accountability*"; Membro do Conselho Nacional de Proteção de Dados (CNPD), designado como titular dentre os representantes de organizações da sociedade civil; Professor da ESPM e do IDP-SP; Fundador e conselheiro da Data Privacy Brasil e Sócio da Bioni Consultoria.

Prefácio

A integridade empresarial não pode mais ser compreendida apenas como a simples existência de normas, políticas e mecanismos de controle. Em um ambiente marcado pela transformação tecnológica e pela crescente complexidade dos riscos, o desafio está também em assegurar que essas estruturas saiam do papel e produzam efeitos concretos sobre a forma como as organizações decidem e atuam[1]. Nesse sentido, trata-se de deslocar o foco da conformidade meramente formal para a sua efetividade: mais do que demonstrar a existência de procedimentos, importa compreender em que medida princípios e obrigações são incorporados às práticas organizacionais e orientam decisões capazes de responder, de forma adequada, aos riscos que emergem de contextos cada vez mais dinâmicos.

A transformação digital amplia esse desafio ao modificar a própria infraestrutura informacional sobre a qual as organizações atuam. O avanço tecnológico intensifica os fluxos de informação, amplia as possibilidades de coleta e processamento de dados e, com isso, altera as relações entre informação, poder e controle[2]. A incorporação de sistemas de Inteligência Artificial (IA) acrescenta mais uma camada: ao ampliar a agência humana e permitir a delegação de tarefas e decisões, também exige atenção à responsabilidade, à supervisão e à preservação do controle humano[3]. Nesse contexto, integridade, proteção de dados e governança tecnológica deixam de constituir agendas estanques. Sua efetividade passa a depender da capacidade de tratá-las de forma coordenada, especialmente quando inovação, risco e tomada de decisão passam a se imbricar e quando a governança passa a ser compreendida não apenas como custo de conformidade, mas também como investimento capaz de sustentar inovação e competitividade[4].

É justamente nessa intersecção que se insere a presente obra. Ao reunir contribuições sobre governança, integridade, compliance, privacidade, proteção de dados e IA, a publicação aproxima temas que, na prática organizacional, se conectam de forma crescente. Seu diferencial

[1] QUELLE, Claudia. Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability- and Risk-based Approach. *European Journal of Risk Regulation*, v. 9, n. 3, p. 502-526, 2018. DOI: 10.1017/err.2018.47. ("compliance should never be a box-ticking exercise", p. 503).

[2] DONEDA, Danilo Cesar Maganhoto. *Da privacidade à proteção de dados pessoais*: fundamentos da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Thomson Reuters Brasil, 2020. E-book. ("a tecnologia operou especificamente a intensificação dos fluxos de informação (...) mudando a natureza e os eixos de equilíbrio na equação entre poder – informação – pessoa – controle", p. 34).

[3] FLORIDI, Luciano *et al*. AI4People—An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations. *Minds and Machines*, v. 28, p. 689-707, 2018. DOI: 10.1007/s11023-018-9482-5. ("Responsibility is therefore essential (...) ensuring that we remain in control", p. 692-693).

[4] BIONI, Bruno Ricardo. Inovar pela lei. *GV-executivo*, São Paulo, v. 18, n. 4, p. 30-33, jul./ago. 2019. Disponível em: https://periodicos.fgv.br/gvexecutivo/article/view/79978. Acesso em: 2 out. 2026.

está também na combinação entre reflexão conceitual, experiências e boas práticas, permitindo observar a governança em sua dimensão transversal: como elemento capaz de articular estratégia, operação, riscos e oportunidades. Mais do que reunir discussões distintas, a obra percorre justamente as fronteiras em que essas agendas se encontram e se transformam, oferecendo uma leitura à altura da complexidade crescente das decisões corporativas.

A obra parte, de forma significativa, da dimensão humana e organizacional da integridade. Os textos iniciais chamam atenção para a distância que pode existir entre aquilo que a companhia declara e aquilo que efetivamente pratica, deslocando o olhar dos códigos, políticas e treinamentos para os comportamentos que são repetidos, tolerados e recompensados no cotidiano. Assim, a cultura aparece não como elemento acessório dos programas de integridade, mas como condição para sua efetividade. É também nesse ponto que a noção de *accountability* ganha relevo: boas práticas não se esgotam em sua adoção, mas precisam ser demonstráveis, efetivas e abertas à prestação e ao julgamento de contas, para dentro e para fora da organização[5]. A governança, assim, deixa de ser apenas arquitetura formal e passa a revelar-se na capacidade de transformar princípios, incentivos e responsabilidades em critérios concretos de decisão.

Essa mesma preocupação com a efetividade acompanha a passagem da obra para a privacidade, a proteção de dados e, posteriormente, a IA. A discussão alcança a resposta a incidentes, a atuação do encarregado e a convergência entre *compliance*, segurança da informação e proteção de dados, evidenciando a necessidade de estruturas de governança capazes de articular riscos tradicionalmente tratados de forma separada. Com a IA, essa lógica é novamente tensionada: entram em cena questões relacionadas à responsabilidade, à supervisão, à transparência e à avaliação dos riscos associados à adoção dessas tecnologias. A própria diligência de sistemas de IA é apresentada como possível extensão dos mecanismos de integridade já conhecidos, aproximando inovação tecnológica e governança empresarial. Ao longo desse percurso, as fronteiras do que se entende por integridade tornam-se mais porosas, acompanhando riscos que já não se deixam conter pelos contornos tradicionais das funções organizacionais.

Os riscos que hoje atravessam a vida empresarial não respeitam as fronteiras traçadas pelo organograma. Integridade, privacidade, segurança da informação, governança e inteligência artificial acabam por se encontrar nos mesmos espaços de decisão, exigindo respostas capazes de dialogar entre si. A contribuição desta obra está justamente em aproximar essas agendas sem perder de vista suas especificidades, combinando reflexão conceitual, experiência prática e diferentes perspectivas profissionais. Ao fazê-lo, oferece ao leitor um retrato consistente dos desafios que hoje atravessam a gestão das organizações e reforça a importância de estruturas capazes de responder a eles de forma coordenada. Por essa razão, é uma satisfação prefaciar esta publicação. Desejo a todos e todas uma excelente leitura.

[5] Cf. BIONI, Bruno Ricardo. Regulação e proteção de dados pessoais: o princípio da accountability. Rio de Janeiro: Forense, 2022. P. 77

Sumário

MENSAGEM DO PRESIDENTE 4

MENSAGEM DA PRESIDENTE DO CONSELHO ESG 6

MENSAGEM DA COORDENADORA DA CÂMARA DE GOVERNANÇA 8

PREFÁCIO 10

CAPÍTULO 1 – DA CULTURA AO COMPORTAMENTO: O QUE REALMENTE FAZ A INTEGRIDADE ACONTECER 15

Cultura não implanta, se disputa 16

Desafios contemporâneos à cultura de integridade nas organizações 26

Cultura de integridade 44

O tom do meio: onde a integridade ganha forma 58

Da norma ao comportamento 66

Incentivos, recompensas e consequências 80

Compliance e integridade 86

CAPÍTULO 2 – GOVERNANÇA: ESTRUTURAS QUE SUSTENTAM A INTEGRIDADE CORPORATIVA 97

Cultura como infraestrutura da governança 98

O compliance como pilar estratégico da governança corporativa 106

Um ambiente de negócios íntegro não é possível sem os pequenos negócios 112

O papel do compliance na governança das empresas estratégicas de defesa 120

Ética na tomada de decisão 128

Governança e compliance tributário no novo cenário fiscal 136

A cultura da integridade como diferencial estratégico 142

Governança corporativa do amanhã 148

Governança corporativa e integridade 160

CAPÍTULO 3 – PRIVACIDADE E PROTEÇÃO DE DADOS COMO VALOR ORGANIZACIONAL NA PRÁTICA 169

Incidentes de segurança na era da IA 170

LGPD além da conformidade 180

O Encarregado de Dados (Data Protection Officer – DPO) como vetor de efetividade na LGPD 190

Oportunidades nas adversidades 206

Gestão de incidentes e vazamentos de dados pessoais 216

Cyber compliance 230

CAPÍTULO 4 – GOVERNANÇA DE INTELIGÊNCIA ARTIFICIAL: EQUILIBRANDO COMPETITIVIDADE E RESPONSABILIDADE 245

Inteligência Artificial 246

Governantes ou governadas? 256

Inteligência Artificial, algoritmos e ética 268

Due diligence de Inteligência Artificial 278

CAPÍTULO 5 – INOVAÇÃO COM INTELIGÊNCIA ARTIFICIAL: RISCOS, RESPONSABILIDADES E TRANSPARÊNCIA NO USO DE ALGORITMOS 293

Inteligência Artificial como ferramenta humana 294

Riscos associados à Inteligência Artificial 300

Criatividade induzida por sistemas de IA 310

Quando tudo parece real 322

Inteligência Artificial 330

Capítulo 1

Da cultura ao comportamento: o que realmente faz a integridade acontecer

Cultura não implanta, se disputa

porque a integridade se forma no comportamento repetido, tolerado e recompensado

Antonio Carlos Hencsey (Tatau)

Antonio Carlos Hencsey (Tatau) é psicólogo social, criminologista empresarial, palestrante e professor. Fundador do Eticalizando e do podcast "É Óbvio Fazer a Coisa Certa?", mestre em Artes da Cena e pós-graduado em Psicopatologia e em Gestão de Riscos Corporativos, com formação especializada em riscos humanos, ética e prevenção de fraudes.

É professor em cursos de MBA e pós-graduação em Gestão de Riscos de Fraude e Compliance na FIA/USP, PUC-SP, LEC e Hospital Sírio-Libanês. Autor de artigos e capítulos de livros sobre compliance e comportamento humano, atua como palestrante em eventos nacionais e internacionais, e foi reconhecido por diversos anos entre os mais admirados profissionais de Compliance do Brasil.

Artista marcial e competidor, é também criador do Mind and Fight, método que une psicologia e artes marciais para desenvolver a capacidade humana de responder sob pressão.

Introdução

Há uma pergunta que costumo fazer quando uma organização me procura dizendo que precisa construir a sua cultura de integridade. Pergunto qual é a cultura que ela tem hoje. O silêncio que vem depois costuma ser o mesmo, e ele diz muita coisa, porque a empresa chegou ali convencida de que precisa erguer algo que não existe, quando na verdade já opera com uma cultura em tempo integral, com regras claras, transmissão eficiente para quem chega e consequências bem definidas para quem as descumpre. O detalhe é que essas regras não estão no código de conduta.

Costumo insistir nessa pergunta porque a resposta que ela provoca revela o tamanho do desencontro. Quando o interlocutor finalmente descreve a cultura existente, ele raramente recorre aos valores institucionais. Fala de coisas como a velocidade com que se decide, o tipo de assunto que não se leva para determinada reunião, o peso que uma área tem sobre as outras, a tolerância maior ou menor com quem entrega resultado. Ou seja, descreve comportamentos que ninguém escreveu, ninguém aprovou em comitê e ninguém divulgou. Descreve, sem saber, exatamente aquilo que este artigo pretende discutir.

Esse desencontro entre o que a organização escreve e o que ela pratica é o problema deste artigo, e ele tem uma formulação incômoda: por que empresas que possuem código aprovado, políticas publicadas, treinamento aplicado e canal em funcionamento continuam produzindo desvios relevantes? A explicação mais comum atribui o fenômeno à falha de implementação, ao treinamento insuficiente ou à ausência de comprometimento da alta direção. São diagnósticos razoáveis, mas incompletos, porque todos eles partem de uma premissa que raramente é examinada: a de que a cultura antecede o comportamento e que, portanto, ajustando o que a organização declara, ajusta-se o que ela faz.

Este texto sustenta o contrário. O objetivo geral é demonstrar que a cultura organizacional se constitui como resultado de comportamentos repetidos, tolerados e recompensados, e que programas de integridade desenhados para atuar sobre o discurso agem sobre o efeito e não sobre aquilo que o produz. Como objetivos específicos, pretende-se descrever o mecanismo de formação da cultura a partir da literatura consolidada, identificar por que o comportamento indesejado dispõe de vantagem estrutural na disputa cultural e propor um deslocamento no ponto de intervenção dos programas.

A justificativa é prática antes de ser acadêmica. A régua brasileira deixou de perguntar se a empresa tem programa e passou a perguntar se o programa funciona. A Lei nº 12.846/2013 já previa a existência dos mecanismos de integridade como fator a ser considerado na avaliação, e o Decreto nº 11.129/2022 explicitou que esse exame abrange existência, aplicação e efetividade. A avaliação, portanto, não se limita à forma. Some-se a isso a exigência crescente de evidência por parte de contratantes, investidores e cadeias globais de valor, e o que se tem é um cenário em que compreender como a cultura realmente se forma deixou de ser refinamento conceitual e virou gestão de risco. Os artigos que seguem neste capítulo tratam de maturidade, de incentivos, de comunicação e educação e de desafios contemporâneos da integridade. Já este texto pretende oferecer a lente com a qual esses temas podem ser lidos.

1. Como a cultura se forma

1.1 O pressuposto é ponto de chegada

Schein é provavelmente o autor mais citado quando o assunto é cultura organizacional e também um dos mais mal aproveitados. A leitura que circula no mercado costuma reter os três níveis, os artefatos visíveis, os valores declarados e os pressupostos profundos, e daí conclui que basta trabalhar os valores para que os comportamentos se alinhem. Só que o mecanismo descrito por Schein (2022) não funciona nessa direção.

O que ele descreve é aprendizado compartilhado. Um grupo enfrenta um problema. Alguém, normalmente com alguma autoridade, propõe uma solução. Se a solução funciona, ela é repetida. Se continua funcionando, deixa de ser discutida. E só depois de muitas repetições bem-sucedidas é que ela desce ao nível daquilo que ninguém mais questiona, que é exatamente o que chamamos de pressuposto. Percebam a ordem: o pressuposto é ponto de chegada, não de partida. Uma crença pode até ser proposta por um líder antes de qualquer teste, e frequentemente é. Mas ela não nasce pronta como pressuposto. Só se consolida como tal quando é praticada, funciona e passa a ser validada repetidas vezes. A empresa não age assim apenas porque acredita naquilo. Ela passa a acreditar naquilo depois de agir assim e dar certo.

Berger e Luckmann (2014) descrevem esse mesmo caminho com uma precisão que serve como um mapa. Uma ação repetida se torna hábito, o hábito é tipificado, a tipificação se institucionaliza e, a partir de certo ponto, passa a ser vivida como realidade objetiva, como se sempre tivesse existido e como se não houvesse alternativa. Quem entra depois não recebe uma escolha, recebe um fato. Aquele "aqui sempre foi assim" que todo profissional de integridade já ouviu não é uma frase de resistência. É o relato exato de um processo de sedimentação.

Geertz (2008) contribui com uma precisão conceitual que evita um erro comum na nossa área. Para ele, cultura não é um poder ao qual se possam atribuir causalmente eventos e comportamentos, e sim um contexto dentro do qual eles se tornam inteligíveis. Isso muda o tipo de pergunta que fazemos. Deixa de fazer sentido perguntar se a cultura causou o desvio e passa a fazer sentido perguntar o que tornou aquele desvio compreensível, aceitável e comentável em voz alta naquele ambiente.

Swidler (1986) leva o argumento adiante e é, entre os autores aqui reunidos, o mais direto. Sustenta que a cultura não influencia a ação fornecendo os valores últimos para os quais a ação se orienta, mas moldando um repertório de hábitos, habilidades e estilos a partir do qual as pessoas montam suas estratégias de ação. Note a implicação prática. Uma organização pode declarar valores impecáveis e mesmo assim não oferecer a ninguém o repertório necessário para agir de acordo com eles. Publicar o valor não ensina a conduta correspondente, do mesmo modo que declarar que a segurança é prioritária não ensina ninguém a operar uma máquina.

Essa inversão tem uma consequência prática imediata, e ela explica o destino da maioria dos projetos de transformação cultural que já acompanhei. Eles costumam começar pelo mesmo lugar: reunir a liderança, revisar a declaração de valores, redigir princípios melhores, produzir material de comunicação e lançar a iniciativa em um evento. Tudo isso é feito com seriedade e com bons profissionais. E a razão pela qual quase nunca funciona não tem a ver com a qualidade da execução. Tem a ver com a ordem das coisas. Está se tentando instalar diretamente no nível dos pressupostos algo que, segundo a própria teoria que fundamenta a iniciativa, só chega lá depois de ter sido praticado e confirmado muitas vezes. É o equivalente a escrever a conclusão antes de ter feito o experimento.

Antes que alguém me acuse de defender uma seta única, vale a ressalva, e ela é importante. Nenhum desses autores afirma que a cultura não influencia o comportamento. Schein e Berger e Luckmann afirmam justamente o oposto, e é evidente para qualquer um que já trabalhou dentro de uma empresa que o ambiente molda quem nele vive. O circuito é fechado: o comportamento sedimenta em cultura e a cultura sedimentada passa a dirigir ou constranger o comportamento seguinte. O que se afirma aqui é sobre origem e sobre ponto de intervenção. A cultura nasce da prática, se mantém pela repetição, e por isso tentar movê-la pelo discurso é agir na ponta errada.

1.2 Não existe uma cultura, existem camadas

Existe um ponto que passa despercebido com frequência e que explica boa parte dos programas que parecem corretos e mesmo assim não chegam ao chão da operação. Um comportamento nunca acontece dentro de uma cultura. Acontece no cruzamento de várias.

O próprio Schein (2022) trata disso ao distinguir macroculturas, culturas organizacionais e subculturas até o nível dos grupos pequenos. Martin (1992) argumenta que a organização não possui uma cultura, mas culturas que convivem em tensão, com zonas de consenso, zonas de diferenciação e zonas de ambiguidade. E Van Maanen e Barley (1984) acrescentam uma camada que a nossa área quase nunca considera, a da comunidade ocupacional, mostrando que profissionais frequentemente respondem mais aos códigos do seu ofício do que aos da empresa que assina a carteira, e que comportamentos vistos como desviantes pela organização podem ser, na prática, condutas historicamente consolidadas entre os pares daquele ofício.

Some as camadas e o quadro fica claro. Há a cultura do país e da região, a do setor de atuação, a da ocupação, a da organização e a do grupo imediato. Elas não concordam entre si, e quando divergem quem costuma vencer é a mais próxima, porque é dela que vêm o exemplo diário, o pertencimento e a consequência imediata. O código de conduta fala na escala corporativa. A decisão acontece na escala da equipe. São endereços diferentes. Isso tem um desdobramento que qualquer gestor de integridade reconhece. Duas áreas da mesma empresa, submetidas ao mesmo código, ao mesmo treinamento e ao mesmo canal, apresentam comportamentos completamente distintos. Não é falha do programa. É que o programa foi desenhado para uma escala em que decisão nenhuma acontece.

Insisto nesse ponto, porque ele é quase sempre tratado como curiosidade e é, na verdade, um problema central de desenho. Imagine um profissional recém-contratado. Ele passa pela integração institucional, recebe o código, assiste ao treinamento e assina o termo. Tudo correto e tudo verdadeiro. Em seguida ele se senta à sua mesa e começa a aprender como as coisas funcionam de fato, e esse aprendizado vem inteiro da camada mais próxima: o que o colega ao lado faz, o que o gestor direto cobra com insistência e o que ele deixa passar, qual atalho é comentado em tom de brincadeira e qual assunto emudece a sala. Em poucas semanas ele já sabe operar naquele ambiente. Nada do que ele aprendeu estava no material de integração, e nada disso foi ensinado por alguém que tivesse a intenção de ensinar.

Note o que acontece nesse intervalo. Não houve conflito entre o código e a prática, houve substituição silenciosa. O código continua lá, íntegro, correto, disponível na intranet, e simplesmente não é consultado, porque a pessoa já obteve uma resposta mais barata, mais rápida e mais confiável sobre como se comportar. Berger e Luckmann (2014) chamariam isso de socialização secundária, e é assim que a cultura incumbente se reproduz sem esforço, sem plano e sem responsável identificável.

Existe também a camada ocupacional, que merece atenção porque produz um efeito contraintuitivo. Profissionais de uma mesma especialidade, espalhados por empresas concorrentes, frequentemente compartilham entre si mais critérios, jargões e noções do que é aceitável do que compartilham com colegas de outras áreas da própria organização. Quando alguém diz que determinada prática é normal no mercado, é bem provável que esteja dizendo a verdade sobre a sua comunidade ocupacional e não sobre a sua empresa. E quando a organização tenta impor uma regra que contraria esse repertório de ofício, ela não está enfrentando má-fé, está enfrentando uma cultura que é mais antiga do que ela e que sobreviverá a ela.

1.3 Valores só existem em ordem

Falta um elemento para fechar esta seção, e ele é tratado com um descuido que me impressiona. Valor isolado não decide nada.

Valor só aparece quando entra em conflito com outro valor, e conflito não se resolve por lista, se resolve por ordem. Rokeach (1973) trata valores exatamente assim, como um sistema organizado por prioridade relativa, em que o que importa não é a presença do valor e sim a posição que ele ocupa quando dois deles se chocam. Quando uma empresa publica cinco valores lado a lado, sem hierarquia declarada, ela não deixou de ter hierarquia. Ela apenas transferiu a decisão para o momento da pressão, e quem decide ali é quem tem mais poder na sala.

A pergunta, então, tem que ser feita sem meio-termo. Negócio ou integridade? Se a resposta for integridade, ela vem antes, e vem antes inclusive quando custa caro. Se a resposta for outra, tudo bem, mas que seja dita, porque a organização que não responde a essa pergunta no dia tranquilo será obrigada a respondê-la no dia difícil, e aí quem responde é o contexto.

Observem o que ocorre no vazio deixado pela ausência de ordem declarada. A decisão não desaparece, ela apenas migra. Migra para o gestor mais próximo, para o momento de maior pressão e para o critério de quem tem mais a perder naquela reunião específica. E como cada uma dessas decisões cria precedente, a hierarquia real acaba sendo construída por acúmulo de casos, um a um, sem que ninguém tenha jamais sentado para defini-la. Ao final de alguns anos, a empresa tem uma ordem de prioridades bastante nítida, conhecida por todos, e que não coincide com a que está na parede.

Argyris e Schön (1974) nomearam esse descompasso de um jeito que me parece o mais honesto que já li sobre o tema. Existe a teoria que a pessoa professa, aquela que ela declara sinceramente quando perguntada, e existe a teoria que de fato governa a sua ação. As duas costumam divergir, e o que torna o fenômeno interessante é que raramente há cinismo envolvido. A pessoa acredita no que diz. Ela apenas não age por aquilo. Transportada para a organização, essa distinção explica por que auditar documento não serve para medir cultura. O documento registra a teoria professada. A cultura está na outra: na teoria que de fato governa a ação.

2. O que a organização ensina todo dia

Se a cultura se forma pela prática repetida, então a pergunta que interessa é o que a organização repete. E aqui chegamos ao ponto mais desconfortável deste artigo, porque na disputa entre o comportamento que queremos e o que não queremos, o segundo joga com vantagem.

A vantagem não é moral, é estrutural, e o primeiro motivo é o mais simples de todos. O desvio prova que funciona. O atalho entrega o número no prazo, salva o contrato, resolve o problema que estava travando a operação. Como a sedimentação cultural depende exatamente disso, de algo que deu certo e por isso é repetido, o comportamento indesejado alimenta o mecanismo com facilidade.

Há um segundo motivo, ligado ao tamanho do primeiro passo. O desvio relevante quase nunca começa relevante. Começa pequeno o bastante para não parecer um problema, pequeno o bastante para caber em uma justificativa razoável e pequeno o bastante para que discutir aquilo pareça exagero. Uma exceção pontual em um cadastro. Um prazo cumprido com documentação incompleta que será regularizada depois. Uma aprovação dada por telefone que ficou de ser formalizada. Nenhum desses episódios, isoladamente, sustentaria uma conversa séria. Somados ao longo do tempo, eles constroem o padrão.

Vaughan (1996), ao estudar a decisão de lançamento do ônibus espacial Challenger, descreveu esse processo com o nome que se tornou referência: a normalização do desvio. Uma anomalia aparece, é avaliada, é considerada aceitável naquele contexto específico e o resultado vem sem incidente. Na vez seguinte, a anomalia já tem precedente. Repetida algumas vezes, ela deixa de ser anomalia e passa a ser o padrão esperado, sem que ninguém, em momento nenhum, tenha tomado a decisão de baixar a régua. A régua desceu sozinha, por acúmulo.

Ashforth e Anand (2003) levam essa lógica para dentro do ambiente corporativo e propõem três processos que se reforçam mutuamente. A institucionalização, em que um ato inicialmente isolado se incorpora a estruturas e processos até virar rotina. A racionalização, em que se

desenvolvem justificativas que tornam a prática aceitável e às vezes até meritória. E a socialização, pela qual os recém-chegados são conduzidos a enxergar aquela prática como admissível, quando não desejável. O modelo explica algo que qualquer investigador experiente já viu e que continua sendo difícil de aceitar: indivíduos que, examinados isoladamente, são pessoas corretas, participam de forma rotineira de práticas irregulares sem experimentar conflito interno.

E é no segundo desses pilares que está, a meu ver, a maior assimetria de todas. Sykes e Matza (1957), em trabalho clássico da criminologia, descreveram cinco técnicas de neutralização: a negação da responsabilidade, a negação do dano, a negação da vítima, a condenação de quem condena e o apelo a lealdades superiores. O achado decisivo, e que a leitura apressada deixa escapar, é que essas racionalizações não surgem apenas depois do ato para aliviar a culpa. Elas o precedem e o tornam possível.

Calma, eu explico por que isso importa tanto para a disputa cultural. Quem transgride precisa se justificar, e a justificativa, para funcionar, tem que ser compartilhável. Ela vira frase, vira explicação pronta, vira vocabulário que circula pelo corredor, é ensinada ao novato e herdada por quem chega depois. Todo mundo faz assim. É prática de mercado. Não prejudica ninguém. É para o bem da empresa. Isso é material cultural puro, transmissível e durável. Já quem cumpre a regra não precisa justificar nada, e por isso não produz vocabulário algum. Um dos lados da disputa fabrica cultura o tempo todo. O outro, quase nunca.

Some-se a isso um problema de visibilidade que agrava o quadro. Weick (1987), ao estudar organizações que operam sob alto risco, observou que a confiabilidade se manifesta pela ausência de acontecimento, o que a torna um fenômeno de difícil percepção e de reconhecimento raro. Traduzindo para a nossa realidade, o comportamento correto tem um defeito grave de comunicação: quando funciona, nada acontece. A fraude que não ocorreu não gera evidência. O negócio recusado não entra em relatório. O profissional que impediu um problema não tem o que mostrar, porque o problema não existiu. Enquanto isso, o resultado obtido por atalho aparece na apresentação de resultados, com número, com gráfico e com aplauso.

Essa assimetria de visibilidade tem uma consequência que raramente é discutida e que atinge diretamente quem trabalha com integridade. A área que previne vive de comprovar aquilo que não aconteceu, e essa é uma das posições mais desconfortáveis que existem dentro de uma organização. Quando o programa funciona, não há nada para mostrar. Quando falha, há o incidente inteiro, com nome, valor e manchete. O efeito perverso é que a área tende a ser avaliada justamente nos seus piores momentos e a ficar invisível nos melhores, o que ajuda a explicar por que orçamentos de integridade crescem depois da crise e encolhem no período de calmaria, exatamente na ordem contrária à que faria sentido.

Por fim, há aquilo que a organização comunica quando não faz nada. Treviño, Weaver e Reynolds (2006) mostram, revisando a literatura de ética comportamental nas organizações, que as pessoas leem a cultura ética por sinais formais e informais da organização, entre eles a liderança, o comportamento dos pares, as recompensas, as punições e a avaliação de desempenho. Os autores observam, inclusive, que a dimensão informal pode pesar tanto quanto o programa formal. Isso significa que a ausência de consequência não é neutra. Ela é uma resposta, e é lida como tal. Quando alguém entrega resultado por fora da regra e nada acontece, a organização acabou de ensinar, com clareza superior à de qualquer treinamento, qual é a sua hierarquia real de valores.

E convém reconhecer que essa leitura é feita com uma precisão notável. As pessoas não precisam de acesso ao processo disciplinar, ao relatório de investigação ou à ata do comitê para saber o que aconteceu. Elas observam se a pessoa continua na empresa, se manteve a equipe, se apareceu no palco da convenção anual, se foi promovida no ciclo seguinte. Essas informações são públicas, circulam rápido e são interpretadas sem margem para dúvida. Nenhuma comunicação institucional compete com esse tipo de evidência, e nenhum discurso desmente o que todos viram acontecer.

Este é, aliás, o único teste que resolve a ambiguidade para todo mundo ao mesmo tempo, e é o evento que a empresa inteira assiste com atenção: que acontece com quem entregou o número por fora.

3. Disputar a cultura existente

Chego então à consequência prática, e ela começa por uma correção de verbo. Ninguém constrói cultura de integridade do zero, porque não existe organização sem cultura. O que existe é uma cultura incumbente, já sedimentada, que socializa bem, que tem vocabulário próprio e que venceu essa disputa antes de qualquer um de nós chegar. Nosso trabalho não é implantar. É disputar.

E disputa se ganha atacando as vantagens do outro lado, uma a uma.

A primeira é a invisibilidade do comportamento correto. Se o certo não gera evidência, cabe à organização fabricá-la. Isso significa dar ao negócio recusado o mesmo tratamento narrativo que se dá ao contrato fechado, reconhecer, quando cabível e sem comprometer a confidencialidade ou a vontade de quem se expôs, aquele que sustentou uma decisão difícil, e tratar essa decisão como caso a ser contado. Não se trata de campanha motivacional. Trata-se de fornecer à cultura aquilo que ela usa como matéria-prima, que é história de algo que deu certo.

A segunda é a racionalização. Como as técnicas de neutralização operam melhor enquanto não são nomeadas, nomeá-las é interferir diretamente no mecanismo. Em auditorias de cultura, uma das informações mais úteis que se pode extrair não são os números de adesão a treinamento, e sim as frases que circulam. O vocabulário de justificativa de uma empresa é um diagnóstico. Quando esse repertório é exposto e discutido abertamente, com as palavras que as pessoas realmente usam, ele perde parte considerável da sua função protetora.

A terceira é a escala. Como a decisão acontece no grupo imediato, é lá que a intervenção precisa chegar. Programas desenhados apenas no nível corporativo falam num endereço onde ninguém decide. Na prática, isso significa parar de tratar a liderança intermediária como público de treinamento e passar a tratá-la como o lugar em que a cultura é efetivamente operada. O gestor direto é quem cobra a meta, autoriza a exceção, conduz a conversa difícil e decide o que vira caso e o que vira silêncio. Se ele não souber o que fazer quando alguém da equipe traz um desconforto, o canal de denúncia, por melhor que seja, receberá apenas o que já virou problema grande.

Isso exige também aceitar algo que incomoda quem gosta de padronização: áreas diferentes da mesma empresa podem precisar de abordagens diferentes. Uma diretriz única, aplicada uniformemente a contextos que têm culturas locais distintas, produz adesão desigual e depois se conclui, erroneamente, que o problema é de engajamento das pessoas.

A quarta é a hierarquia de valores. Ela precisa ser declarada antes do conflito e, principalmente, precisa ser confirmada quando custa. Um único caso em que a organização abre mão de um resultado relevante para preservar um princípio ensina mais do que todo o material de comunicação produzido no ano. E o inverso também é verdadeiro, com a mesma força e a mesma velocidade.

Há um exercício simples e revelador para testar se essa hierarquia existe de fato. Peça aos executivos que descrevam a última vez em que a empresa recusou um negócio por razão de integridade. Se a resposta vier rápida, com detalhes e com o nome de quem tomou a decisão, existe hierarquia. Se vier acompanhada de esforço de memória, de generalidades ou de exemplos hipotéticos, a ordem de prioridade ainda não foi testada, e uma ordem que nunca foi testada não é uma ordem, é uma intenção.

A quinta é a consequência, e aqui não há saída elegante. Consequência aplicada de forma desigual conforme o nível hierárquico, ou conforme o quanto a pessoa entrega, não enfraquece o programa. Ela o substitui. Passa a ser ela a regra ensinada, e passa a ser ensinada com mais eficácia do que qualquer conteúdo formal, porque chega acompanhada de prova. É desconfortável dizer isso, mas nenhuma das quatro alavancas anteriores sobrevive se esta falhar.

Convém acrescentar que consequência não significa apenas punição. O reconhecimento também é consequência, e é a forma menos explorada de todas. Organizações que sabem exatamente o que fazer com quem descumpre raramente sabem o que fazer com quem cumpre em situação difícil, e essa lacuna mantém intacta a assimetria de visibilidade discutida na seção anterior.

Preciso ser honesto quanto aos limites. Nada disso funciona em contextos nos quais a pressão não é efeito colateral da operação e sim o próprio modelo de negócio. Existem organizações em que a cultura incumbente é inseparável da estratégia, e nesses casos o Programa de

integridade cumpre função decorativa, por melhor que seja quem o conduz. Reconhecer isso cedo é uma decisão técnica e não uma derrota.

Também é preciso dizer que disputa cultural não acontece em curto prazo. Se a cultura atual se formou por acúmulo de comportamentos ao longo de anos, é razoável supor que a nova se forme pelo mesmo mecanismo e em ritmo semelhante. Isso coloca um problema real de gestão, porque mandatos executivos são mais curtos do que processos de sedimentação, e há um incentivo natural para se preferir a iniciativa que produz entregável visível dentro do ciclo de avaliação. Campanha se mede em três meses. Precedente se mede em anos. Essa diferença de horizonte explica boa parte das escolhas ruins que a nossa área faz por boas razões.

Por fim, vale registrar o que não foi tratado aqui. Não discuti o comportamento do indivíduo diante da pressão no instante da decisão, que é um campo próprio e que exige tratamento à parte. Este artigo permaneceu no nível organizacional, que é o âmbito em que o Programa de Integridade opera e em que o organizador de um bloco sobre cultura deve, a meu ver, se posicionar.

Conclusão

Retomo a pergunta inicial. Por que empresas com código aprovado, política publicada, treinamento aplicado e canal em funcionamento continuam produzindo desvios relevantes? A resposta que este artigo sustenta é que esses instrumentos foram desenhados para atuar sobre aquilo que a cultura produz, e não sobre aquilo que a produz.

A literatura converge nesse ponto com uma consistência que surpreende quem espera encontrar controvérsia. O pressuposto cultural é resultado de aprendizado repetido, a instituição nasce do hábito tipificado, a cultura funciona como repertório disponível e não como valor determinante, e a normalização do desvio se dá por acúmulo de precedentes que ninguém decidiu criar. Some-se a isso a constatação de que os comportamentos acontecem no cruzamento de várias culturas simultâneas, que valores só operam quando ordenados e que a organização ensina muito mais pela consequência do que pelo discurso, e o que resta é um deslocamento de foco: o objeto de gestão deixa de ser o que a empresa declara e passa a ser o que ela repete, tolera e recompensa.

Há limitações evidentes. Este é um artigo de natureza teórica e reflexiva, sem dados primários próprios, e as intervenções aqui propostas derivam da literatura e da prática profissional, não de mensuração controlada. A própria distinção entre origem e manutenção da cultura, central ao argumento, comporta debate legítimo. E a construção de indicadores capazes de capturar o que aqui se defende permanece um problema em aberto, sobre o qual os artigos seguintes deste capítulo trazem contribuições relevantes.

Se algo deve ficar, que seja o incômodo produtivo de olhar para a própria organização e reconhecer que ela já tem uma cultura, que essa cultura foi construída por comportamentos que alguém repetiu, alguém tolerou e alguém recompensou, e que o trabalho que temos pela frente não é o de erguer algo novo sobre terreno vazio. É o de disputar terreno ocupado.

Referências

ARGYRIS, Chris; SCHÖN, Donald A. Theory in practice: increasing professional effectiveness. San Francisco: Jossey-Bass, 1974.

ASHFORTH, Blake E.; ANAND, Vikas. The normalization of corruption in organizations. *Research in Organizational Behavior*, [S. l.], v. 25, p. 1-52, 2003 DOI: doi.org/10.1016/S0191-3085(03)25001-2.

BERGER, Peter L.; LUCKMANN, Thomas. *A construção social da realidade*: tratado de sociologia do conhecimento. Tradução de Floriano de Souza Fernandes. Petrópolis: Vozes, 2014.

BRASIL. Decreto nº 11.129, de 11 de julho de 2022. Regulamenta a Lei nº 12.846, de 1º de agosto de 2013, que dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira. *Diário Oficial da União*: seção 1, Brasília, DF, 12 jul. 2022.

BRASIL. Lei nº 12.846, de 1º de agosto de 2013. Dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira, e dá outras providências. *Diário Oficial da União*: seção 1, Brasília, DF, 2 ago. 2013.

GEERTZ, Clifford. *A interpretação das culturas*. Rio de Janeiro: LTC, 2008.

MARTIN, Joanne. *Cultures in organizations:* three perspectives. New York: Oxford University Press, 1992.

ROKEACH, Milton. *The nature of human values*. New York: Free Press, 1973.

SCHEIN, Edgar H.; SCHEIN, Peter A. *Cultura organizacional e liderança*. 5. ed. São Paulo: GEN Atlas, 2022.

SWIDLER, Ann. Culture in action: symbols and strategies. *American Sociological Review*, [S. l.],v. 51, n. 2, p. 273-286, 1986. DOI: https://doi.org/10.2307/2095521.

SYKES, Gresham M.; MATZA, David. Techniques of neutralization: a theory of delinquency. *American Sociological Review*, [S. l.], v. 22, p. 664-670, 1957. DOI: https://doi.org/10.1590/S0103-49792008000100012.

TREVIÑO, Linda K.; WEAVER, Gary R.; REYNOLDS, Scott J. Behavioral ethics in organizations: a review. *Journal of Management*, [*S. l.*], v. 32, n. 6, p. 951-990, 2006. DOI: https://doi.org/10.1177/014920630629425.

VAN MAANEN, John; BARLEY, Stephen R. Occupational communities: culture and control in organizations. *Research in Organizational Behavior*, [*S. l.*], v. 6, p. 287-365, 1984. Disponível em: https://www.semanticscholar.org/paper/Occupational-Communities%3A-Culture-and-Control-in-Maanen-Barley/f8f0e6fb20bca135cf58965412420d017b6aaf31. Acesso em: 17 out. 2026.

VAUGHAN, Diane. *The Challenger launch decision*: risky technology, culture, and deviance at NASA. Chicago: University of Chicago Press, 1996.

WEICK, Karl E. Organizational culture as a source of high reliability. *California management review*, [*S. l.*], v. 29, n. 2, p. 112-127, 1987. Disponível em: https://www.semanticscholar.org/paper/Organizational-Culture-as-a-Source-of-High-Weick/2401f0a8ee5f100d64ff1f731bce2fe7755a1c9d. Acesso em: 17 out. 2026.

Desafios contemporâneos à cultura de integridade nas organizações:

uma análise à luz da ética, das transformações sociais e da moralidade humana

Ana Carla Coutinho Torres

Ana Carla Coutinho Torres é Consultora em Integridade Corporativa da Firjan. Doutora e mestre em Educação, na linha de pesquisa Representações Sociais; Pós-graduada em *Compliance*, Riscos e Auditoria, e em Recursos Humanos. Certificada em *Compliance* (CPC-A) e Privacidade e Proteção de Dados (CPPD). Possui mais de 20 anos de experiência com empresas do setor industrial e combina sólida formação acadêmica com atuação prática em projetos estratégicos de integridade.

Introdução

A consolidação de uma cultura de integridade nas organizações contemporâneas constitui um dos principais desafios da governança corporativa. Em um ambiente marcado por transformações tecnológicas aceleradas, pressão por resultados imediatos e crescente vigilância social, decisões éticas tornaram-se ao mesmo tempo mais complexas, mais velozes e mais impactantes. Cada decisão organizacional, por menor que pareça, carrega implicações éticas, reputacionais e humanas que não podem ser ignoradas.

É nesse contexto que a cultura de integridade emerge não como um luxo moral, mas como uma necessidade estratégica. Novas dinâmicas sociais e pressões surgem em um cenário complexo no qual decisões éticas se tornaram mais difíceis, mais rápidas e mais impactantes.

Compreender esse fenômeno implica revisitar conceitos fundamentais como moral, ética, valores e cultura. Conforme Morin (2011), a ética expressa a capacidade humana de orientar ações considerando o impacto sobre o outro, enquanto a moral consolida normas e expectativas sociais de comportamento.

Para Schein (2022), a cultura organizacional representa o conjunto de pressupostos compartilhados que orientam como pessoas percebem, pensam e agem dentro de uma organização.

Ao aprofundar a definição de cultura, Santos (1949) descreve-a como o conjunto de valores, práticas, conhecimentos e modos de vida que são aprendidos e compartilhados socialmente, orientando a forma como as pessoas pensam, agem e interpretam o mundo. O autor destaca que a cultura não é algo natural ou biológico, mas construída nas relações sociais, sendo diversa, dinâmica e atravessada por contextos históricos e relações de poder. Assim, mais do que manifestações artísticas ou eruditas, a cultura está presente no cotidiano, moldando comportamentos e dando sentido à vida em sociedade.

Já para Laraia (2000), que trabalha a cultura sob a perspectiva antropológica, ela é compreendida como um sistema aprendido de comportamentos, conhecimentos e significados que orienta a vida humana, distinguindo o homem dos demais animais. O autor enfatiza que a cultura não é determinada biologicamente, mas adquirida por meio da convivência social, sendo responsável por moldar percepções, valores e formas de agir. Laraia (2000) também destaca o caráter dinâmico e adaptativo da cultura, além de criticar o etnocentrismo, defendendo que as diferenças culturais devem ser entendidas em seus próprios contextos, e não hierarquizadas, evidenciando que cada sociedade desenvolve soluções próprias para suas necessidades e seus desafios.

Seguindo nesse contexto, e conectando os conceitos de cultura com ética e moral, Konrad Lorenz contribui com reflexões relevantes ao destacar que o desenvolvimento moral humano ocorre de forma mais lenta e menos previsível do que o desenvolvimento intelectual e tecnológico (Lorenz, 1973). Esse descompasso cria um 'vazio moral' que se torna mais evidente quando tecnologias como inteligência artificial e sistemas algorítmicos se inserem na vida social e no ambiente de trabalho.

Este artigo propõe uma reflexão sobre os desafios contemporâneos à cultura de integridade, articulando fundamentos teóricos da ética, da moral e da cultura organizacional com dilemas concretos enfrentados pelas organizações modernas.

1. Fundamentação teórica: moral, ética e cultura

1.1 Moral

A moral pode ser compreendida como o conjunto de valores, normas e princípios que orientam o comportamento humano em sociedade, estabelecendo critérios sobre o que é considerado certo ou errado, justo ou injusto, adequado ou inadequado. Diferentemente de regras jurídicas, que são formalmente instituídas e coercitivas, a moral opera principalmente no campo da consciência individual e da regulação social informal, sendo construída historicamente e compartilhada por grupos sociais. Nesse sentido, a moral não é universal e imutável, mas varia conforme o contexto cultural, social e temporal, refletindo as crenças e práticas de determinada coletividade.

No campo da filosofia, a moral é objeto de estudo da ética, que busca analisar criticamente os fundamentos dos valores e normas. Para Aristóteles (1915), por exemplo, a moral está relacionada à busca da virtude e da felicidade (eudaimonia), sendo construída a partir do hábito e do equilíbrio entre excessos e faltas. Já Kant (1797) propõe uma concepção de moral baseada no dever e na razão, expressa no imperativo categórico, segundo o qual as ações devem ser orientadas por princípios que possam ser universalizados. Em outra perspectiva, Durkheim (2018) entende a moral como um fato social, ou seja, um conjunto de regras e valores que existem independentemente do indivíduo e exercem sobre ele um poder coercitivo. Ainda conforme Durkheim (2018), trata-se de um fenômeno coletivo, que se impõe aos indivíduos como um padrão de conduta. Essas normas podem ser explícitas (leis, regulamentos) ou implícitas (convenções, tradições).

A moral também está intimamente ligada à cultura, uma vez que os valores morais são aprendidos e transmitidos socialmente, sendo internalizados pelos indivíduos ao longo do processo de socialização. Assim, aquilo que é considerado moralmente aceitável em uma sociedade pode não ser em outra, evidenciando o caráter relativo e dinâmico da moral. Essa relação entre moral e cultura é fundamental para a compreensão de comportamentos sociais e para o respeito à diversidade, evitando posturas etnocêntricas.

No contexto organizacional, a moral se manifesta de forma frequentemente implícita, expressa em práticas cotidianas, tolerâncias informais e padrões de comportamento que orientam condutas sem necessidade de formalização explícita.

Já nas relações contemporâneas, a moral assume papel central em discussões sobre responsabilidade social, ética profissional e governança, especialmente em ambientes organizacionais. A construção de Códigos de Ética, Políticas e programas de *Compliance* ou de Integridade refletem a tentativa de formalizar princípios morais em diretrizes práticas, orientando a conduta de indivíduos e organizações. Nesse sentido, a moral deixa de ser apenas uma questão individual e passa a integrar estratégias organizacionais voltadas à transparência, à confiança e à sustentabilidade.

O desafio surge quando essa moral entra em conflito com valores éticos mais amplos ou com princípios legais. É nesse ponto que normas morais internalizadas precisam ser submetidas à reflexão ética crítica.

Em síntese, a moral constitui um elemento essencial da vida em sociedade, funcionando como um guia para a ação humana e para a convivência coletiva. Embora sujeita a variações históricas e culturais, ela permanece como um referencial indispensável para a construção de relações sociais mais justas e equilibradas.

1.2 Ética

A ética é o campo da filosofia que se dedica à reflexão crítica sobre os valores, princípios e fundamentos que orientam a conduta humana, buscando compreender o que é o bem, o justo e o correto nas ações individuais e coletivas. Diferentemente da moral — que corresponde ao conjunto de normas e costumes efetivamente praticados por uma sociedade —, a ética tem caráter teórico e analítico, questionando e avaliando esses padrões, propondo critérios para sua legitimidade. Assim, enquanto a moral diz "o que é feito" ou "o que se considera certo", a ética investiga "por que isso é considerado certo" e "se deveria ser assim".

Ao longo da história, diferentes correntes filosóficas buscaram fundamentar a ética. Kant (1797) propõe uma ética do dever, baseada no imperativo categórico, segundo o qual devemos agir apenas conforme princípios que possam ser universalizados, independentemente das consequências. Em contraste, correntes consequencialistas, como a de Mill (2020), defendem que a moralidade das ações deve ser avaliada eticamente por seus resultados, especialmente pela capacidade de promover o maior bem-estar possível para o maior número de pessoas, ou seja, uma ação é considerada correta se produzir consequências boas, e incorreta se gerar consequências ruins.

A ética pode ser também um campo reflexivo, como demonstra Arendt (2004), para quem a ética diz respeito ao exercício da liberdade para pensar criticamente sobre o que é certo ou errado, considerando o impacto das ações sobre a coletividade. Enquanto a moral pode ser obedecida, a ética precisa ser compreendida e deliberada.

No campo contemporâneo, a ética se expande para além da filosofia, influenciando áreas como o direito, a política e a gestão organizacional. Autores como Vázquez (2017) destacam que a ética possui também uma dimensão prática, orientando a ação humana em contextos concretos e contribuindo para a transformação social. Nesse sentido, a ética não se limita à reflexão abstrata, mas se materializa em decisões cotidianas, políticas públicas e práticas institucionais.

No ambiente organizacional, a ética ganha relevância estratégica, sendo incorporada a códigos de conduta, programas e políticas de compliance ou de integridade. Esses instrumentos buscam alinhar o comportamento dos indivíduos aos valores institucionais, promovendo transparência, responsabilidade e confiança nas relações internas e externas. A ética, portanto, passa a ser vista não apenas como um ideal normativo, mas como um ativo que contribui para a sustentabilidade e a reputação das organizações — o que exige, adicionalmente, a criação de espaços de diálogo, escuta ativa e segurança psicológica para que questionamentos possam emergir sem medo de retaliação.

Em síntese, a ética é um instrumento essencial para a compreensão e orientação da conduta humana, permitindo avaliar criticamente normas e práticas sociais e promover ações mais justas e responsáveis. Ao articular princípios universais com contextos concretos, a ética se mantém como um campo dinâmico e indispensável para a vida em sociedade.

1.3 Cultura de Integridade

A cultura de integridade nasce da interação entre moral e ética no cotidiano organizacional. Ela é construída quando valores éticos são praticados de forma consistente, inclusive — e principalmente — quando isso implica custos ou escolhas difíceis.

A cultura de integridade pode ser compreendida como o conjunto de valores, princípios, normas e práticas compartilhadas que orientam o comportamento ético de indivíduos dentro de uma organização, promovendo decisões alinhadas à legalidade, à transparência e à responsabilidade. Mais do que a existência formal de regras, a cultura de integridade se manifesta na forma como essas diretrizes são efetivamente vivenciadas no cotidiano, influenciando atitudes, relações e processos decisórios. Trata-se, portanto, de um elemento estruturante da governança organizacional, que conecta discurso e prática, reduzindo a distância entre o que a organização declara e o que ela realiza.

Diferentemente de abordagens baseadas apenas em controle e conformidade, a cultura de integridade pressupõe a internalização de valores éticos pelos colaboradores, indo além do cumprimento obrigatório de normas. Nesse sentido, ela está intimamente ligada ao conceito de cultura organizacional, entendido como o sistema de

significados compartilhados que orienta o comportamento dos membros de uma instituição.

Schein (2022) explica que a cultura se expressa em níveis profundos, incluindo pressupostos inconscientes que influenciam a forma de agir, de modo que a cultura organizacional constitui um sistema de significados compartilhados que orientam comportamentos.

Assim, a cultura de integridade é a expressão dessa cultura aplicada à ética: trata-se do ambiente no qual decisões transparentes, responsáveis e alinhadas a valores são estimuladas, reconhecidas e monitoradas. De forma complementar, para Bennis (2009), uma cultura de integridade sólida depende não apenas de códigos de ética, políticas ou outros documentos relevantes de uma estrutura organizacional, mas de liderança exemplar, com coerência de discurso, comunicação consistente e incentivos alinhados.

No campo da integridade corporativa, organismos internacionais como a Organização para a Cooperação e Desenvolvimento Econômico ressaltam que programas eficazes devem ser baseados em valores e não apenas em regras, promovendo ambientes em que comportamentos éticos sejam incentivados e desvios sejam prevenidos de forma proativa. No Brasil, a Lei Anticorrupção e suas regulamentações reforçam a importância de mecanismos de integridade, como códigos de conduta, canais de denúncia e treinamentos, como elementos essenciais para a prevenção de irregularidades e a responsabilização de pessoas jurídicas.

Além disso, a cultura de integridade está diretamente relacionada à gestão de riscos, incluindo aqueles de natureza ética, reputacional e, mais recentemente, tecnológica, como o uso de inteligência artificial. Nesse contexto, a integridade passa a ser um diferencial competitivo, contribuindo para a construção de confiança junto a *stakeholders*, a sustentabilidade dos negócios e a mitigação de riscos legais e institucionais.

Em síntese, a cultura de integridade representa a consolidação de um ambiente organizacional em que agir corretamente não é apenas uma obrigação formal, mas um valor incorporado às práticas diárias. Sua efetividade depende da coerência entre liderança, normas e comportamentos, sendo um fator essencial para organizações que buscam não apenas resultados, mas legitimidade e perenidade em suas relações.

2. Desafios contemporâneos à cultura de integridade

A consolidação de uma cultura de integridade nas organizações contemporâneas ocorre em um cenário marcado por profundas transformações tecnológicas, sociais e econômicas. Se, por um lado, tais mudanças ampliam oportunidades de inovação, eficiência e crescimento, por outro, também introduzem riscos éticos complexos e, muitas vezes, inéditos. Nesse contexto, a ética deixa de ser um elemento acessório e passa a ocupar posição estratégica na sustentabilidade e legitimidade das organizações (Floridi, 2015; Harari, 2016).

A cultura de integridade, portanto, precisa evoluir continuamente para responder a esses novos desafios, incorporando não apenas normas e controles, mas também valores, práticas e mecanismos que garantam decisões responsáveis em ambientes cada vez mais dinâmicos e incertos.

2.1 Transformação digital

A transformação digital é um dos principais vetores de mudança nas organizações contemporâneas. A digitalização de processos e o uso intensivo de dados têm permitido ganhos expressivos de produtividade, mas também trazem implicações éticas relevantes.

Um dos principais desafios está relacionado à velocidade das decisões, que reduz o espaço para reflexão ética. Além disso, a coleta massiva de dados pessoais, muitas vezes sem transparência adequada, configura um cenário que Zuboff (2019) denomina "capitalismo de vigilância", no qual dados são explorados como ativos econômicos, frequentemente em detrimento da autonomia dos indivíduos.

A crescente dependência de sistemas digitais também

amplia os riscos relacionados à segurança da informação e à exposição a vulnerabilidades cibernéticas. Nesse sentido, marcos regulatórios como o *General Data Protection Regulation* e a Lei Geral de Proteção de Dados Pessoais surgem como instrumentos fundamentais para mitigar riscos e promover maior responsabilidade no tratamento de dados.

Diante desse cenário, a cultura de integridade deve incorporar práticas de governança de dados, transparência e os princípios de *privacy by design e privacy by default*, garantindo que a ética esteja presente desde a concepção das soluções tecnológicas (Floridi, 2015). A integração entre tecnologia e ética impõe às organizações uma transformação não apenas operacional, mas também cultural, na qual a pergunta central deixa de ser "podemos fazer?" e passa a ser "devemos fazer?".

2.2 Inteligência Artificial e automação

A inteligência artificial adiciona uma camada extra de complexidade nas decisões organizacionais. Sistemas automatizados podem reproduzir vieses existentes nos dados e gerar decisões discriminatórias, muitas vezes de forma invisível.

Lanier (2018) alerta para o risco de delegarmos decisões moralmente relevantes a sistemas que não possuem compreensão ética, o que pode resultar em uma perda de controle humano sobre processos críticos. Da mesma forma, Bostrom (2014) discute os riscos associados ao desenvolvimento de sistemas inteligentes que operam além da plena compreensão humana.

A Organização para a Cooperação e Desenvolvimento Econômico (2019) reforça a necessidade de que sistemas de inteligência artificial sejam transparentes, explicáveis e responsáveis, garantindo justiça e segurança no seu uso.

Nesse contexto, a cultura de integridade deve incluir a criação de comitês de ética em inteligência artificial, auditorias algorítmicas e manutenção do controle humano nas decisões mais sensíveis (*human in the loop*). A automação, portanto, não dispensa a responsabilidade humana — ela a exige de forma ainda mais estruturada, com supervisão ativa, mecanismos de explicabilidade e canais de contestação acessíveis.

2.3 Diversidade, inclusão e pertencimento

A promoção da diversidade e inclusão representa um avanço importante, mas também introduz novos desafios éticos relacionados à convivência e à equidade. Ambientes diversos exigem maior maturidade organizacional para lidar com diferenças culturais, sociais e cognitivas.

Segundo Sen (2009), a justiça está diretamente relacionada à capacidade de garantir condições equitativas de participação e reconhecimento das diferenças. Nesse sentido, a diversidade só se traduz em valor quando acompanhada de práticas inclusivas efetivas.

A cultura de integridade deve, portanto, promover políticas antidiscriminação, treinamentos contínuos e mecanismos seguros de denúncia, assegurando que todos os indivíduos possam atuar em um ambiente respeitoso e ético. A efetividade dessas iniciativas depende da disposição organizacional de revisar práticas consolidadas, enfrentar desconfortos institucionais e assegurar que vozes historicamente sub-representadas sejam efetivamente consideradas nos processos decisórios.

2.4 ESG e responsabilidade socioambiental

A agenda ESG amplia o escopo da responsabilidade ética das organizações, incorporando dimensões ambientais, sociais e de governança. No entanto, um dos principais desafios é evitar que tais práticas sejam utilizadas apenas como estratégia de reputação, sem comprometimento real com seus fundamentos.

A Organização das Nações Unidas (2015), por meio da Agenda 2030, reforça a necessidade de compromisso real com o desenvolvimento sustentável. Da mesma forma, a *Global Reporting Initiative* estabelece padrões para transparência e prestação de contas, essenciais para a credibilidade das ações ESG.

Sem métricas claras e *accountability,* iniciativas ESG correm o risco de se tornarem meramente simbólicas, comprometendo a confiança dos *stakeholders.* Assumir responsabilidade socioambiental implica, portanto, reconhecer impactos reais — inclusive negativos —, adotar mecanismos de prestação de contas e agir para mitigar danos, mesmo quando isso não gera retornos imediatos.

2.5 Trabalho remoto e novas relações de trabalho

A expansão do trabalho remoto e híbrido redesenhou as fronteiras entre vida profissional e pessoal, ampliando a autonomia dos trabalhadores, mas também introduzindo novas formas de pressão e de invisibilidade das condutas.

Sennett (2012) destaca que a cooperação em ambientes flexíveis exige novos mecanismos de construção de confiança, baseados menos em controle direto e mais em valores compartilhados.

Além disso, o aumento da pressão individual por resultados e a menor separação entre vida pessoal e profissional podem favorecer práticas inadequadas, como o assédio virtual e a sobrecarga de trabalho.

Nesse cenário, torna-se essencial reforçar a cultura organizacional por meio de comunicação clara, liderança ativa e mecanismos estruturados de acompanhamento. A integridade, nesse contexto, abrange também o respeito ao tempo, à saúde mental e aos limites humanos, exigindo que as organizações estabeleçam expectativas claras e protejam os vínculos éticos que a distância física tende a fragilizar.

2.6 Pressões competitivas e dilemas éticos

As pressões competitivas dos mercados contemporâneos representam um dos maiores riscos à integridade organizacional. A busca por resultados pode incentivar comportamentos de risco e decisões antiéticas.

Como já alertava Lorenz (2001), impulsos como competição e agressividade fazem parte da natureza humana e podem se intensificar em ambientes de disputa. No contexto organizacional, isso pode levar a manipulação de dados, omissões e justificativas éticas baseadas nos resultados.

Casos como o da Enron evidenciam como culturas orientadas exclusivamente por desempenho podem resultar em colapsos institucionais (McLean; Elkind, 2013).

Diante disso, uma cultura sólida de integridade atua como barreira moral, alinhando comportamento individual e valores organizacionais mesmo sob pressão. Os desafios contemporâneos à cultura de integridade são multifacetados e interdependentes: a transformação digital, a inteligência artificial, a diversidade, a agenda ESG, as novas formas de trabalho e as pressões competitivas exigem uma abordagem ética cada vez mais estruturada, integrada e consciente — condição essencial para a sustentabilidade organizacional no século XXI (Floridi, 2015; OCDE, 2019).

3. Da fragilidade moral à racionalização do desvio: fundamentos teóricos para o debate ético nas organizações

A compreensão dos desafios éticos que as organizações enfrentam no século XXI exige ir além do diagnóstico dos fenômenos contemporâneos — transformação digital, pressões competitivas, novas formas de trabalho — para investigar as raízes mais profundas da fragilidade moral humana. Por que indivíduos e organizações se desviam de normas éticas mesmo quando as conhecem? Por que programas de compliance ou de Integridade, Códigos de Ética e Políticas bem estruturadas frequentemente não se traduzem em comportamentos coerentes? Responder a essas questões implica mobilizar uma base teórica que articule dimensões evolutivas, sociológicas, psicológicas, neurocientíficas e filosóficas do desvio moral.

Existem muitas perspectivas teóricas sobre o tema, e este artigo abarcará cinco delas, que contribuem, de forma complementar, para essa compreensão: (i) Konrad Lorenz, que identifica, no plano evolutivo, o descompasso entre o ritmo do desenvolvimento técnico-intelectual e o da maturidade moral humana; (ii) Zygmunt Bauman, que demonstra como estruturas burocráticas modernas dissolvem a responsabilidade moral ao fragmentar tarefas e distanciar indivíduos das consequências de suas ações; (iii) Albert Bandura, que mapeia os mecanismos psicológicos pelos quais pessoas moralmente funcionais suspendem seus próprios padrões éticos em contextos de pressão; (iv) Joshua Greene, que revela que o julgamento moral humano opera por dois sistemas cognitivos distintos — um intuitivo-emocional e um deliberativo-racional —, ambos sujeitos a distorções situacionais; e (v) Hannah Arendt, que argumenta que o mal, em sua forma mais corriqueira e perigosa, não emerge de intenções malignas, mas da incapacidade de pensar criticamente sobre as consequências das próprias ações em contextos institucionais. Juntos, esses cinco autores oferecem um quadro teórico robusto para compreender por que estruturas éticas formais são condição necessária, mas insuficiente, para a integridade organizacional.

3.1 Konrad Lorenz: instintos, evolução e o descompasso moral

Konrad Lorenz, reconhecido como um dos fundadores da etologia moderna, dedicou sua trajetória científica à compreensão dos padrões comportamentais instintivos presentes tanto em animais quanto em seres humanos[1]. Em "A agressão", o autor analisa a natureza da agressividade e sua função evolutiva, identificando como impulsos como competição, autopreservação e dominância — que desempenharam papel relevante na sobrevivência da espécie — permanecem presentes no comportamento humano mesmo em ambientes altamente organizados e regulados, como empresas, governos e instituições. O problema, segundo Lorenz, não está na existência desses impulsos, mas na ausência de mecanismos morais suficientemente desenvolvidos para mediá-los em contextos de alta complexidade.

Em "Os oito pecados mortais do homem civilizado",

[1] É necessário registrar que Konrad Lorenz filiou-se ao Partido Nacional-Socialista dos Trabalhadores Alemães (NSDAP) em 1938 e produziu, durante o período nazista, textos que associavam suas teorias etológicas a perspectivas racistas e à política racial do regime — dimensão de sua trajetória que o próprio autor, em declarações posteriores, disse lamentar. Essa circunstância não invalida automaticamente suas contribuições científicas ao campo da etologia, mas exige que seu pensamento seja mobilizado com precisão e consciência crítica. Este artigo utiliza exclusivamente suas análises sobre padrões comportamentais instintivos e sobre o descompasso entre desenvolvimento técnico-intelectual e maturidade moral, descartando qualquer leitura determinista, racista ou eugenista de sua obra. Não deixa de ser historicamente significativo que o pensador que mais claramente teorizou o descompasso entre capacidade intelectual e maturidade ética tenha sido, ele mesmo, um exemplo dessa tensão.

Lorenz aprofunda esse argumento em uma dimensão mais ampla: o desenvolvimento humano não ocorre de maneira equilibrada. Enquanto a capacidade técnica, científica e tecnológica avançou de forma exponencial, a maturidade ética e moral não acompanhou esse ritmo, gerando um perigoso desequilíbrio entre o poder de agir e a sabedoria de agir com responsabilidade. Quanto maior a escala das decisões humanas e o alcance de suas consequências, mais visível e custosa se torna essa defasagem.

No cenário organizacional contemporâneo, esse descompasso se manifesta de formas diversas. A busca incessante por eficiência, inovação e resultados pode conduzir a decisões rápidas, insuficientemente refletidas quanto aos seus impactos sociais, ambientais e humanos. A pressão por desempenho, em culturas corporativas competitivas, tende a sobrepor valores éticos fundamentais, criando condições favoráveis a desvios de conduta. O uso crescente de tecnologias baseadas em algoritmos intensifica esse desafio: sem reflexão ética estruturada, essas ferramentas podem reproduzir vieses, ampliar desigualdades e gerar decisões opacas e de difícil contestação.

Além disso, ao reduzir certos mecanismos naturais de regulação — como os conflitos diretos entre indivíduos —, a civilização não eliminou os impulsos competitivos e agressivos, mas deslocou-os para outras formas de manifestação. No ambiente corporativo, esse processo pode se traduzir em práticas como competição desleal, assédio moral, manipulação de informações ou decisões que privilegiam ganhos de curto prazo em detrimento da sustentabilidade e da integridade organizacional.

As contribuições de Lorenz, portanto, oferecem uma lente valiosa para compreender os fundamentos evolutivos da fragilidade moral humana, ajudando a explicar por que, mesmo em organizações sofisticadas e bem reguladas, desvios éticos persistem — e porque programas de compliance ou de Integridade e estruturas de governança são condição necessária, ainda que insuficiente, para compensar essa defasagem estrutural entre capacidade técnica e maturidade moral.

3.2 Zygmunt Bauman: distância moral e a dissolução da responsabilidade

Se Lorenz situa a fragilidade moral em nossa herança evolutiva, Zygmunt Bauman demonstra como as estruturas da modernidade — em especial a organização burocrática — criam as condições para amplificar essa fragilidade a escalas socialmente destrutivas. "Modernidade e holocausto", Bauman argumenta que as condições que tornaram possível o maior crime coletivo do século XX não constituíram uma aberração da modernidade, mas decorreram de algumas de suas características mais típicas: a especialização funcional, a fragmentação de responsabilidades e o distanciamento entre quem executa uma ação e quem sofre suas consequências.

O conceito central de Bauman para esse processo é o de adiaphorização — a neutralização ética das ações por meio do distanciamento entre o agente e os efeitos de suas decisões. Em estruturas burocráticas altamente especializadas, cada indivíduo é responsável apenas por sua etapa técnica do processo, sem acesso real à dimensão ética do conjunto. A divisão do trabalho, projetada para otimizar a eficiência, funciona simultaneamente como um mecanismo de diluição da responsabilidade moral: ninguém se sente plenamente responsável pelo resultado, porque cada um fez apenas "a sua parte".

No ambiente organizacional, esse mecanismo é recorrente e frequentemente invisível. Casos de manipulação contábil, metas cumpridas por vias irregulares, tolerância ao assédio ou decisões que causam dano ambiental raramente resultam de intenções explicitamente antiéticas de um único agente. Com frequência, são produtos de cadeias decisórias nas quais a responsabilidade se dissolve entre múltiplos atores, cada um agindo dentro de sua função definida, sem que nenhum perceba — ou seja levado a perceber — a dimensão ética do conjunto.

Bauman destaca ainda que a modernidade líquida, ao erodir estruturas estáveis de pertencimento — tradições, comunidades, compromissos duradouros —, deixa os indivíduos mais expostos a pressões imediatas e menos capazes de sustentar posições éticas firmes ao longo do tempo. No ambiente corporativo contemporâneo, marcado por vínculos contratuais fluidos, alta rotatividade e metas trimestrais, essa vulnerabilidade se intensifica, tornando a racionalização de desvios ainda mais provável.

A implicação direta para os Programas de *Compliance* ou de Integridade é significativa: uma organização que distribui normas, coleta assinaturas e registra treinamentos, mas não promove a aproximação entre seus colaboradores e as consequências humanas de suas decisões, reproduz, em escala reduzida, a mesma lógica de neutralização ética que Bauman descreveu. A distância moral não se resolve com mais regras — ela exige que as pessoas sejam expostas, de forma sistemática, às implicações reais de suas escolhas.

3.3 Albert Bandura: os mecanismos do desengajamento moral

Enquanto Bauman examina como as estruturas organizacionais dissolvem a responsabilidade moral, Albert Bandura mapeia os mecanismos psicológicos pelos quais os próprios indivíduos suspendem seus padrões éticos internos sem perceber que o estão fazendo. Em "Moral disengagement", Bandura descreve um conjunto de processos cognitivos que permitem a pessoas com valores morais funcionais participar de comportamentos que, em outras circunstâncias, considerariam inaceitáveis — e, ao fazê-lo, manter a percepção positiva de si mesmas.

O primeiro e mais comum desses mecanismos é a justificação moral, por meio da qual ações prejudiciais são reinterpretadas como eticamente aceitáveis ou necessárias à luz de propósitos superiores: "era pelo bem da empresa", "era o único caminho para manter empregos", "era necessário para competir". O segundo mecanismo é o uso de linguagem eufemística, que suaviza o peso ético das ações ao renomeá-las: "otimização de resultados" no lugar de "fraude", "adequação de processos" no lugar de "supressão de direitos". O deslocamento de responsabilidade transfere a agência moral para a hierarquia ou para o processo — "eu apenas segui as instruções" —, enquanto a difusão de responsabilidade fragmenta a culpa entre tantos participantes que ela se torna imperceptível para cada um individualmente.

Bandura identifica ainda outros mecanismos: a comparação vantajosa — "nossa empresa é muito melhor do que as concorrentes nesse aspecto" —, a desumanização dos afetados — que transforma clientes, colaboradores ou comunidades em categorias abstratas —, a atribuição de culpa às vítimas e a distorção das consequências, minimizando ou negando os danos causados.

Para os programas de compliance ou de Integridade, a teoria tem implicações diretas e urgentes. Políticas, treinamentos informativos e canais de denúncia são insuficientes para neutralizar esses mecanismos, porque eles operam precisamente nas situações de pressão e ambiguidade que os programas pretendem regular. A supressão do desengajamento moral exige intervenções mais profundas: espaços de reflexão ética genuína, aproximação dos colaboradores das consequências reais de suas decisões, responsabilização consistente e liderança que modele, de forma visível, o comportamento esperado. Um programa que trata seus colaboradores como executores de regras e não como agentes morais capazes de julgamento, deixa esses mecanismos operarem livremente — mesmo na presença de estruturas formais de conformidade.

3.4 Joshua Greene: neurociência e os limites do julgamento moral

Joshua Greene oferece uma perspectiva complementar ao situar a fragilidade moral no próprio funcionamento do cérebro humano. Em "Moral Tribes", Greene propõe uma teoria dual do processamento moral, demonstrando empiricamente que as decisões éticas envolvem dois sistemas cognitivos distintos: um sistema automático e intuitivo, que produz respostas emocionais rápidas; e um sistema deliberativo e racional, que opera de forma mais lenta e analítica. Esses dois sistemas não são igualmente acionados em todas as situações — o contexto determina qual deles prevalece, e essa assimetria tem implicações éticas profundas.

O experimento mais célebre utilizado por Greene é o dilema do bonde, que existe em duas versões. Na primeira, uma pessoa pode desviar um bonde descontrolado de cinco pessoas puxando uma alavanca, causando a morte de uma pessoa em outro trilho. A maioria aceita essa escolha, pois o sistema deliberativo avalia as con-

sequências de forma utilitária. Na segunda versão, para salvar as mesmas cinco pessoas, é necessário empurrar fisicamente uma pessoa sobre os trilhos. Mesmo que o resultado seja matematicamente idêntico, a maioria das pessoas recusa — porque o contato físico direto ativa o sistema emocional com intensidade suficiente para bloquear o raciocínio utilitário.

O que Greene demonstra não é que uma resposta é mais correta do que a outra, mas que a moralidade humana é profundamente sensível ao tipo e à proximidade do envolvimento — e que esse sistema pode ser sistematicamente distorcido por contextos artificialmente construídos. Decisões tomadas à distância, mediadas por sistemas automatizados ou por camadas burocráticas, tendem a ativar o sistema deliberativo, mais suscetível a racionalizações utilitaristas. A proximidade emocional com os afetados ativa o sistema intuitivo, que funciona como um freio moral natural.

Essa constatação converge diretamente com a análise de Bauman: o distanciamento entre agente e consequência não é apenas uma condição estrutural da burocracia, é também um fator que suprime os freios morais intuitivos. No contexto organizacional, estruturas que afastam decisores das consequências humanas de suas escolhas — por meio de hierarquias extensas, automação de processos ou gestão por indicadores abstratos — criam condições neurológicas favoráveis ao desvio ético, mesmo sem que ninguém o tenha planejado deliberadamente.

A dimensão tecnológica dessa análise é especialmente relevante: ao delegar decisões moralmente significativas a sistemas de inteligência artificial — como triagem de candidatos, concessão de crédito ou avaliação de desempenho —, as organizações eliminam simultaneamente os dois sistemas de processamento moral humano, substituindo-os por lógica algorítmica que, conforme alertam Lanier (2018) e Bostrom (2014), não possui compreensão ética. A responsabilidade, nesse caso, não desaparece — ela se torna opaca, distribuída e difícil de contestar.

3.5 Hannah Arendt: pensamento, responsabilidade e mediação institucional

As quatro perspectivas anteriores situam a fragilidade moral em dimensões evolutivas, estruturais, psicológicas e neurológicas. Hannah Arendt acrescenta a essas análises uma dimensão filosófica que as transcende e as unifica: a compreensão de que o mal, em sua forma mais comum e perigosa, não resulta de intenção maligna, mas de ausência de pensamento — da recusa ou da incapacidade de exercer julgamento crítico sobre as consequências das próprias ações.

Essa tese foi formulada por Arendt a partir do julgamento de Adolf Eichmann em Jerusalém, em 1961. Eichmann era o funcionário da SS responsável pela logística do transporte de milhões de pessoas para os campos de extermínio. Arendt esperava encontrar um monstro ideológico. O que encontrou foi um homem comum, obediente, eficiente e incapaz de pensar além das categorias do sistema em que operava. Eichmann havia cessado de se perguntar o que estava fazendo, para quem estava fazendo e o que isso significava para os afetados. A esse fenômeno, Arendt deu o nome de "banalidade do mal" — e sua análise permanece uma das contribuições filosóficas mais perturbadoras e relevantes do século XX (Arendt, 1999).

A transposição para o contexto organizacional é direta e inquietante. Instituições que valorizam obediência irrestrita, execução eficiente e conformidade procedural acima do julgamento crítico criam as condições para um equivalente corporativo da banalidade do mal: colaboradores tecnicamente competentes que produzem resultados antiéticos sem má-fé, simplesmente porque nunca foram incentivados a pensar sobre as implicações mais amplas de suas ações. Um analista que aprova uma operação irregular porque "os parâmetros do sistema indicaram aprovação"; um gerente que ignora relatos de assédio porque "o protocolo formal não foi acionado"; um executivo que assina documentos sem lê-los porque "o jurídico já revisou" — todos são, em alguma medida, variações do personagem que Arendt descreveu.

Em "Responsabilidade e julgamento", Arendt argumenta que a responsabilidade ética é pessoal e intransferível — não pode ser delegada à estrutura, ao superior hierárquico ou ao processo. Isso não significa que as instituições sejam irrelevantes: pelo contrário, são elas que criam ou suprimem as condições para que o pensamento crítico

floresça. Organizações que estimulam o questionamento, protegem quem levanta dúvidas, reconhecem a complexidade das decisões e promovem espaços genuínos de reflexão ética estão, na prática, cultivando o antídoto que Arendt prescreveu.

A complementaridade entre Arendt e os demais autores desta seção é reveladora: se Lorenz identifica o descompasso evolutivo, Bauman mostra como as instituições o amplificam estruturalmente, Bandura revela os mecanismos cognitivos de autoabsolvição e Greene demonstra que mesmo nosso funcionamento cerebral é vulnerável a distorções contextuais, Arendt conclui que a saída não está em heróis morais excepcionais, mas em pessoas comuns capazes de pensar — e em instituições que cultivem ativamente essa capacidade.

As cinco perspectivas mobilizadas nesta seção convergem para uma compreensão multidimensional do desvio ético organizacional: ele não é uma anomalia produzida por indivíduos mal-intencionados, mas um produto previsível de condições evolutivas, estruturais, psicológicas, neurológicas e institucionais que, em conjunto, enfraquecem os freios morais e facilitam a racionalização de condutas prejudiciais.

Esse diagnóstico redefine o que se espera de um Programa de Compliance ou de Integridade genuinamente eficaz. Não basta distribuir normas, coletar assinaturas e registrar treinamentos: é necessário atuar sobre as condições que tornam o desvio provável — reduzindo distâncias morais, nomeando mecanismos de auto-justificação, aproximando decisores das consequências de suas escolhas e cultivando ambientes em que o pensamento crítico seja estimulado e protegido. É nesse quadro teórico que o debate sobre tecnologia, tratado na próxima seção, ganha sua dimensão ética mais profunda: se já enfrentamos fragilidades morais estruturais em ambientes humanos convencionais, o que ocorre quando esses ambientes são permeados por sistemas que aceleram decisões, distanciam agentes de consequências e delegam julgamentos a algoritmos?

4. Outros autores que contribuem para o debate ético no âmbito tecnológico

O avanço tecnológico contemporâneo não apenas redefine processos produtivos e relações sociais, mas também impõe novos desafios éticos que exigem reflexão interdisciplinar. Diversos autores, oriundos de campos como ciência, filosofia, sociologia e tecnologia, têm contribuído significativamente para a compreensão dos impactos éticos da inovação. Entre eles, destacam-se Isaac Asimov, Jaron Lanier e Clay Shirky, cujas reflexões permanecem extremamente atuais no contexto da transformação digital.

4.1 Isaac Asimov: tecnologia, personalização e responsabilidade

Isaac Asimov, amplamente reconhecido por suas contribuições à ficção científica e à divulgação científica, antecipou muitos dos dilemas éticos que hoje se materializam com o avanço da inteligência artificial e das tecnologias digitais. Sua obra não apenas imaginou futuros possíveis, mas também propôs reflexões profundas sobre a responsabilidade humana diante da criação tecnológica.

Em entrevista concedida a Bill Moyers em 1988, Asimov defende com entusiasmo a ideia de que a educação será verdadeiramente eficaz quando for personalizada, permitindo que cada pessoa aprenda no seu ritmo e conforme seus interesses. Essa visão, transportada para o contexto contemporâneo, abre uma questão ética relevante: sistemas capazes de adaptar conteúdos e experiências às características individuais podem tanto ampliar a autonomia quanto restringi-la, dependendo da intencionalidade de quem os concebe e opera. A linha entre personalização e manipulação, nesse sentido, não é técnica, e sim ética.

Sistemas de recomendação, plataformas digitais e ferramentas de inteligência artificial utilizam dados comportamentais para personalizar experiências, influenciar decisões e, muitas vezes, direcionar escolhas de consumo, informação e até mesmo opinião. Essa questão sobre

quem controla a intencionalidade por trás dos sistemas que personalizam nossas experiências é precisamente o ponto em que a preocupação de Asimov encontra, décadas depois, um diagnóstico ainda mais incisivo: o de Jaron Lanier, para quem essa disputa já está sendo amplamente perdida pelos indivíduos.

4.2 Jaron Lanier: dependência tecnológica e perda de autonomia

Jaron Lanier, pioneiro da realidade virtual e crítico das grandes plataformas digitais, oferece uma das análises mais contundentes sobre os efeitos sociais e éticos da tecnologia contemporânea. Em algumas de suas obras, Lanier alerta para os riscos associados à crescente dependência de sistemas automatizados e de algoritmos.

Segundo o autor, a automação sem responsabilidade cria sistemas que diminuem nossa autonomia e reduzem nossa capacidade de escolha (Lanier, 2018). Essa crítica está diretamente relacionada ao modelo de negócios de muitas empresas de tecnologia, que utilizam algoritmos para capturar atenção, prever comportamentos e influenciar decisões. Nesse cenário, usuários deixam de ser agentes plenamente conscientes e passam a ser, em certa medida, condicionados por sistemas que operam com base em interesses econômicos.

Lanier também destaca que essa dependência tecnológica pode impactar negativamente aspectos fundamentais da vida social, como a empatia, a construção de identidade e a capacidade crítica. Ao delegarmos decisões a sistemas automatizados, corremos o risco de reduzir o espaço para reflexão ética e julgamento humano.

No contexto organizacional, essa discussão ganha ainda mais relevância. A adoção de inteligência artificial em processos decisórios — como recrutamento, avaliação de desempenho e análise de risco — pode gerar ganhos de eficiência, mas também levanta questionamentos sobre transparência, justiça e responsabilidade.

A contribuição de Lanier, portanto, reforça a necessidade de que a cultura de integridade incorpore limites claros ao uso da automação, garantindo que a tecnologia seja utilizada como ferramenta de apoio, e não como substituta da responsabilidade humana.

4.3 Clay Shirky: excesso de informação e ausência de filtros

Clay Shirky, estudioso das transformações provocadas pela internet e pelas mídias digitais, oferece uma perspectiva complementar ao debate ético contemporâneo. Para o autor, o principal problema da era digital não é o excesso de informação em si, mas a incapacidade coletiva de filtrar, organizar e atribuir sentido a esse volume crescente de dados.

O autor afirma que não estamos enfrentando uma explosão de informação; estamos enfrentando uma falha coletiva em construir novos filtros para dar sentido a ela (Shirky, 2010).

Essa análise é particularmente relevante em um contexto marcado pela disseminação de notícias falsas (*fake news*) e conteúdos manipulados. A ausência de filtros eficazes compromete a qualidade das decisões, tanto no âmbito individual quanto organizacional.

Para as organizações, esse cenário representa um desafio ético significativo. A tomada de decisão baseada em informações incompletas, enviesadas ou incorretas pode levar a erros estratégicos, danos reputacionais e impactos sociais negativos. Além disso, a pressão por velocidade — característica do ambiente digital — tende a priorizar respostas rápidas em detrimento de análises mais aprofundadas e responsáveis.

Shirky também chama atenção para o papel das plataformas digitais na mediação da informação. Algoritmos que priorizam engajamento em vez de qualidade podem amplificar conteúdos sensacionalistas ou polarizadores, contribuindo para a deterioração do debate público e para a fragmentação social.

Nesse contexto, a cultura de integridade deve incluir não apenas práticas de governança da informação, mas também o desenvolvimento de competências críticas nos indivíduos, permitindo que sejam capazes de avaliar a confiabilidade e a relevância das informações com as quais interagem.

As contribuições de Asimov, Lanier e Shirky convergem para um ponto central: os desafios éticos da tecnologia não decorrem apenas de sua complexidade técnica, mas, sobretudo, de suas implicações humanas, sociais e organizacionais.

Enquanto Asimov alerta para o potencial ambivalente da personalização tecnológica, Lanier evidencia os riscos da perda de autonomia diante da automação, e Shirky destaca os impactos da desordem informacional. Em conjunto, esses autores oferecem uma visão abrangente dos dilemas contemporâneos, reforçando a necessidade de uma abordagem ética integrada.

Para as organizações, isso implica reconhecer que a cultura de integridade deve evoluir no mesmo ritmo das transformações tecnológicas. Não se trata apenas de cumprir normas ou evitar riscos, mas de construir uma postura ética proativa, capaz de orientar decisões em ambientes complexos, incertos e altamente conectados.

5. Respeito, bom senso e ética como fundamentos da integridade

O respeito e o bom senso constituem pilares essenciais para a construção de uma cultura de integridade consistente e sustentável nas organizações. Mais do que conceitos abstratos, esses elementos orientam comportamentos concretos e decisões cotidianas, influenciando diretamente a forma como indivíduos se relacionam entre si e com a própria instituição. A ética, nesse contexto, não se limita ao cumprimento de normas, mas envolve a capacidade de julgamento equilibrado diante de situações complexas e, muitas vezes, ambíguas.

A reflexão clássica de Aristóteles, especialmente em "Ética a Nicômaco", permanece extremamente atual ao afirmar que a virtude está no "justo meio", ou seja, no equilíbrio entre extremos. Essa ideia pode ser diretamente aplicada ao ambiente organizacional, no qual decisões frequentemente exigem a conciliação entre diferentes interesses — como desempenho e responsabilidade, inovação e prudência, resultado e impacto social. O bom senso, nesse cenário, atua como a capacidade prática de encontrar esse equilíbrio, orientando escolhas que não apenas atendam aos objetivos institucionais, mas que também respeitem princípios éticos fundamentais.

A integridade, por sua vez, não deve ser compreendida como a ausência absoluta de falhas ou desvios, o que seria irrealista em qualquer contexto humano. Pelo contrário, ela se manifesta na forma como indivíduos e organizações lidam com erros, riscos e dilemas. Uma organização íntegra é aquela capaz de reconhecer vulnerabilidades, identificar riscos de conduta, corrigir desvios com responsabilidade e agir com transparência diante de suas decisões. Isso implica também considerar, de maneira contínua, os impactos de suas ações sobre pessoas, comunidades e sociedade como um todo.

Nesse sentido, o respeito assume um papel central. Ele se traduz na valorização do outro como sujeito de direitos, na escuta ativa, na consideração de diferentes perspectivas e na construção de ambientes seguros e inclusivos. Organizações que cultivam o respeito tendem a desenvolver relações mais saudáveis, maior confiança interna e maior engajamento de seus colaboradores — fatores que fortalecem a própria cultura de integridade.

Entretanto, um dos principais desafios contemporâneos está na distância entre discurso e prática. Muitas organizações possuem códigos de ética, políticas e diretrizes bem estruturadas, mas não conseguem efetivamente incorporar esses princípios no dia a dia. A ética, quando restrita a documentos formais, perde sua força transformadora. Para que a cultura de integridade seja efetiva, ela precisa ser vivida nas interações cotidianas, refletida nas decisões da liderança e percebida nas práticas organizacionais.

Isso exige coerência — um dos elementos mais críticos da integridade. A coerência entre o que se diz e o que se faz é o que sustenta a credibilidade institucional. Quando líderes e gestores demonstram, por meio de suas ações, compromisso genuíno com valores éticos, eles estabelecem referências claras para toda a organização. Por outro lado, incoerências, mesmo que pontuais, podem comprometer rapidamente a confiança construída ao longo do tempo.

Além disso, o desenvolvimento de uma cultura ética baseada em respeito e bom senso demanda investimento

contínuo em educação, comunicação e reflexão. Treinamentos, diálogos abertos sobre dilemas éticos e espaços de escuta são fundamentais para fortalecer a capacidade de crítica dos indivíduos e prepará-los para lidar com situações complexas.

O respeito e o bom senso não são apenas complementos da ética organizacional, mas seus fundamentos mais essenciais. São eles que permitem transformar princípios abstratos em práticas concretas, sustentando uma cultura de integridade que vai além da conformidade e se consolida como elemento estruturante das relações e decisões organizacionais.

Conclusão

A análise dos desafios contemporâneos à cultura de integridade evidencia que as organizações estão inseridas em um ambiente cada vez mais complexo, dinâmico e marcado por tensões éticas constantes. Ao longo deste artigo, buscou-se compreender como transformações tecnológicas, sociais e organizacionais impactam diretamente a forma como decisões são tomadas e como valores são vivenciados no cotidiano corporativo. Nesse sentido, o objetivo proposto — de analisar esses desafios à luz de diferentes referenciais teóricos — permite concluir que a integridade deixou de ser apenas um ideal normativo para se consolidar como um elemento estratégico e indispensável à sustentabilidade das organizações.

A partir da fundamentação teórica, foi possível compreender que moral, ética e cultura são dimensões interdependentes. Enquanto a moral orienta comportamentos socialmente aceitos, a ética promove a reflexão crítica sobre esses padrões, e a cultura organiza e perpetua esses valores no contexto coletivo. Autores como Edgar Schein demonstram que a cultura organizacional influencia profundamente as decisões e práticas, muitas vezes de forma inconsciente, reforçando a importância de se construir ambientes em que a integridade seja efetivamente vivida e não apenas formalizada.

No campo dos desafios contemporâneos, observou-se que a transformação digital e o uso intensivo de dados ampliaram significativamente o poder das organizações, mas também os riscos associados à privacidade, à transparência e à responsabilidade. Nesse contexto, reflexões como as de Shoshana Zuboff evidenciam como a exploração de dados pode comprometer a autonomia dos indivíduos, exigindo novas formas de governança ética. De forma complementar, o avanço da inteligência artificial intensifica esses dilemas, conforme alerta Jaron Lanier, ao destacar os riscos da automação sem responsabilidade e da perda de controle humano sobre decisões relevantes.

Além disso, questões como diversidade, inclusão, agenda ESG e novas formas de trabalho demonstram que a ética organizacional não pode mais ser analisada de forma isolada ou restrita a normas internas. Trata-se de um fenômeno que envolve relações humanas, impactos sociais e expectativas crescentes por parte de diferentes *stakeholders*. Autores como Amartya Sen contribuem ao reforçar a importância da equidade e da justiça como fundamentos para organizações mais responsáveis e inclusivas.

A análise desenvolvida na seção "Da fragilidade moral à racionalização do desvio: fundamentos teóricos para o debate ético nas organizações" aprofunda essa compreensão ao revelar que o desvio ético organizacional não é uma anomalia produzida por indivíduos mal-intencionados, mas um produto previsível de condições que atuam em múltiplas dimensões simultaneamente. Konrad Lorenz situa o problema em nossa herança evolutiva, identificando o descompasso entre capacidade técnica e maturidade moral como uma fragilidade estrutural da condição humana. Zygmunt Bauman demonstra como estruturas burocráticas amplificam essa fragilidade ao dissolver a responsabilidade individual por meio da especialização e do distanciamento. Albert Bandura nomeia os mecanismos psicológicos pelos quais indivíduos moralmente funcionais suspendem seus próprios padrões éticos sem perceber que o fazem. Joshua Greene revela que o julgamento moral é biologicamente sensível ao contexto e à proximidade, podendo ser distorcido por arranjos organizacionais que afastam decisores das consequências humanas de suas escolhas. E Hannah Arendt conclui que o antídoto não está em regulamentos mais rígidos, mas no cultivo ativo da capacidade de pensar — e em instituições que criem as condições para que esse pensamento floresça. Juntas, essas perspectivas reforçam que os desafios éticos contemporâneos não são apenas tecnológicos, mas essencialmente humanos, es-

truturais e cognitivos. Autores como Isaac Asimov, Jaron Lanier e Clay Shirky ampliam essa discussão ao abordar os impactos da tecnologia sobre autonomia, comportamento e construção da realidade. Suas contribuições convergem ao indicar que, diante de sistemas cada vez mais complexos e invasivos, torna-se indispensável o desenvolvimento de filtros éticos, limites claros e mecanismos que preservem a centralidade do humano nas decisões.

Por fim, a reflexão sobre respeito, bom senso e ética como fundamentos da integridade evidencia que, apesar da sofisticação dos desafios contemporâneos, as bases da conduta ética permanecem ancoradas em princípios fundamentais. Inspirado em Aristóteles, o equilíbrio entre interesses, a coerência entre discurso e prática e a capacidade de considerar o impacto das decisões sobre o outro são elementos essenciais para a construção de uma cultura de integridade sólida.

Conclui-se, portanto, que enfrentar os desafios contemporâneos à cultura de integridade exige uma abordagem integrada, que combine governança, tecnologia e, sobretudo, desenvolvimento humano. Mais do que implementar normas ou controles, é necessário promover uma transformação cultural que valorize a ética como prática cotidiana. Em um cenário marcado pela velocidade, pela complexidade e pela incerteza, a integridade se afirma não apenas como um diferencial competitivo, mas como condição essencial para a legitimidade, a confiança e a perenidade das organizações.

Referências

ARISTÓTELES. *Nicomachean Ethics*. Tradução de William David Ross. Oxford: Oxford University Press, 1925.

ARENDT, Hannah. *Responsabilidade e Julgamento*. São Paulo: Companhia das Letras, 2004.

ARENDT, Hannah. *Eichmann em Jerusalém:* um relato sobre a banalidade do mal. São Paulo: Companhia das Letras, 1999.

ISAAC ASIMOV WORLD OF IDEAS #2 SUBTITULADO. [S. l.]: S. Sacasqui, 2018. 1 vídeo (27 min 15 seg.). Disponível em: https://www.youtube.com/watch?v=dobBf6jBhBE. Acesso em: 19 maio 2026.

BANDURA, Albert. *Moral Disengagement:* How People Do Harm and Live with Themselves. New York: Worth Publishers, 2016.

BAUMAN, Zygmunt. *Modernidade e Holocausto*. Tradução de Marcus Penchel. Rio de Janeiro: Zahar, 1998.

BENNIS, Warren. *On Becoming a Leader*. New York: Basic Books, 2009.

BRASIL. Lei nº 12.846, de 1º de agosto de 2013. Dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira, e dá outras providências. *Diário Oficial da União*: seção 1, Brasília, DF, 2 ago. 2013.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). *Diário Oficial da União*: seção 1, Brasília, DF, 15 ago. 2018.

DURKHEIM, Émile. *A educação moral*. São Paulo: Edipro, 2018.

DURKHEIM, Émile. *Educação e Sociologia*. Rio de Janeiro: Vozes, 2014.

EUROPEAN UNION. *Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016*. General Data Protection Regulation (GDPR). Disponível em: https://eur-lex.europa.eu/eli/reg/2016/679/oj. Acesso em: 19 maio 2026.

FLORIDI, Luciano. *The Ethics of Information*. Oxford: Oxford University Press, 2015.

GREENE, *Joshua. Moral Tribes:* Emotion, Reason, and the Gap Between Us and Them. New York: Penguin Books, 2013.

HARARI, Yuval Noah. *Homo Deus:* Uma Breve História do Amanhã. São Paulo: Companhia das Letras, 2016.

KANT, Immanuel. *Fundamentação da Metafísica dos Costumes.* Alemanha: F. Nicolovius, 1797.

LANIER, Jaron. *Ten Arguments for Deleting Your Social Media Accounts Right Now*. New York: Henry Holt and Company, 2018.

LARAIA, Roque de Barros. *Cultura:* um conceito antropológico. Rio de Janeiro: Zahar, 2000.

LORENZ, Konrad. *A Agressão:* uma história natural do mal. Portugal: Relógio D'Água Editores, 2001.

LORENZ, Konrad. *Os Oito Pecados Mortais do Homem Civilizado*. São Paulo: Editora Brasiliense, 1988.

MCLEAN, Bethany; ELKIND, Peter. *The Smartest Guys in the Room*: The Amazing Rise and Scandalous *Fall of Enron*. New York: Penguin, 2013.

MILL, John Stuart. *Utilitarismo*. São Paulo: Iluminuras, 2020.

MORIN, Edgar. *Ética Cultura e Educação*. São Paulo: Cortez, 2011.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD). *OECD Principles on Artificial Intelligence*. Paris: OECD Publishing, 2019.

SANTOS, José Luiz dos. *O que é cultura*. São Paulo: Brasiliense, 1949.

SCHEIN, Edgar. *Cultura Organizacional e Liderança*. 5. ed. São Paulo: GEN Atlas, 2022.

SEN, Amartya. *The Idea of Justice*. Cambridge: Harvard University Press, 2009.

SENNETT, Richard. *Together:* The Rituals, Pleasures and Politics of Cooperation. London: Allen Lane, 2012.

SHIRKY, Clay. *Cognitive Surplus:* Creativity and Generosity in a Connected Age. New York: Penguin Books, 2010.

UNITED NATIONS. *Transforming our World:* The 2030 Agenda for Sustainable Development. New York: United Nations, 2015.

VÁZQUEZ, Adolfo Sánchez. *Ética*. Rio de Janeiro: Civilização Brasileira, 2017.

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

Cultura de integridade:

como transformar códigos em comportamento

Desirée Ulsen Ferreira

Desirée Ulsen Ferreira é formada em Administração de Empresas, com MBA em Gestão de Pessoas e MBA em Petróleo & Gás pela UFRJ/COPPE, além de especializações em Compliance e Governança.

Possui mais de 20 anos de experiência nas áreas de Governança, Compliance, Auditoria, Gestão de Processos e Planejamento Estratégico, com atuação nos setores de energia, tecnologia e serviços financeiros.

Construiu sua trajetória profissional em empresas do segmento de energia, tecnologia e serviços financeiros. Desde 2015 atua na PETRONECT, liderando iniciativas relacionadas a compliance, auditoria, governança, processos, riscos e segurança da Informação.

Maria Claudia Pedroso

Maria Claudia Pedroso é advogada, com MBA em Direito Eletrônico pela Escola Paulista de Direito e pós-graduações em Direito Ambiental, Gestão Ambiental e Direito do Trabalho, além de certificação EXIN – LGPD (PDPE).

Possui mais de 20 anos de experiência, com atuação jurídica generalista, consultiva e contenciosa em empresas de grande e médio porte. Possui sólida experiência em contratos, licitações, proteção de dados pessoais, estruturação e gestão de área jurídica, auditorias e interlocução com órgãos de controle.

Desde 2022, integra o escritório Volia Bomfim, com consultoria jurídica trabalhista, revisão de contratos e documentos, Visual Law, palestras e adequação de processos à regulamentação de dados pessoais.

Bianca Helena dos Santos

Bianca Helena dos Santos é advogada, especialista em Gestão em ESG (Ambiental, Social e Governança) e atualmente cursa o MBA em Gestão e Business Law da FGV.

Possui experiência nas áreas Jurídica e de Governança Corporativa, com atuação em temas societários, contratos, propriedade intelectual, privacidade e proteção de dados, além de iniciativas de inovação e melhoria de processos.

Atua na PETRONECT desde 2021 e, atualmente, é Coordenadora de Governança, com atuação em temas estratégicos e societários da c-ompanhia e no suporte aos órgãos de governança.

1. Da maturidade formal à efetividade cultural

A análise do grau de maturidade dos programas de compliance e integridade nas empresas brasileiras, especialmente a partir de 2020, revela um cenário de evolução progressiva, porém assimétrica, com diferenças relacionadas aos setores de atuação, às estruturas de governança e à capacidade de integração do compliance às práticas de gestão das organizações.

Dados recentes da KPMG (2024)[1] indicam que o nível médio de maturidade do compliance no Brasil situa-se em 3,09 em uma escala de 1 a 5, o que denota um estágio intermediário de desenvolvimento, representando o maior índice apurado desde o início da série, em 2015, e supera resultado de 3,07 registrado em 2021.

A pesquisa avalia a maturidade a partir de nove pilares: governança e cultura; avaliação de riscos; pessoas e estrutura; políticas e procedimentos; comunicação e treinamento; tecnologia e análise de dados; monitoramento e testes; investigações e linha ética; e reporte. Entre os aspectos que mais contribuíram para o resultado médio de 2024 estão investigações e linha ética (3,3), políticas e procedimentos (3,2), governança e cultura (3,1) e reporte (3,1).

Sob a perspectiva setorial, os resultados demonstram diferenças no nível de maturidade. O setor de Serviços Financeiros apresentou o maior índice, de 3,5, seguido por Governo e Infraestrutura, com 3,3; Tecnologia, Mídia e Telecomunicações, com 3,1; Mercados Industriais, com 3,0; e Consumo e Varejo, com 2,9. Esses resultados evidenciam que o desenvolvimento dos programas de compliance não ocorre de maneira uniforme entre as organizações.

Importa destacar, contudo, que a pesquisa não estabelece uma correlação direta entre o porte das empresas e as faixas específicas de maturidade. A amostra foi composta por 106 organizações, das quais 55% possuem receita anual superior a R$ 1 bilhão, 22% apresentam faturamento entre R$ 300 milhões e R$ 1 bilhão, e 23% possuem receita de até R$ 300 milhões. Dessa forma, os resultados não permitem afirmar, com base nesse levantamento, que pequenas, médias e grandes empresas correspondam, respectivamente, a níveis predeterminados de maturidade.

Os dados da KPMG revelam, por outro lado, relevante grau de formalização dos programas avaliados. Segundo a pesquisa, 97% das organizações informaram possuir Código de Ética e Conduta com referência a aspectos regulatórios e de compliance, 92% disponibilizam canal de denúncias aos públicos interno e externo e 84% possuem protocolos e metodologia para investigação das denúncias recebidas. Além disso, 77% afirmaram que as políticas e controles de compliance influenciam a conduta de colaboradores e terceiros.

Esse elevado grau de formalização, contudo, não significa que os programas estejam integralmente incorporados à estratégia e à gestão das organizações. A própria pesquisa identifica oportunidades relevantes de aprimoramento, especialmente no gerenciamento de riscos de terceiros, na adaptação aos riscos emergentes e ao dinamismo regulatório, na integração do compliance às práticas de gestão de desempenho e na construção de uma agenda estratégica para a função.

Em ambientes mais complexos, o risco está na fragmentação entre áreas, no excesso de formalismo, na burocratização do compliance e na dificuldade de fazer com que a integridade influencie, de fato, toda a cadeia hierárquica e todas as decisões relevantes do negócio.

Essa dificuldade de integração também pode ser observada nos indicadores relacionados à gestão de desempenho. Embora haja elevado nível de implementação de políticas e controles, 56% das organizações pesquisadas informaram não utilizar metas de compliance como indicadores de avaliação de desempenho, enquanto apenas 25% declararam aplicá-las a todos os colaboradores, executivos e terceiros.

Em grande parte das organizações, a integridade já está formalmente estabelecida. Códigos de ética são publicados, políticas são aprovadas e treinamentos são realizados.

[1] https://kpmg.com/br/pt/insights/2024/10/pesquisa-maturidade-compliance-brasil-6-edicao.html

No entanto, seja qual for o setor, a estrutura ou o grau de maturidade da empresa, existe um desafio, transversal: a distância entre o que está escrito e o que efetivamente orienta as decisões do dia a dia. Em outras palavras, o problema não está necessariamente na inexistência de regras, mas na dificuldade de transformá-las em comportamento e integrá-las aos processos de gestão e tomada de decisão.

O comportamento organizacional não é meramente individual ou racional, mas profundamente condicionado por estruturas culturais, muitas vezes invisíveis, internalizadas e reforçadas socialmente.

É exatamente aqui que a discussão deixa de ser sobre a existência do programa e passa a ser sobre sua efetividade, uma vez que não basta perguntar se a organização tem código, é preciso perguntar se o código altera a forma como a organização decide, recompensa, tolera e corrige.

Para Clóvis de Barros Filho, cultura não se reduz a normas formais ou discursos institucionais. Trata-se de um conjunto de significados, valores e referências simbólicas que orientam a percepção do que é "adequado", "esperado" ou "valioso" dentro de um grupo.

No ambiente corporativo, isso significa que a cultura organizacional define o que é considerado sucesso, erro, mérito ou desvio e atua como uma espécie de "filtro invisível" que orienta decisões e julgamentos cotidianos. E, diga-se de passagem, que, muitas vezes, não está escrita, mas é amplamente compreendida pelos membros da organização. É justamente por isso que a cultura real da empresa nem sempre coincide com a cultura declarada em seus documentos institucionais.

O ilustríssimo filósofo nos ensina[2] que cultura é o sistema simbólico que orienta o sentido das ações e o comportamento é a expressão concreta desse sistema. E, portanto, a coerência entre ambos é condição para a efetividade organizacional.

Portanto, a cultura de integridade se manifesta não nos documentos institucionais, mas no comportamento. Imaginemos, como exemplo, a forma como decisões são tomadas diante de situações concretas, especialmente quando há pressão por resultados, ambiguidade ou conflito de interesses, pois é nesses ambientes de pressão que se verifica se a integridade é um valor operacional ou apenas um valor declaratório. Programas eficazes dependem de práticas integradas ao negócio, e não apenas de instrumentos formais aprovados internamente.

Assim, mais do que um conjunto de diretrizes, a integridade está diretamente relacionada à consciência individual perante determinada coletividade. Mas essa consciência individual não nasce espontaneamente, ela é moldada pelo ambiente, pelos exemplos, pelos incentivos, pelos medos, pelas permissões e pelas consequências que a organização constrói.

O primeiro elemento estruturante dessa cultura é o comprometimento da alta liderança. O chamado *tone at the top*, amplamente reconhecido em referenciais de integridade, traduz-se na coerência entre discurso e prática.

Quando líderes tomam decisões alinhadas a princípios éticos, mesmo diante de perdas financeiras ou operacionais, estabelecem um padrão claro para toda a organização. Por outro lado, qualquer desalinhamento nesse nível compromete a credibilidade de todo o programa.

Na prática, a liderança exerce influência contínua, em todas as decisões do dia a dia. Não se trata apenas de diretrizes formais, mas de micro comportamentos como conflitos são resolvidos, metas são cobradas e desvios são tratados.

A confiança na liderança é um fator determinante para a consolidação da cultura. Se o líder não acredita ou não pratica os valores que comunica, dificilmente a organização os incorporará. Nesse contexto, reforça-se a premissa de que não é apenas o resultado que importa, mas a forma como ele é alcançado.

No entanto, a liderança, por si só, não é suficiente. A cultura organizacional é um segundo elemento dessa estrutura sendo profundamente influenciada pelos incentivos e pelas consequências existentes. Organizações que valorizam exclusivamente resultados quantitativos, sem considerar a forma como são alcançados, tendem a criar ambientes propícios a desvios.

Por isso, boas práticas de integridade recomendam a incorporação de critérios éticos em avaliações de desempenho, bem como a aplicação consistente de medidas

[2] "BARROS FILHO, Clóvis de. *Happy hour é na segunda:* porque na sexta fica tarde demais. Porto Alegre: Citadel Grupo Editorial, 2025.

disciplinares, independentemente do nível hierárquico, salvaguardada a prática de comunicação proporcional e adequada, preservando a confidencialidade.

A existência de *accountability* clara e efetiva é essencial. Isso inclui a aplicação de sanções disciplinares quando necessário, mas também o reconhecimento de comportamentos alinhados aos valores organizacionais.

A consistência nesse processo reforça a percepção de justiça e fortalece a confiança interna. Quando as regras são aplicadas de forma igual para todos, a cultura deixa de ser apenas declarada e passa a ser efetivamente vivida.

Outro fator crítico é a forma como as regras são comunicadas. Linguagem excessivamente técnica ou jurídica dificulta a compreensão e reduz o engajamento. Treinamento eficaz, portanto, não é mera transmissão de norma, é tradução de critérios de decisão. A boa comunicação em integridade não serve apenas para informar políticas, mas para orientar condutas em situações ambíguas.

A experiência prática demonstra que iniciativas baseadas em situações reais, como dilemas cotidianos enfrentados por colaboradores, são mais eficazes para internalizar valores. Em vez de apenas informar o que não pode ser feito, essas abordagens ajudam a orientar decisões concretas.

Nesse contexto, diversas organizações têm adotado práticas inovadoras para aproximar a integridade da realidade dos colaboradores. Programas de *onboarding* estruturados, por exemplo, são utilizados para inserir desde o início os valores organizacionais, muitas vezes por meio de iniciativas específicas voltadas à cultura, como jornadas de integração que abordam ética e comportamento esperado de forma prática.

Outras iniciativas incluem a criação de redes de "embaixadores de compliance" ou de valores, nas quais colaboradores com perfil de liderança atuam como multiplicadores da cultura nas áreas de negócio.

Da mesma forma, rodas de conversa e espaços de diálogo aberto têm se mostrado eficazes para discutir dilemas éticos reais, promovendo reflexão e engajamento coletivo.

Treinamentos também precisam evoluir. Modelos tradicionais, centrados na transmissão passiva de conteúdo, têm impacto limitado na mudança de comportamento.

Em contraste, abordagens baseadas em casos práticos, *storytelling* e até mesmo personagens que representem situações de integridade no cotidiano tornam o aprendizado mais acessível e aplicável. Essas iniciativas contribuem para que os colaboradores se identifiquem com os temas e incorporem os valores no dia a dia.

A existência de canais de denúncia confiáveis é outro pilar essencial. A legislação e as orientações dos órgãos de controle reforçam a importância de mecanismos que permitam o relato de irregularidades com segurança e confidencialidade.

Mas o ponto central não é a existência do canal, mas sim a confiança na ferramenta. Um canal só fortalece a cultura quando as pessoas acreditam que podem falar sem sofrer retaliação, que sua manifestação será tratada com seriedade e que haverá apuração, resposta e consequência.

Entretanto, mais do que disponibilizar o canal, é fundamental garantir a proteção contra retaliações e demonstrar, na prática, que as manifestações são tratadas com seriedade, com apuração adequada e prestação de contas sobre as medidas adotadas.

Adicionalmente, programas de integridade mais maduros têm em comum a integração com o negócio. O compliance deixa de atuar apenas como instância de controle e passa a participar das decisões, contribuindo para a identificação e mitigação de riscos de forma preventiva.

Essa atuação integrada é especialmente relevante em ambientes complexos, marcados pela transformação digital, pela diversidade geracional e pela crescente exigência de transparência.

A adaptação das práticas à realidade de cada organização também é um fator determinante. Programas eficazes são proporcionais ao porte, ao setor de atuação e aos riscos envolvidos.

Iniciativas como *due diligence* de integridade em contratações, controle de brindes e hospitalidades e critérios de integridade em processos de seleção e avaliação de parceiros são exemplos de práticas que podem ser ajustadas conforme o contexto organizacional.

Referenciais nacionais e internacionais, incluindo orientações de órgãos de controle e da norma ISO 37001, reforçam a importância da cultura para a efetividade dos sistemas de integridade. A ISO 37001:2025 estabelece, especificamente, que a cultura antissuborno deve ser desenvolvida, mantida e promovida em todos os níveis da organização e que o comprometimento da governança,

da alta direção e da gestão deve ser ativo, visível, consistente e sustentado.

Isso significa que ações pontuais não são suficientes, é necessário um esforço contínuo, com iniciativas permanentes, monitoramento e evolução constante. Essa compreensão da cultura como elemento determinante para a efetividade dos programas de integridade também vem sendo incorporada de forma cada vez mais explícita aos referenciais internacionais. A ISO 37001:2025, em sua versão mais recente, deu um passo relevante nesse sentido ao passar a tratar expressamente a cultura antissuborno como requisito específico do sistema de gestão. Mais do que recomendar a existência de políticas, controles e procedimentos, a norma reforça a responsabilidade da governança, da alta direção e dos demais níveis de gestão na construção de um ambiente em que o comportamento esperado seja compreendido, estimulado e efetivamente praticado. Ao exigir que essa cultura seja desenvolvida, mantida e promovida em todos os níveis da organização, a norma aproxima os requisitos formais da realidade cotidiana da organização, reforçando a coerência entre o que a organização estabelece, o que suas lideranças demonstram e aquilo que as pessoas percebem como verdadeiramente valorizado ou tolerado no dia a dia. A mudança é especialmente significativa porque reconhece algo essencial: controles podem reduzir a exposição a riscos e a ocorrência de desvios, mas é a cultura que influencia a decisão quando nenhuma regra é capaz de antecipar todas as situações.

Se a cultura precisa ser desenvolvida e sustentada, ela também precisa ser observada. Indicadores como participação em treinamentos, utilização de canais de denúncia, percepção dos colaboradores e aderência a práticas éticas fornecem insumos relevantes para ajustes e melhorias. Trata-se de um processo dinâmico, que deve evoluir na mesma velocidade em que evoluem as organizações e o ambiente de negócios.

Diante desse cenário, torna-se evidente que a integridade não se consolida por meio de documentos, mas por meio de práticas consistentes. Organizações que conseguem alinhar liderança, incentivos, comunicação e mecanismos de controle criam ambientes em que fazer o certo deixa de ser uma exceção e passa a ser o padrão esperado.

Como incialmente dito, cultura não é o que está formalizado, mas o que é efetivamente praticado. É comportamento. É o que se observa nas pessoas, nas decisões cotidianas e na forma como a organização responde a desafios. E é nesse espaço, entre a regra e a decisão, que a integridade se constrói.

A seguir, ilustramos de forma resumida o que falamos até aqui em um modelo mental.

2. Boas práticas para fortalecer a cultura de integridade

Para apoiar a implementação e adaptação da cultura de integridade nas organizações, destacam-se algumas práticas aplicáveis a diferentes contextos empresariais:

- *Onboarding* com foco em integridade: significa incluir, desde a entrada do colaborador, conteúdos práticos baseados em situações reais da empresa, demonstrando como os valores se traduzem em decisões do dia a dia.
- "Embaixadores de integridade ou compliance": nos quais são selecionados determinados colaboradores com perfil de liderança e influência para atuar como multiplicadores da cultura, promovendo diálogo e apoio nas áreas de negócio.
- Rodas de conversa e dilemas éticos: espaços que constituam momentos efetivos e, se possível, espaços de diálogo aberto e periódicos, nos quais são discutidas situações reais, incentivando o pensamento crítico e a troca de experiências entre equipes.
- Integração com avaliação de desempenho: isto é, critérios de integridade são incorporados nas metas e avaliações, inclusive conectando-os a indicadores ESG, para alinhar comportamento e incentivos.
- Gestão de terceiros com foco em integridade: por meio de verdadeira atuação de parceria entre fornecedores e parceiros, revelada, inclusive, nas cláusulas contratuais que reforçam os padrões éticos esperados entre as partes, sem contar a inclusão de previsão de *due dilligence* de forma positiva e agregadora.
- Controles claros para temas sensíveis: com a prática de instituir regras simples e transparentes, com critérios bem definidos, para registro e recebimento de brindes, hospitalidades e conflitos de interesse.
- Canais de denúncia confiáveis e efetivos: nos quais haja garantia efetiva da aplicação de mecanismos seguros, com proteção contra retaliações e tratamento adequado das manifestações, reforçando a confiança no sistema.
- *Accountability* consistente: com a aplicação de medidas disciplinares de forma proporcional e uniforme, independentemente do nível hierárquico, fortalecendo a percepção de justiça, com ampla divulgação dessas medidas para toda a comunidade corporativa.
- Liderança ativa e exemplar: na qual se evidencie o comportamento incorporado à integridade nas decisões cotidianas, demonstrando, na prática, que "como" se alcança o resultado é tão importante quanto o resultado em si.

Entendemos que a efetividade dessas práticas depende de sua aplicação contínua, visível e integrada à estratégia do negócio, transformando a integridade de um princípio formal em um comportamento organizacional consistente.

A seguir, listamos alguns exemplos práticos e cotidianos dos erros mais comuns e as respectivas oportunidades de melhoria comportamental, a ponto de se tornarem, quem sabe, boas práticas na sua empresa.

3. *Checklist* prático para implementação da cultura de integridade – empresas de pequeno e médio porte

1. **Comece pelo básico (sem complexidade)**
   - Elaborar um código de conduta simples, claro e acessível
   - Comunicar diretamente aos colaboradores (reuniões, vídeos curtos ou conversas)
   - Garantir que todos compreendam as regras principais
2. **Liderança como exemplo**
   - Alinhar sócios e gestores sobre a importância da integridade
   - Demonstrar coerência nas decisões do dia a dia
   - Evitar "atalhos" mesmo sob pressão por resultados
3. **Treinamentos simples e frequentes**
   - Realizar conversas curtas sobre ética em reuniões de equipe
   - Discutir situações reais vividas pela empresa
   - Evitar treinamentos complexos ou excessivamente técnicos
4. **Regras claras para situações sensíveis**
   - Definir diretrizes básicas para: brindes e hospitalidades, conflitos de interesse, relacionamento com fornecedores e clientes
   - Registrar decisões relevantes, mesmo que de forma simples
5. **Canal de escuta acessível**
   - Disponibilizar um meio simples para relato de situações (formulário ou canal interno)
   - Garantir confidencialidade e ausência de retaliação
   - Tratar todos os relatos com seriedade
6. **Critérios justos e consistentes**
   - Aplicar regras igualmente para todos
   - Evitar favorecimentos pessoais
   - Adotar medidas corretivas quando necessário
7. **Cuidado na escolha de parceiros**
   - Avaliar reputação básica de fornecedores e parceiros
   - Formalizar acordos com cláusulas simples de integridade
   - Evitar relações com histórico de irregularidades
8. **Integridade no dia a dia**
   - Inserir o tema em decisões operacionais
   - Incentivar dúvidas e discussões sobre o que é "certo a fazer"
   - Reforçar constantemente os valores da empresa
9. **Evolução contínua (passo a passo)**
   - Revisar práticas periodicamente
   - Ajustar conforme crescimento da empresa
   - Implementar melhorias de forma gradual

4. O alto custo da baixa maturidade

Falar em maturidade de compliance pode, à primeira vista, soar como tema técnico demais. Mas, na prática, a pergunta é bastante simples: o que a empresa arrisca quando sua integridade não amadurece? A resposta também é simples, embora desconfortável: arrisca mais do que multas. Arrisca reputação, confiança, contratos, relações comerciais, acesso a oportunidades e, em casos mais graves, a própria continuidade de certas operações.

A baixa maturidade não significa apenas ausência de sofisticação, muitas vezes ela revela fragilidade estrutural justamente nos aspectos em que a empresa mais precisa de previsibilidade: na forma de decidir, prevenir, reagir e responder.

O primeiro grupo de riscos é o mais visível: o risco jurídico. No Brasil, a Lei nº 12.846/2013 prevê a responsabilização objetiva administrativa e civil de pessoas jurídicas pela prática de atos lesivos contra a administração pública. Na esfera administrativa, as sanções incluem multa de

0,1% a 20% do faturamento bruto do último exercício anterior ao da instauração do processo, nunca inferior à vantagem auferida quando estimável, além da publicação extraordinária da decisão condenatória.

Na esfera civil, as consequências podem alcançar perda de bens, suspensão de atividades, fechamento da empresa e proibição de receber incentivos do poder público. Não é pouca coisa.

E, embora a existência de um Programa de Integridade não funcione como salvo-conduto, a legislação e a regulamentação expressamente o consideram na aplicação das sanções.

Nesse sentido, vale destacar o disposto no artigo 23, inciso V, do Decreto nº 11.129/2022[3], que prevê a redução de até 5% na dosimetria da multa para quem demonstra a implementação de um Programa de Integridade. Em outras palavras: maturidade não elimina risco, mas sua ausência pode agravar a exposição quando o problema já aconteceu.

Há, porém, um ponto importante de nuance. Nem toda empresa com maturidade baixa será automaticamente sancionada, porque a simples imaturidade do programa, por si só, não é sempre um ilícito autônomo no setor privado.

O problema é outro: a baixa maturidade fragiliza a prevenção, dificulta a detecção, enfraquece a reação e reduz a capacidade da empresa de demonstrar boa governança quando precisa ser escrutinada.

Quando o programa não é aplicado no dia a dia, ele alimenta a descrença interna e deixa de cumprir justamente a função para a qual foi criado. Por isso, um compliance pouco maduro não é apenas um programa incompleto; é um sistema que falha justamente quando mais se precisa dele.

O segundo grupo é menos imediato, mas igualmente sério: o risco reputacional. A integridade, hoje, não se resume ao combate à corrupção.

Quando a maturidade de compliance é baixa, o dano reputacional não surge apenas após um grande escândalo; ele pode começar muito antes, em sinais menores e recorrentes: exceções sem justificativa, tratamento desigual, ruído na liderança, falhas na resposta a denúncias, má gestão de terceiros e perda de confiança interna. E reputação, uma vez desgastada, raramente é recomposta com a mesma velocidade com que se perde.

Há ainda um terceiro grupo de consequências, muitas vezes subestimado, que podemos chamar de sanções comerciais. Nem sempre elas aparecem com esse nome, mas são reais.

Em muitos mercados, a empresa com baixa maturidade de integridade não sofre apenas risco regulatório; sofre perda de atratividade. Negócios que operam com integridade ajudam a construir mercados mais saudáveis e maior confiança de investidores.

O contrário também é verdadeiro: baixa maturidade pode significar mais *due diligence*, mais restrições, maior desconfiança, cláusulas mais duras, perda de espaço em cadeias de fornecimento e diminuição da competitividade. É uma sanção de mercado, mesmo quando não há punição estatal formal.

A legislação acompanha e reforça esse entendimento.

No campo das contratações públicas de grande vulto, isto é, acima de R$ 250 milhões, essa consequência deixa de ser apenas indireta e se torna expressa. A Lei nº 14.133/2021 e o Decreto nº 12.304/2024 deixam claro que o Programa de Integridade passou a ser exigido do licitante vencedor e ainda pode funcionar como critério de desempate, além de ser condição para reabilitação de licitante ou contratado declarado inidôneo.

Em 2027, no estado do Rio de Janeiro, o artigo 1º da Lei estadual nº 7.753/2017 passou a exigir Programa de Integridade de quem contrata com o Estado em contratos de valor superior a R$ 1,5 milhão em obras e serviços de engenharia e R$ 650 mil em compras e serviços, com multa diária pelo descumprimento (art. 6º).

[3] Art. 23. Do resultado da soma dos fatores previstos no art. 22 serão subtraídos os valores correspondentes aos seguintes percentuais da base de cálculo:

(...)

V - até cinco por cento no caso de comprovação de a pessoa jurídica possuir e aplicar um programa de integridade, conforme os parâmetros estabelecidos no Capítulo V.

Isso mostra que, em determinados contextos, a maturidade de compliance deixou de ser diferencial reputacional e passou a integrar o próprio acesso ao mercado público. Portanto, a falta de amadurecimento não expõe apenas a empresa a risco de multa; ela pode também limitar sua elegibilidade, sua competitividade e sua capacidade de voltar a contratar após uma sanção.

Existe, por fim, um quarto grupo de riscos, mais silencioso, mas profundamente corrosivo: o risco organizacional. Quando o programa é percebido como formalidade, a empresa não perde apenas proteção externa; perde coerência interna. A descrença dos colaboradores em relação ao programa e às lideranças é um efeito nocivo de um programa apenas formal.

Sem confiança interna, o canal de denúncia perde força, a liderança perde legitimidade, os controles são contornados, os problemas são ocultados e os desvios passam a ser racionalizados.

Nesse estágio, o risco deixa de ser apenas jurídico ou reputacional e passa a ser também de governança: a empresa começa a funcionar com menos transparência, menos previsibilidade e menos capacidade de correção. E uma organização que não aprende com seus próprios sinais de falha se torna mais vulnerável a crises futuras.

Por tudo isso, a maturidade de compliance não deve ser vista como troféu institucional, nem como item de *checklist*. Ela é, antes de tudo, um mecanismo de proteção. Protege a empresa contra ilícitos, mas também contra perdas de confiança, rupturas comerciais, desgaste da marca e enfraquecimento da sua governança. Em termos simples, quanto menor a maturidade, maior o custo potencial do improviso.

E quanto mais a empresa posterga esse amadurecimento, mais ela transfere para o futuro riscos que já deveriam estar sendo tratados no presente. É justamente por isso que o próximo passo da reflexão não pode ser apenas perguntar como evitar sanções, mas como fazer a integridade permanecer como parte real do funcionamento da organização.

5. Para além do código: o que faz a integridade permanecer

Se, nas seções anteriores, vimos que a integridade precisa sair do plano formal para alcançar a prática, que existem ferramentas concretas para fortalecer essa cultura e que mesmo empresas de pequeno e médio porte podem começar de forma simples, talvez reste agora a pergunta mais importante de todas: o que faz a integridade permanecer?

A resposta não está em uma grande campanha, em um treinamento isolado ou em um documento muito bem escrito. A permanência da cultura de integridade nasce da repetição coerente. Ela se forma quando a empresa, dia após dia, confirma que os valores que comunica também orientam as escolhas que faz.

É por isso que a integridade não se mede apenas pela existência de regras, mas pela constância com que elas aparecem na rotina, nas conversas, nos critérios de decisão e, sobretudo, nos momentos em que fazer o certo parece mais difícil.

Há um aspecto que merece destaque especial nesse encerramento: entre o discurso da alta liderança e a conduta efetiva das equipes existe uma ponte decisiva, que é a média liderança.

São os gestores diretos que traduzem valores em rotina. São eles que cobram metas, administram prazos, lidam com conflitos, autorizam exceções, percebem desconfortos e dão o tom do que realmente é aceitável. Se a alta administração fala em ética, mas a liderança intermediária premia o atalho, relativiza o desvio ou trata a regra como obstáculo, a cultura real será construída ali, e não no código.

Por isso, uma cultura de integridade madura não depende apenas de líderes inspiradores no topo, ela exige coerência em toda a cadeia de liderança.

Também é preciso dizer, com clareza, que cultura de integridade não é um ambiente sem erro, sem conflito ou sem dilema. Ao contrário, organizações íntegras são justamente aquelas que criam condições para que dúvidas apareçam antes que o problema cresça.

Isso significa construir espaços em que as pessoas possam perguntar, discordar, pedir orientação e reportar situações sensíveis sem medo de retaliação ou exposição desnecessária. A integridade floresce melhor em ambientes em que existe segurança para falar, e quando o colaborador percebe que levantar um risco é sinal de responsabilidade, e não de inconveniência, a empresa dá um passo importante na direção certa.

Outro ponto relevante é que a integridade não pode se tornar um ritual vazio, pois existe um risco silencioso, mas muito real, de transformar o compliance em excesso de formalidade: políticas demais, assinaturas demais, treinamentos demais, e significado de menos.

Quando isso acontece, a organização corre o risco de gerar fadiga e até cinismo, e as pessoas passam a cumprir etapas sem conexão com o propósito, e o programa começa a ser visto como burocracia, não como orientação.

Por isso, tão importante quanto ter instrumentos é garantir que eles façam sentido. Assim, integridade eficaz não é a que produz mais documentos, é a que ajuda a decidir melhor.

Esse cuidado é especialmente importante porque o ambiente de negócios se tornou mais complexo. Hoje, a cultura de integridade não pode ser pensada apenas a partir da relação entre empresa e empregado, ela atravessa fornecedores, parceiros, terceiros, prestadores de serviço, ambientes digitais, uso de dados, inteligência artificial, automação de processos e novas formas de interação com clientes e *stakeholders*.

Em outras palavras, a integridade contemporânea é relacional, e precisa alcançar não apenas o que a organização faz internamente, mas também a forma como escolhe com quem se relaciona, como supervisiona sua cadeia e como protege sua reputação em um ambiente cada vez mais conectado e veloz.

Nesse cenário, talvez uma das habilidades mais importantes de uma organização íntegra seja a capacidade de aprender, uma vez que empresas maduras não são apenas aquelas que investigam desvios, mas aquelas que conseguem transformar ocorrências em aprendizado institucional.

Um incidente, uma denúncia, uma falha de processo ou um conflito de interesse não devem ser vistos apenas como problema a se resolver, mas como oportunidades de compreender vulnerabilidades, rever fluxos, ajustar incentivos e prevenir repetições. A integridade se fortalece quando a empresa deixa de reagir apenas ao problema e passa a aprender com ele.

É por isso que medir cultura também exige um olhar mais sofisticado. Não basta contar quantos treinamentos foram realizados ou quantas denúncias entraram no canal. Esses dados são úteis, mas não suficientes; é preciso observar o que eles revelam sobre a organização.

As pessoas se sentem seguras para falar? As lideranças praticam o que comunicam? Os mesmos desvios se repetem? Há coerência nas consequências? Os parceiros mais críticos estão sendo observados com cuidado? A empresa corrige apenas o caso ou também o processo que permitiu que ele acontecesse? Cultura de integridade não é fotografia, é movimento.

Ao mesmo tempo, convém lembrar que integridade não exige perfeição; exige direção, coerência e evolução. Muitas vezes, especialmente em empresas menores, o erro está em imaginar que só é possível construir uma cultura robusta quando se tem uma estrutura sofisticada. Não é assim! Em muitos casos, o que realmente transforma o ambiente não é a complexidade do sistema, mas a clareza das expectativas, a coerência das lideranças, a seriedade diante dos desvios e a simplicidade com que o tema é tratado no cotidiano.

Uma empresa pode não ter uma grande estrutura formal e, ainda assim, ser profundamente íntegra; da mesma forma, pode ter todos os instrumentos e ainda não ter construído uma cultura confiável.

No fundo, transformar códigos em comportamento é tornar a integridade mais humana e menos abstrata, é fazer com que as pessoas compreendam não apenas o que a regra diz, mas porque ela existe e como ela protege a organização, o negócio e as relações. É reduzir o espaço do improviso ético e ampliar o espaço da consciência prática, é garantir que ninguém precise ser herói para fazer o certo, porque o ambiente já foi desenhado para tornar o certo mais claro, mais possível e mais esperado.

Por isso, talvez a melhor forma de encerrar esta seção, e, de certa forma, todo o percurso, seja retomar a ideia central: cultura não é o que a empresa declara sobre si mesma, mas o que ela confirma em suas escolhas.

O código é importante. As políticas são importantes. Os treinamentos, os canais, os controles e os processos também são. Mas tudo isso só ganha vida quando encontra coerência na liderança, credibilidade nas consequências, espaço para diálogo e humildade para aprender.

Quando isso acontece, a integridade deixa de ser uma obrigação formal e passa a ser parte da identidade da organização, e é exatamente nesse momento que o programa amadurece de verdade: quando fazer o certo deixa de depender de esforço extraordinário e passa a ser, simplesmente, a forma como a empresa funciona.

O tom do meio: onde a integridade ganha forma

como a liderança sustenta a cultura de integridade nas organizações

Anna Carolina de Vico Basile

Anna Carolina de Vico Basile é advogada com 18 anos de experiência, especializada em Compliance, Governança e Investigações Corporativas.
Atualmente atua na Fábrica Carioca de Catalisadores S.A., conduzindo iniciativas de integridade, gestão de riscos e fortalecimento da cultura ética.
Possui sólida experiência em jurídicos corporativos de grandes empresas e participação ativa em fóruns de discussão sobre Compliance e Governança.

Introdução

Muitas organizações já compreenderam a importância do chamado "tom vindo do topo". No entanto, é nos demais níveis que a cultura organizacional ganha forma concreta. Se o topo define a direção, é o meio que determina como essa direção se materializa no cotidiano. Ainda assim, é fundamental ampliar essa análise para incluir um terceiro elemento nessa dinâmica: o "tom do chão". Representado pelo nível operacional, esse grupo vivencia, na prática, a cultura de integridade da organização e, não raro, é o primeiro a identificar e reportar situações de desconformidade com normativos internos e boas práticas.

Assim, este breve artigo pretende não apenas explicar conceitos, mas também propor uma reflexão: o nível operacional tem, de fato, materializado a cultura de integridade definida pelo topo?

Vale ressaltar que os conceitos aqui apresentados devem ser aplicados com razoabilidade, podendo se adaptar tanto a empresas de menor porte quanto àquelas mais complexas e com maior número de colaboradores. A cultura de integridade, nessa perspectiva, não depende do tamanho ou da estrutura do negócio: deve estar presente no dia a dia de qualquer organização, como um ativo perene, contínuo e essencial.

O papel da alta direção no tom do topo

A consolidação de uma cultura de integridade nas empresas passa, inevitavelmente, pelo papel exercido pela liderança. Sob essa ótica, ganha destaque o conceito de "tom vindo do topo" (*tone from the top*), amplamente difundido nas práticas de governança corporativa e programas de compliance.

O termo tem origem em discussões internacionais sobre controles internos e ética corporativa, sendo incorporado por organizações como o Committee of Sponsoring Organizations of The Treadway Commission (COSO), que o define como a postura ética e o compromisso demonstrado pela alta administração em relação à integridade, à transparência e ao cumprimento de normas. Mais do que um belo discurso institucional, o tom vindo do topo se manifesta por meio de decisões, prioridades e comportamentos concretos adotados pela liderança.

No âmbito nacional, a Controladoria Geral da União também reconhece o papel central da alta administração ao estabelecer que o apoio inequívoco da liderança é condição indispensável para a credibilidade e o funcionamento adequado dos programas de integridade.

Quando os executivos e os conselhos atuam de forma coerente com os valores que defendem, contribuem para a construção de um ambiente de confiança, no qual a conduta ética deixa de ser apenas uma expectativa formal e passa a ser percebida por todos como um valor real.

Esse entendimento encontra respaldo também em movimentos recentes no cenário internacional. Em 2026, a United Nations Office on Drugs and Crime (UNODC) e o United Nations Global Compact publicaram a segunda edição do guia *"An anti-Corruption ethics and compliance programme for business: a practical guide"*, marcando uma evolução conceitual relevante: sem abandonar a importância do comprometimento da alta direção, o documento amplia essa perspectiva ao propugnar uma liderança ética distribuída por todos os níveis da organização — com ênfase especial sobre os gestores intermediários[1].

Como observa Zenkner em comentário ao documento, o *"tone at the top"* inspira, mas é o *"tone at the middle"* que executa; e é a execução que define a realidade vivida pelos colaboradores[2].

[1] UNITED NATIONS GLOBAL COMPACT; UNITED NATIONS OFFICE ON DRUGS AND CRIME (UNODC). *An Anti-Corruption Ethics and Compliance Programme for Business: A Practical Guide*. 2. ed. [*S. l.*]: United Nations Global Compact; UNODC, 2026.

[2] ZENKNER, Marcelo. Publicação sobre o novo guia anticorrupção da UNODC e do *United Nations Global Compact*. LinkedIn, 2026. Disponível em: https://www.linkedin.com/posts/marcelozenkner_integridade-compliance-integrity-share-7457752610637291523-USlq/. Acesso em: 16 jun. 2026.

Ou seja, já vimos que o tom do topo não se concretiza apenas em pronunciamentos formais ou na aprovação de um Código de Ética. Para que o comprometimento da alta direção seja percebido como genuíno, é necessário que ele se manifeste em atitudes cotidianas, decisões coerentes com os valores declarados e presença ativa nas iniciativas do Programa de Integridade. Como observa Kusserow[3], quando os líderes não demonstram esse engajamento de forma visível, os colaboradores tendem a interpretar o discurso ético como meramente protocolar, o que acaba enfraquecendo à adesão ao programa. Em contrapartida, organizações cujas lideranças são reconhecidas por agir com integridade constroem um ambiente em que os próprios colaboradores se tornam protagonistas da cultura ética, não apenas destinatários de normas.

A expressão que melhor sintetiza essa ideia é o chamado *"walk the talk"*: o tom do topo se refere ao indispensável compromisso da alta gestão com a efetividade do programa, não somente pelas palavras, mas pela tomada de atitudes e decisões de maneira ética. Concretiza-se por gestos como a presença dos dirigentes nos treinamentos, o envio de mensagens periódicas e vídeos de incentivo, e a transparência quanto ao modo como a organização reage à violação dos seus valores.

Por outro lado, a ausência desse alinhamento compromete significativamente a efetividade de qualquer iniciativa de integridade. Políticas, códigos de conduta e treinamentos perdem força quando não encontram respaldo nas atitudes daqueles que ocupam posições de liderança.

Meio que determina a direção da integridade

Embora essencial, o tom vindo do topo, por si só não é suficiente para garantir a consolidação de uma cultura ética. Entre as diretrizes estratégicas e a realidade operacional, existe um nível organizacional que exerce papel decisivo na tradução desses valores em comportamentos concretos: a liderança intermediária.

Aqui vale reforçar que essa lógica se aplica tanto a ambientes com nove ou com 200 colaboradores. Nesse contexto, os gestores intermediários atuam como verdadeiros mediadores entre a estratégia e a execução. São eles que interpretam políticas, orientam equipes, estabelecem prioridades e lidam com os dilemas práticos que nem sempre estão previstos em normas formais.

Muito se fala que a base estrutural de um Programa de Compliance efetivo é o apoio da alta administração. Porém, é no nível intermediário que o sistema é operacionalizado. Curiosamente, documentos normativos de referência, como a ISO 37.301, não utilizam a expressão *"tone at the middle"* — nem mesmo *"tone at the top*: a norma trabalha com o vocabulário de liderança e comprometimento da alta direção e do órgão de governança, atribuindo aos gestores responsabilidades de compliance dentro de suas respectivas áreas. Essa estrutura, ainda que sob nomenclatura distinta, reforça a premissa central deste artigo: a integridade organizacional exige comprometimento ativo em todos os níveis hierárquicos. Se um gestor intermediário não compreende ou não dá a devida importância ao compliance, as prioridades éticas são diluídas ou simplesmente filtradas antes de chegarem à base.

Ao longo da minha atuação em Compliance, já me deparei com situações em que funcionários terceirizados recorriam diretamente ao supervisor da empresa tomadora para resolver questões cotidianas ou entregar atestados médicos — rotina que, do ponto de vista jurídico, alimenta o risco de reconhecimento de vínculo empregatício. Em outros casos, esses mesmos profissionais acionavam o canal de denúncias da tomadora para relatar ausência de *feedbacks* ou de oportunidades de desenvolvimento por parte da liderança da contratante — evidenciando um problema de escopo do canal, que passa a receber temas de gestão de pessoas alheios ao seu

[3] KUSSEROW, Richard P. **Culture of Compliance Begins with the Tone at the Top**. Strategic Management Services, LLC. Disponível em: https://www.compliance.com/resources/culture-of-compliance-begins-with-the-tone-at-the-top/. Acesso em: 13 abr. 2026.

propósito original. Nos dois casos, a falha não estava na norma escrita: estava no tom do meio. Um supervisor que não compreende os limites do seu papel em relação ao terceirizado, ou um gestor que não orienta corretamente os colaboradores sobre o uso do canal, transforma uma boa estrutura de compliance em risco concreto para a organização.

Imaginemos o cenário de um pequeno empreendedor. Se o funcionário observa o próprio dono sonegando impostos ou negociando com fornecedores mediante favores ou presentes em troca de melhores condições, que tipo de referência está sendo construída? Que comportamento tende a ser replicado? O tom vem do topo, não apenas por meio de discursos bem estruturados, mas, sobretudo, pelos exemplos. E ele se aplica à liderança intermediária, cuja atuação também é moldada e percebida a partir das práticas que adota no cotidiano. A cultura não se declara. Se demonstra.

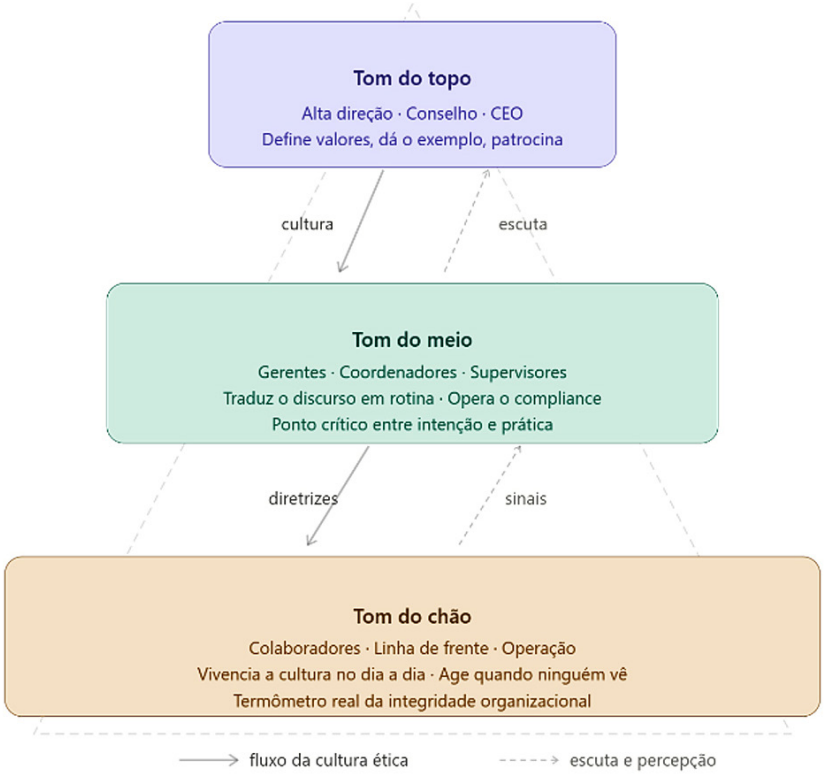
Os exemplos acima evidenciam não apenas o papel da liderança intermediária, mas também a importância de um terceiro elemento nessa dinâmica: "o tom do chão". É no nível operacional que a cultura da integridade é, de fato, vivenciada e no qual eventuais desvios se tornam mais visíveis.

O tom do chão

Quando há alinhamento entre o tom vindo do topo, a atuação da liderança intermediária e a experiencia vivida no nível operacional, a integridade deixa de ser um valor declarado e passa a ser incorporada como um elemento estruturante da cultura organizacional. Mais do que um requisito regulatório, a integridade se consolida, assim, como um ativo estratégico, uma vez que é capaz de fortalecer a confiança, orientar decisões e sustentar relações mais éticas e transparentes no ambiente corporativo.

Diante desse cenário, o nível operacional deixa de ocupar uma posição meramente executora e passa a atuar como agente ativo da cultura de integridade. É quando os colaboradores se sentem seguros para questionar, reportar e decidir com base nos valores e não apenas em regras. A integridade, então, deixa de depender exclusivamente da liderança e passa a ser sustentada coletivamente, como parte do próprio funcionamento da empresa.

A imagem a seguir sintetiza os principais pontos abordados até aqui.



O professor Kirk O. Hanson, do Markkula Center for Applied Ethics da Universidade de Santa Clara, é um autor com muitas matérias sobre o tema. Em seu artigo *"Ethics and the middle manager: creating tone in the middle"*, entre as ações sugeridas por Hanson para que a alta liderança fortaleça o tom do meio — e, consequentemente, o tom do chão —, destacam-se: [4]pedir aos gestores intermediários que identifiquem os dilemas éticos que se tornam obstáculos em sua área; oferecer orientação geral sobre como aplicar os valores da empresa a esses dilemas; delegar a eles a responsabilidade de resolver dilemas éticos; deixar claro que o desempenho ético e financeiro são monitorados com igual peso; e tornar a competência ética parte formal da avaliação de desempenho dos gestores.

Hanson acrescenta ainda que a empresa deve oferecer oportunidades para que os gestores intermediários trabalhem com seus pares na resolução dos casos mais difíceis, e que, a alta administração deve estar disponível para discutir, orientar e resolver os casos mais complexos.

A diversidade de conceitos encontrados durante a pesquisa evidencia a relevância e a atualidade do tema. Ainda assim, é importante reconhecer que as organizações (especialmente as de maior porte) precisam avançar na difusão não apenas do conceito, mas também de sua aplicação prática, para que possamos, de fato, transitar do ideal para o real.

Ainda durante a pesquisa para elaboração deste artigo, encontrei um artigo das advogadas e pesquisadoras Ana Paula Ávila e Caroline Sturmer Corrêa sobre o tema. De forma bastante precisa, elas destacam que o grande desafio de desenvolver uma cultura de compliance está em tornar a ética e os valores da organização em algo orgânico e naturalmente perceptível, de modo que estruturas concebidas de forma abstrata se concretizem por meio de atitudes, comportamentos e relações com as partes interessadas.

O que mais me chamou a atenção, no entanto, foi a frase de fechamento do artigo delas. A conexão entre conceitos tão contemporâneos e a filosofia sempre encontra um lugar especial em mim. Na conclusão, as autoras recorrem a Aristóteles ao afirmar: "Portanto, se a 'virtude está no meio'[5] — como já preconizava o filósofo —, a plena eficiência dos programas de compliance, de certo modo, também está".

A resposta à pergunta feita no início do artigo não está nos documentos de política interna, nos relatórios de treinamento ou nos indicadores de canal de denúncias. Ela está no comportamento cotidiano de quem ocupa cada um desses níveis – no gesto do líder que recusa um presente de um fornecedor mesmo quando ninguém está olhando, na decisão do gestor intermediário que orienta sua equipe a reportar uma inconformidade mesmo que isso gere desconforto, e na coragem do colaborador operacional que confia que sua voz será ouvida e protegida. É nesse espaço, entre o que se declara e o que se pratica, que a cultura de integridade se constrói ou se desfaz.

Transitar do ideal para o real exige, portanto, mais do que compromisso formal da alta direção. Exige que o tom do topo encontre ressonância no meio e chegue vivo ao chão. Quando esses três níveis se alinham (não por obrigação regulatória, mas por convicção genuína), a integridade deixa de ser um programa e passa a ser parte do próprio modo de ser da organização. E é esse o verdadeiro ativo estratégico que nenhuma auditoria consegue criar, mas que toda liderança tem o poder de cultivar.

[4] HANSON, Kirk O. *Ethics and the Middle Manager*: Creating Tone in the Middle. Santa Clara: Markkula Center for Applied Ethics, Santa Clara University, 2008. Disponível em: https://www.scu.edu/ethics/focus-areas/business-ethics/resources/ethics-and-the-middle-manager-creating-tone-in-the-middle/. Acesso em: 13 abr. 2026.

[5] ÁVILA, Ana Paula; CORRÊA, Caroline Sturmer. O "tone from the middle" na construção da cultura de compliance. *Consultor Jurídico*, 8 dez. 2021. Disponível em: https://www.conjur.com.br/2021-dez-08/avila-correa-tone-from- -the-middle-cultura-de-compliance/. Acesso em: 13 abr. 2026.

Referências

ÁVILA, Ana Paula; CORRÊA, Caroline Sturmer. O "tone from the middle" na construção da cultura de compliance. *Consultor Jurídico*, 8 dez. 2021. Disponível em: https://www.conjur.com.br/2021-dez-08/avila-correa-tone-from-the-middle-cultura-de-compliance/. Acesso em: 13 abr. 2026.

BRASIL. CONTROLADORIA-GERAL DA UNIÃO (CGU). *Programa de Integridade*: diretrizes para empresas privadas. Brasília, DF: CGU, 2015. Disponível em: https://www.gov.br/cgu/pt-br/centrais-de-conteudo/publicacoes/integridade/arquivos/programa-de-integridade-diretrizes-para-empresas-privadas.pdf/view. Acesso em: 18 out. 2026.

COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION (COSO). *Internal Control – Integrated Framework*. Durham: American Institute of Certified Public Accountants, 2013.

HANSON, Kirk O. *Ethics and the Middle Manager: Creating Tone in the Middle.* Santa Clara: Markkula Center for Applied Ethics, Santa Clara University, 2008. Disponível em: https://www.scu.edu/ethics/focus-areas/business-ethics/resources/ethics-and-the-middle-manager-creating-tone-in-the-middle/. Acesso em: 13 abr. 2026.

KUSSEROW, Richard P. *Culture of compliance begins with the tone at the top.* [*S. l.*]: Strategic Management Services, LLC, 2022. Disponível em: https://www.compliance.com/resources/culture-of-compliance-begins-with-the-tone-at-the-top/. Acesso em: 13 abr. 2026.

ORGANIZAÇÃO INTERNACIONAL DE NORMALIZAÇÃO (ISO). ISO 37301:2021 – *Compliance Management Systems – Requirements with Guidance for use.* Genebra: ISO, 2021.

UNITED NATIONS GLOBAL COMPACT; UNITED NATIONS OFFICE ON DRUGS AND CRIME (UNODC). A*n Anti-Corruption Ethics and Compliance Programme for Business:* a practical guide. 2. ed. [*S. l.*]: United Nations Global Compact; UNODC, 2026..

ZENKNER, Marcelo. *Do tone at the top ao tone at the middle: a nova abordagem da UNODC para programas de integridade* [post]. LinkedIn, 6 maio 2026. Disponível em: https://www.linkedin.com/posts/marcelozenkner_integridade-compliance-integrity-share-7457752610637291523-USlq/. Acesso em: 16 jun. 2026.

Da norma ao comportamento:

o desafio da comunicação e educação ética nas organizações

Luiz Claudio Cabral Coelho

Luiz Claudio Cabral Coelho é analista de Integridade Corporativa da Firjan. Advogado especialista em *Compliance* pela Fundação Getúlio Vargas de São Paulo (FGV Law - SP); especialista em Direito Digital pela Escola Paulista de Direito (EPD); e em Direito Público pela Escola Superior da Magistratura Federal do Rio Grande do Sul (ESMAFE - RS); bacharel em Direito pela Universidade Federal do Rio de Janeiro (UFRJ). Atua há 7 anos com assessoria e consultoria empresarial nas áreas de *Compliance*, Privacidade e Proteção de Dados Pessoais.

1. Normas não mudam culturas sozinhas

A implantação de programas de compliance nas organizações brasileiras vem sendo progressivamente reconhecida como um instrumento central de governança e de promoção de uma cultura ética sustentável. De acordo com as diretrizes da Controladoria-Geral da União, tanto em sua versão inaugural de 2015 quanto no guia atualizado de 2024, um Programa de Compliance efetivo deve ser estruturado a partir de pilares essenciais que garantam sua legitimidade, coerência e aderência à realidade do negócio. Entre esses pilares, destacam-se: (i) o comprometimento inequívoco da alta administração — expresso não apenas em discursos, mas em decisões e comportamentos concretos —; (ii) a definição de uma instância responsável pelo Programa, dotada de autonomia e recursos adequados; (iii) a identificação, análise e gestão contínua dos riscos de integridade, considerando o contexto operacional, setorial e regional da organização.

Sobre essa base estrutural, o Programa de Compliance se materializa por meio de seu quarto pilar: um plano de ação que compreende a elaboração e a implementação de instrumentos normativos e orientativos, como o Código de Ética e Conduta, políticas, procedimentos e protocolos internos de compliance. A complexidade desses instrumentos deverá ser proporcional ao porte, à estrutura e ao nível de risco a que está exposta a organização.

Aqui, porém, surge uma questão incômoda: a mera existência desses documentos garante que as pessoas realmente os entendam e os coloquem em prática? Chen e Soltes (2018) observam que é comum empresas "demonstrarem" conformidade por meio de simples relatórios de assinaturas, nos quais os colaboradores afirmam ter lido e compreendido essas políticas. O problema é evidente: assinar um documento não significa que o conhecimento dele se transformou em comportamento cotidiano. A lacuna entre o "ter lido" e o "ter compreendido" é precisamente onde muitos programas de compliance fracassam. Reconhecendo essa realidade, as Diretrizes da CGU (2024) identificam treinamentos e ações de comunicação ética como elementos essenciais do Programa, ao enfatizar que não basta ter políticas bem redigidas — é indispensável investir de forma sistemática nessas estratégias. É por meio de ações contínuas de comunicação clara e de processos educativos estruturados que o Programa deixa de ser um conjunto formal de regras e passa a orientar, de maneira concreta, o comportamento cotidiano de dirigentes, empregados e terceiros, contribuindo para a consolidação de uma cultura de integridade viva e funcional.

Mas aqui reside um paradoxo perturbador. Mesmo com investimentos consideráveis em todas essas iniciativas de compliance — especialmente por parte de empresas de grande porte[1] —, a má conduta corporativa persiste de modo surpreendente. Chen e Soltes (2018) identificam uma frustração dupla: de um lado, executivos se veem presos a custos crescentes de conformidade sem enxergar benefícios claros; de outro, colaboradores percebem os programas como uma série de rotinas burocráticas e treinamentos genéricos sem propósito real. O resultado é previsível: as pessoas dedicam apenas a atenção necessária a treinamentos genéricos e pouco eficazes para serem aprovados na dinâmica final, permitindo à empresa "demonstrar aos órgãos reguladores que cumpriram a tarefa". Quanto às comunicações[2] sobre conformidade emitidas pela alta administração, mesmo um alto volume delas pode revelar-se uma métrica falsa, especialmente quando pesquisas internas mostram que colaboradores não confiam na gestão ou temem represálias ao denunciar irregularidades de boa-fé.

A conclusão dos autores, porém, traz alguma esperança: esse custo e essa frustração, embora trágicos, são evitáveis. Uma melhor mensuração do Programa leva a uma melhor gestão do compliance. Em outras palavras, o problema não está na impossibilidade de mudar culturas, mas em não saber medir se a mudança está realmente acontecendo.

[1] Empresas norte-americanas.

[2] Tema que será aprofundado no Tópico 3.

2. Os desafios culturais no cenário fluminense

Uma pesquisa relevante, realizada pela Federação das Indústrias do Estado do Rio de Janeiro (Firjan 2026), conduzida por sua Gerência de Estudos e Pesquisas (GEP) entre maio e julho de 2025, buscou compreender as práticas de governança corporativa aplicadas nas cadeias produtivas de 388 (trezentas e oitenta e oito) empresas fluminenses, majoritariamente indústrias de portes variados, nacionais e multinacionais.

O que revelam esses números é simultaneamente esperado e preocupante. Apesar dos avanços evidenciados na incorporação de práticas de governança em integridade, dentre os 27 critérios de governança mais adotados pelas empresas pesquisadas, apenas 60,5% afirmam possuir programas de compliance implementados relacionados a práticas anticorrupção. Quando se observa especificamente os Códigos de Ética e Conduta, considerados o instrumento mais visível e fácil de implementar, o percentual sobe para 74,4%. Mas quando se desce para políticas antiassédio, o número cai para 58,1%, e para canais de denúncias em funcionamento, apenas 55,0% das organizações os possuem.

A situação se agrava quando se examina controles mais sofisticados. Apenas 52,7% das empresas incluem cláusulas de compliance em contratos com terceiros, e somente 51,2% realizam gestão de riscos de integridade. No tocante a diligência na contratação de colaboradores e terceiros, esse percentual cai para 48,8%, e auditorias de terceiros alcançam apenas 43,4% das organizações pesquisadas.

O mais revelador, contudo, é o dado sobre relacionamento com autoridades públicas: apenas 35,7% das organizações implementaram critérios para isso, um número que contrasta dramaticamente com o fato de que a maioria afirmou possuir programas de compliance anticorrupção. Há, portanto, uma contradição estrutural: as empresas declaram ter programas, mas carecem de controles específicos em áreas de alto risco.

Essa lacuna se torna ainda mais evidente quando se examina a educação ética. Dentre as organizações que possuem internalizadas todas, ou pelo menos grande parte das boas práticas acima mencionadas, apenas 29,8% efetivamente implementaram projetos de educação sobre integridade para seus colaboradores e terceiros; outros 26,7% ainda estão em fase de planejamento dessas ações; e 43,5% não possuem qualquer projeto educacional sobre o tema. Nenhuma delas declarou possuir metodologias de mensuração de seus respectivos programas. Os dados sugerem que, em grande parte das organizações analisadas, o Programa de Compliance ainda não completou a transição do plano formal para o plano comportamental. Embora os dados não mensurem diretamente o comportamento organizacional, a escassez de iniciativas de educação ética, a ausência de metodologias de mensuração e as lacunas em controles específicos de alto risco constituem indícios consistentes de que muitos programas permanecem predominantemente normativos, o que Pagani e Soares (2022, p. 112) denominam "compliance de gaveta". Essa condição, conforme os autores alertam, decorre da falta de compreensão sobre o verdadeiro sentido do termo "compliance" que, antes de qualquer definição técnica, envolve comportamento. Portanto, sem o compromisso com uma cultura de integridade, por melhor que seja o programa, ele não será válido.

Há ainda outro segmento que merece atenção: as organizações que declararam não possuir Programa de Compliance implementado. Entre elas, 43,9% afirmam não ver sequer essa necessidade. Outros 18,2% alegam falta de tempo ou prioridade em suas agendas. Já 17,4% das empresas atribuem a não implementação à falta de conhecimento adequado sobre o tema, enquanto 15,2% entendem não possuir recursos financeiros ou humanos suficientes.

Esse quadro ganha contornos ainda mais preocupantes quando se considera o marco normativo específico do Estado do Rio de Janeiro. A Lei Estadual nº 7.753/2017 exige a implementação de Programas de Integridade pelas empresas que firmam contratos com a Administração Pública estadual acima de determinados valores e, entre os parâmetros por ela elencados para avaliação desses programas, figuram expressamente as ações comprovadas de promoção da cultura ética por meio de palestras, seminários, *workshops* e iniciativas similares. Esse é precisamente o elemento que os dados da Firjan revelam como o mais negligenciado pelas organizações pesquisadas. Isso significa que, para as empresas fluminenses que mantêm ou pretendem manter contratos com o Estado do Rio de Janeiro, a ausência de iniciativas sistemá-

ticas de comunicação e educação ética não configura apenas uma fragilidade de gestão ou uma limitação estratégica, ela representa uma potencial desconformidade legal, com consequências diretas sobre a elegibilidade e a continuidade dessas relações contratuais.

Os achados da pesquisa da Firjan corroboram, de forma contundente, as reflexões teóricas anteriormente apresentadas: normas, por si só, não constroem culturas, tampouco sustentam comportamentos éticos duradouros. Embora parte significativa das organizações fluminenses declare possuir Programas de Compliance e instrumentos normativos estruturados, a escassez de iniciativas sistemáticas de comunicação e educação ética revela uma lacuna crítica entre a formalização e a vivência cotidiana da integridade. Os dados indicam que, ao negligenciarem as ações de comunicação e educação ética — responsáveis por dar sentido, compreensão e legitimidade às regras —, muitas organizações esvaziam o potencial transformador de seus Pprogramas, perpetuando práticas de "conformidade aparente". Assim, o desafio central não reside apenas na criação de políticas, mas na capacidade de traduzi-las em aprendizado organizacional contínuo, capaz de moldar percepções, decisões e comportamentos de forma coerente e sustentável.

3. Comunicação ética como instrumento de engajamento

Segundo Paine (1994), a ética organizacional vai além de simplesmente evitar violações à lei, e apenas disponibilizar códigos de ética e políticas internas aos colaboradores pouco contribui para a solução de problemas relacionados à conduta ilícita. Torna-se necessária às organizações uma abordagem abrangente, que vá além da postura de conformidade legal meramente punitiva. Isso significa não mais enxergar a ética como um comportamento individualista, imutável e impermeável às influências organizacionais. É compreender o papel da própria organização na formação comportamental individual de seus colaboradores, a fim de que a necessidade de obedecer à lei passe a ser vista como um aspecto positivo da vida organizacional, como a força motriz da própria empresa, e não mais como uma restrição indesejável imposta pelo Poder Público.

Nesse cenário, destacam-se a comunicação dos valores corporativos e os debates éticos, haja vista que ambos contribuem para a criação de um compromisso genuíno por parte dos colaboradores, e não apenas para gerar o "medo de sanções". Kaptein (2011) esclarece que a comunicação ativa e de alta qualidade – que pode englobar o envio de e-mails corporativos, *newsletters*, cartazes, quadros de aviso, vídeos institucionais na *intranet*, mesas redondas, dentre outros – é fundamental para que um Código de Ética e Conduta seja eficaz na redução de comportamentos antiéticos. O modelo estatístico utilizado pelo autor em sua pesquisa demonstrou que quanto maior a frequência dessas ações, menos desvios de conduta são observados. E se, além da frequência, a comunicação se mostrar de boa qualidade – acessível, compreensível e útil –, a redução de comportamentos antiéticos é substancial[3]. Isso porque, segundo o autor, o engajamento real ocorre quando os colaboradores sentem que a informação é útil para o seu trabalho e está disponível quando dela precisam. Quando o código é bem comunicado, os funcionários já estão familiarizados com ele e esperam que a gestão atue como modelo, o que cria um ambiente de reforço mútuo entre as normas escritas e a prática diária.

Os achados de Kaptein (2011) permitem identificar, na prática, quatro atributos essenciais que toda estratégia de comunicação ética deve observar para ser eficaz. O primeiro é a *clareza*: as mensagens relacionadas a valo-

[3] O modelo de regressão apresenta R^2 de aproximadamente 0,32, indicando que as variáveis de qualidade e frequência da comunicação explicam cerca de 32% da variação observada nos comportamentos antiéticos, resultado estatisticamente relevante no campo da ética organizacional.

res, normas e condutas esperadas precisam ser diretas e objetivas, sem ambiguidades que possam gerar interpretações divergentes diante de situações concretas. O segundo é a *acessibilidade*, entendida não apenas como a facilidade de acesso físico ou digital ao conteúdo, mas, sobretudo, como a adequação da linguagem à diversidade de públicos internos — considerando diferentes níveis de escolaridade, funções e contextos culturais presentes na organização. O terceiro atributo é a *consistência*: a comunicação ética não pode ser contraditória em si mesma, tampouco divergir das práticas efetivamente adotadas pela liderança, pois a percepção de incoerência entre o discurso institucional e o comportamento observado no cotidiano organizacional mina a credibilidade do Programa de Compliance e fragiliza o compromisso dos colaboradores com os valores que se pretende cultivar. Por fim, a *frequência* — já demonstrada empiricamente pelo autor como variável estatisticamente relevante na redução de desvios de conduta — assegura que a integridade permaneça presente de forma contínua no cotidiano organizacional, impedindo que o tema se restrinja a momentos pontuais, como a integração de novos colaboradores ou a publicação esporádica de um código de conduta.

Mais do que um alerta sobre o que comunicar, Kaptein (2011) vai além ao alertar para o risco inverso: quando o código é mal comunicado, seja de forma inacessível, infrequente ou descolada da realidade cotidiana do colaborador, ele pode se tornar contraproducente, gerando ceticismo, distanciamento e até resistência ativa em lugar de engajamento. Esse achado reforça que não se trata apenas de comunicar mais, mas de comunicar bem: uma estratégia de comunicação ética deficiente não é simplesmente ineficaz — ela pode comprometer ativamente a credibilidade do Programa e minar o vínculo entre o colaborador e os valores que a organização pretende cultivar.

A concretização desses atributos, contudo, depende da utilização articulada de diferentes canais e atores organizacionais, tanto no plano formal quanto no informal. No âmbito dos canais formais, campanhas internas estruturadas — como treinamentos periódicos, comunicados institucionais, boletins temáticos, cartilhas e materiais visuais distribuídos nos ambientes de trabalho — cumprem o papel de garantir alcance amplo e uniforme das mensagens de integridade, conferindo ao Programa de Compliance visibilidade e regularidade. Já os canais informais, como conversas de equipe, reuniões de alinhamento e espaços de diálogo aberto, permitem que os valores éticos sejam discutidos de forma contextualizada e próxima à realidade do colaborador, conferindo ao tema uma dimensão humana e prática que os instrumentos normativos escritos, isoladamente, não conseguem alcançar. Nesse processo, a liderança exerce papel insubstituível: gestores e líderes intermediários são, na prática, os principais comunicadores de valores dentro de uma organização, pois seu comportamento cotidiano sinaliza, de forma mais poderosa do que qualquer política escrita, o que a empresa genuinamente valoriza e tolera. Quando a liderança age de forma alinhada ao discurso institucional, reforça a credibilidade do Programa; quando age de modo contrário, invalida qualquer esforço comunicativo, por mais bem estruturado que seja. Por sua vez, o canal de denúncias — frequentemente compreendido apenas como um mecanismo sancionatório — possui também uma relevante dimensão pedagógica: ao permitir que colaboradores relatem condutas inadequadas ou formulem consultas sobre situações de dúvida ética, ele funciona como um espelho do ambiente organizacional, sinalizando à gestão em que aspectos da organização se encontram as lacunas de compreensão e os pontos de maior vulnerabilidade comportamental. Nessa perspectiva, o canal de denúncias não encerra sua função na apuração de irregularidades; ele retroalimenta o próprio ciclo comunicativo, orientando o aprimoramento contínuo das estratégias de engajamento ético.

Segundo Paine (1994), é dessa forma que a integridade deixa de ser vista como um custo operacional e se torna um princípio norteador das empresas. Integridade não se impõe, se engaja.

4. Não basta treinar; é necessário medir, analisar e revisar

Segundo Chen e Soltes (2018), o objetivo dos treinamentos em conformidade é a prevenção de condutas inadequadas, auxiliando colaboradores a internalizar leis e regulamentos de forma que o comportamento adequado se perpetue. Mas aqui surge uma questão fundamental que muitas organizações negligenciam: como saber se o treinamento realmente funcionou?

Pagani e Soares (2022, p. 108-109) oferecem uma resposta direta: programas de compliance só são efetivos quando todos os colaboradores estão adequadamente cientes de seus papéis, responsabilidades e, principalmente, das consequências da violação das regras aplicáveis. Para alcançar isso, a comunicação clara, objetiva e acessível à diversidade de públicos, bem como o treinamento aprofundado[4] das diretrizes legais e internas, não podem ser meros desdobramentos do programa, precisam ser tratados como verdadeiras ferramentas estratégicas de prevenção e orientação comportamental.

Quando cada membro do time é capaz de identificar, tratar, comunicar e prevenir situações com potenciais indícios de irregularidades, a conformidade deixa de ser uma obrigação e passa a ser uma competência. Isso só se alcança com o conhecimento adequado tanto das leis quanto das diretrizes corporativas internas.

Reconhecer que diferentes públicos internos estão expostos a riscos distintos é o passo seguinte. Uma estratégia educativa que oferece um conteúdo único e genérico a todos os colaboradores ignora essa realidade. A alta administração, por exemplo, precisa ser capacitada com ênfase em sua responsabilidade institucional e no papel modelador que exerce sobre toda a organização, uma vez que seus comportamentos e decisões reverberam diretamente na cultura ética da empresa. As lideranças intermediárias — gerentes, coordenadores e supervisores —, por sua vez, demandam treinamentos orientados à gestão de equipes com integridade, à identificação de desvios de conduta e à condução de conversas éticas no cotidiano. Já os colaboradores em geral devem ser capacitados sobre as normas e valores que orientam suas atividades específicas. E os terceirizados, frequentemente negligenciados nesse processo, também precisam ser alcançados, sobretudo quando atuam em atividades sensíveis ou em nome da organização contratante.

Os temas que devem compor essas trilhas formativas variam em profundidade conforme o público, mas alguns são transversais. Dentre eles, destacam-se o conflito de interesses — cuja identificação exige sensibilidade situacional que nem sempre decorre da simples leitura de uma política —, o assédio moral e sexual, as regras de relacionamento com a Administração Pública e, cada vez mais, a privacidade e a proteção de dados pessoais, dada a centralidade que o tema adquiriu com a vigência da Lei Geral de Proteção de Dados (Lei nº 13.709/2018 – LGPD).

Uma alternativa eficaz para estruturar essa abordagem segmentada é a implementação de um Programa Anual de Capacitação com Trilha de Aprendizagem, por meio do qual os conteúdos são organizados de forma progressiva e personalizada para cada público, garantindo que o desenvolvimento ético seja planejado, monitorado e revisado de forma sistemática ao longo do ano, e não relegado a iniciativas esparsas e desconexas.

Mas aqui reside um problema prático que compromete a efetividade de muitos treinamentos, mesmo quando bem planejados e segmentados. O primeiro deles é o uso de linguagem excessivamente técnica. Quando o conteúdo é apresentado em termos jurídicos ou normativos sem a devida contextualização, ele se torna distante da realidade cotidiana do colaborador — que pode até compreender as palavras, mas não consegue traduzi-las em decisões e comportamentos concretos. O segundo fator é a ausência de exemplos práticos: treinamentos que se limitam a reproduzir o texto de políticas e regulamentos, sem ilustrá-los com situações reais ou hipotéticas próximas ao universo do público-alvo, tendem a gerar pouco engajamento e baixa retenção de conhecimento.

Aqui está o ponto crítico que Chen e Soltes (2018) enfati-

[4] Palestras, seminários, *workshops*, certificações, materiais de estudo etc., cujo conteúdo pode ser geral ou específico, e de realização obrigatória.

zam: a simples aferição do entendimento dos colaboradores sobre o que deles se espera após o término de um treinamento é insuficiente para concluir a sua eficácia. Um nível elevado de compreensão pode derivar de conhecimento prévio sobre o tema, e não necessariamente representar o efeito da educação recebida. Por isso, as organizações precisam avaliar o conhecimento dos colaboradores antes e após a atividade educativa: caso a mudança seja pouco significativa, o treinamento pode ser considerado desnecessário ou carente de aprimoramentos, e, portanto, incapaz de promover o engajamento esperado. Isso reforça ainda que os treinamentos não devem ser tratados como eventos pontuais, mas como um processo contínuo e recorrente, capaz de acompanhar a evolução dos riscos, das normas e da própria cultura organizacional.

As reflexões acima evidenciam que a eficácia dos treinamentos não pode ser presumida, devendo ser constantemente validada por critérios objetivos e metodologias adequadas de avaliação. Segundo a Norma ABNT NBR ISO 37301:2021 (2021, p. 41), o monitoramento é o "processo de coleta de informação com o propósito de avaliar a eficácia do sistema de gestão de compliance e o desempenho de compliance da organização". Cabe à organização determinar quando e o que deve ser monitorado e medido, bem como os respectivos métodos de análise e avaliação. Em suma, não basta treinar; é necessário medir, analisar e revisar. De acordo com a mesma Norma:

> A organização deve desenvolver, implementar e manter um conjunto de indicadores apropriado que orientem a organização na avaliação do alcance dos seus objetivos de compliance, para avaliar o seu desempenho de compliance (ABNT NBR ISO 37301:2021, p. 19).

É por essa razão que Chen e Soltes (2018) enxergam a conformidade não como um mero exercício jurídico, mas como uma verdadeira ciência comportamental — por eles intitulada "Engenharia de Conformidade". Nessa perspectiva, códigos de ética e conduta devem articular políticas e procedimentos internos para o sucesso da empresa, e o canal de denúncias assume papel que vai além do reporte de irregularidades, funcionando também como instrumento de consulta dos colaboradores para a prevenção de atitudes inadequadas. Com o auxílio da Engenharia de Conformidade, gestores passam a poder avaliar o que funciona e o que não funciona — o que exige experimentação e inovação. Nas palavras dos autores: "Uma engenharia de conformidade bem-sucedida exige criatividade, testes e um design de modelo cuidadoso para mensurar os resultados de forma apropriada" (Chen; Soltes, 2018).

5. O papel das consultorias e escritórios especializados

A construção de um Programa de Compliance efetivo raramente ocorre de forma isolada. Em muitos casos, especialmente em organizações que ainda não dispõem de *expertise* interna consolidada na área, a contratação de assessoria externa especializada — seja por meio de escritórios de advocacia com atuação em compliance, seja por consultorias dedicadas à governança e integridade corporativa — representa não apenas uma escolha estratégica, mas uma etapa necessária do processo de maturação do Programa. Nesse sentido, as Diretrizes para Empresas Privadas da Controladoria-Geral da União, em sua edição de 2024, oferecem balizas importantes sobre como essa contratação deve ser concebida e conduzida.

As Diretrizes da CGU (2024) orientam que a assessoria externa especializada deve ser concebida como complemento estratégico ao protagonismo interno da organização, e não como sua substituta. A responsabilidade pela condução e efetividade do Programa permanece, intransferível, com a própria organização. A partir dessas orientações e da experiência consolidada em programas de integridade, é possível identificar três situações típicas em que esse apoio externo se mostra especialmente valioso: quando a organização está estruturando seu Programa pela primeira vez e não dispõe de *expertise* interna suficiente; quando busca uma avaliação independente da maturidade do Programa já existente; ou quando pretende revisar e aprimorar iniciativas em curso

à luz de novas exigências normativas ou de mudanças no perfil de risco. Em todos esses casos, o assessor externo atua como parceiro técnico que, por sua independência, tem condições de oferecer diagnóstico mais objetivo e propor intervenções que, de outro modo, poderiam ser minimizadas por razões políticas ou institucionais.

Nessa perspectiva, o *United Nations Office on Drugs and Crime (UNODC)* já sinalizava, em seu guia prático sobre programas de ética e compliance anticorrupção para empresas (2013), que associações empresariais, escritórios de advocacia, empresas de auditoria e consultorias especializadas em compliance podem prestar assistência valiosa às organizações que desejam estruturar ou aprimorar seus programas. O guia destaca, em especial, que esse apoio externo é relevante não apenas na fase de implementação, mas de forma contínua, para manter o Programa atualizado e sustentar um processo permanente de melhoria. Mais do que isso, a UNODC sublinha que os assessores externos desempenham papel central em ajudar as organizações a traduzir princípios éticos abstratos em orientações operacionais concretas, adequadas ao seu setor de atuação e ao seu perfil de risco — e é precisamente nessa tradução que reside o processo de internalização, ou seja, a passagem das normas escritas para o comportamento cotidiano.

Essa distinção entre implementação e internalização é fundamental. Implementar um programa significa dotá-lo de estrutura: políticas, procedimentos, canais, treinamentos e instâncias de governança. Internalizar, por sua vez, significa fazer com que esses elementos deixem de ser percebidos como obrigações externas e passem a orientar genuinamente as decisões e os comportamentos dos colaboradores em todos os níveis hierárquicos. É nesse segundo movimento — mais profundo e mais difícil — que a atuação de consultores e escritórios especializados pode se revelar mais valiosa, pois eles trazem não apenas conhecimento técnico, mas uma perspectiva independente que frequentemente permite identificar lacunas culturais e comportamentais que equipes internas, por razões de proximidade ou viés institucional, tendem a não perceber.

O Departamento de Justiça dos Estados Unidos (DOJ), em seu documento "Evaluation of Corporate Compliance Programs", atualizado em setembro de 2024 e disponível publicamente no site do DOJ, incorporou essa compreensão ao seu critério de avaliação de programas corporativos. O documento orienta que os procuradores considerem, entre outros fatores, se a organização envidou esforços concretos para avaliar a efetividade de seu Programa, o que pode incluir a busca por *expertise* externa. Nesse contexto, a contratação de consultores ou advogados especializados para conduzir avaliações independentes, identificar *gaps* em relação aos padrões do setor, desenvolver treinamentos culturalmente adequados e propor melhorias estruturais pode ser lida como evidência do comprometimento genuíno da organização com a conformidade — em contraposição à chamada "conformidade cosmética".

É importante registrar, contudo, que a atuação de terceiros especializados não substitui o engajamento interno. O consultor pode diagnosticar, propor, capacitar e monitorar, mas a transformação cultural depende, em última análise, do comprometimento da liderança e da disposição da organização em tratar a integridade como valor central e não como obrigação regulatória. Nesse sentido, o papel das consultorias e escritórios especializados é o de catalisar e sustentar um processo que, por sua natureza, precisa ser apropriado de dentro para fora — e não imposto de fora para dentro.

6. Riscos jurídicos, operacionais e reputacionais

A ausência ou a ineficácia de um Programa de Compliance não é apenas uma lacuna de gestão — é uma exposição concreta e multidimensional a riscos que podem comprometer de forma irreversível a sustentabilidade de uma organização. Esses riscos se distribuem em três dimensões que, embora analiticamente distintas, estão profundamente interligadas na prática: a jurídica, a operacional e a reputacional. Um risco jurídico que se materializa em processo administrativo ou ação judicial quase invariavelmente gera repercussão reputacional; uma falha operacional não detectada pode evoluir para uma irregularidade com consequências jurídicas graves; e um dano reputacional severo frequentemente desencadeia investigações que expõem vulnerabilidades operacionais e jurídicas até então latentes. Compreender essa interdependência é condição indispensável para que as lideranças organizacionais atribuam ao Programa de Compliance o peso estratégico que ele merece — e não o tratem como mera formalidade regulatória.

No plano jurídico, o marco normativo brasileiro é inequívoco. A Lei nº 12.846/2013, conhecida como Lei Anticorrupção, introduziu no ordenamento jurídico brasileiro a responsabilidade objetiva das pessoas jurídicas por atos lesivos praticados contra a Administração Pública, nacional ou estrangeira. Isso significa que a organização pode ser responsabilizada independentemente de dolo ou culpa, bastando que o ato lesivo tenha sido praticado em seu interesse ou benefício, exclusivo ou não. As sanções previstas são severas. No plano administrativo, o artigo 6º da lei prevê multa que pode alcançar até 20% do faturamento bruto do exercício anterior ao da instauração do processo, excluídos os tributos, e nunca inferior à vantagem auferida, quando estimável, além da publicação extraordinária da decisão condenatória. No plano judicial, o artigo 19º da mesma lei autoriza a propositura de ação pela Advocacia-Geral da União ou pelos órgãos de representação judicial dos entes federativos, que pode resultar, nos casos mais graves, na dissolução compulsória da pessoa jurídica e na proibição de receber incentivos, subsídios, subvenções, doações ou empréstimos de órgãos e entidades públicos. O Decreto nº 11.129/2022, que revogou o Decreto nº 8.420/2015 e regulamenta a Lei nº 12.846/2013, estabelece os parâmetros para avaliação dos Programas de Integridade e determina que a comprovação da existência e aplicação de um programa robusto no momento da ocorrência da infração pode resultar na redução de até 5% sobre a multa aplicável. Esse dado, por si só, evidencia que a ausência ou a ineficácia do Programa não é uma omissão neutra: ela configura um risco jurídico concreto e mensurável, com reflexos diretos na dosimetria das sanções administrativas.

No plano estadual, e de especial relevância para o contexto fluminense abordado nesta seção, a Lei nº 7.753/2017 do Estado do Rio de Janeiro estabelece a obrigatoriedade de Programa de Integridade para empresas que contratam com a Administração Pública estadual em valores acima do limite legal, incluindo, entre seus parâmetros de avaliação, as ações comprovadas de promoção da cultura ética, conforme já mencionado no tópico 2 desta seção. Essa exigência reforça, no âmbito regional, a exposição jurídica das organizações que negligenciam a dimensão comunicativa e educativa de seus programas, e evidencia que o argumento desta seção não se move apenas no campo das recomendações estratégicas, mas também no das obrigações legais aplicáveis a parcela significativa das empresas pesquisadas.

No plano operacional, os riscos se manifestam de forma mais silenciosa, mas igualmente danosa. A ausência de controles internos robustos, de processos claros de gestão de riscos e de mecanismos eficazes de detecção e prevenção de desvios cria um ambiente propício a fraudes, desperdícios, falhas contratuais e irregularidades que, muitas vezes, só se tornam visíveis quando já causaram prejuízos significativos. As Diretrizes para Empresas Privadas da CGU (2015) identificam os riscos operacionais como aqueles relacionados à ineficiência de processos, a falhas de controles internos e à exposição a condutas irregulares que comprometem a integridade das operações da organização. O *framework* COSO, em sua versão atualizada de 2017 — "Enterprise Risk Management: Integrating with Strategy and Performance" —, reforça essa perspectiva ao distinguir o risco inerente, presente antes da adoção de controles, do risco residual, que persiste mesmo após sua implementação, sinalizando que a

gestão de riscos operacionais é um processo dinâmico e contínuo, e não um estado estático a ser alcançado.

No plano reputacional, os riscos são talvez os mais difíceis de quantificar, mas frequentemente os mais duradouros em suas consequências. Escândalos de compliance — especialmente aqueles que envolvem corrupção, assédio, fraude contábil ou violações de privacidade — tendem a gerar danos que extrapolam amplamente os limites da penalidade formal imposta. A credibilidade de uma organização perante seus clientes, parceiros comerciais, investidores, colaboradores e a sociedade em geral é um ativo construído ao longo de anos e que pode ser destruído em questão de dias. A CGU, em suas Diretrizes de 2015, reconhece expressamente essa dimensão ao incluir, entre os riscos decorrentes da ausência de um Programa de Compliance efetivo, os danos à imagem institucional da organização e a deterioração de suas relações com *stakeholders*. Em um ambiente de negócios cada vez mais orientado por critérios ESG — ambientais, sociais e de governança —, a reputação em matéria de integridade tornou-se também um fator determinante na atração de investimentos, na celebração de parcerias e no acesso a mercados.

Conclusão — Recomendações práticas para as organizações

Ao longo desta seção, o argumento central que emergiu de cada tópico pode ser resumido em uma constatação simples, mas de consequências profundas: comunicação e educação não são acessórios de um Programa de Compliance — são sua espinha dorsal. Sem elas, políticas bem redigidas permanecem documentos sem vida, treinamentos se tornam rituais esvaziados e os valores que a organização declara professar nunca chegam a orientar, de fato, o comportamento cotidiano de seus colaboradores. Tratá-las como investimentos estratégicos — e não como custos administrativos ou obrigações regulatórias — é o primeiro movimento que distingue as organizações que constroem cultura de integridade genuína daquelas que apenas simulam conformidade.

Esse movimento, contudo, não pode ser delegado. A primeira e mais urgente das recomendações práticas que esta seção autoriza formular é dirigida diretamente à alta liderança: nenhuma das iniciativas aqui discutidas produzirá efeito duradouro se a cúpula da organização não as incorporar como prioridade efetiva de gestão. Não basta patrocinar formalmente o Programa — é preciso praticá-lo visivelmente, comunicá-lo com autenticidade e responder por ele com responsabilidade. Como demonstrado nos tópicos anteriores, o chamado *tone at the top* não é uma metáfora inspiracional; é um mecanismo concreto de influência sobre o comportamento organizacional, e sua ausência é percebida pelos colaboradores com uma precisão que nenhuma pesquisa de clima precisa confirmar.

É nesse ponto que a heterogeneidade do tecido empresarial brasileiro precisa ser reconhecida. Os dados da Firjan revelam estágios muito distintos de maturidade: há organizações que já dispõem de programas estruturados, mas que ainda carecem de iniciativas consistentes de educação ética. Entre aquelas que já internalizaram ao menos parte das boas práticas de integridade, apenas 29,8% efetivamente implementaram projetos educativos nessa área. Há aquelas em fase de planejamento, que ainda precisam construir os fundamentos do Programa antes de pensar em comunicação e treinamento. E há as que sequer reconhecem a necessidade de um programa formal. Para cada um desses estágios, o peso e a urgência das recomendações a seguir são diferentes, mas sua direção é a mesma.

Inserir comunicação e treinamento no planejamento estratégico anual da organização é uma recomendação que, enunciada dessa forma, pode soar trivial. Mas sua relevância se torna evidente quando se considera que, na prática, essas iniciativas ainda são frequentemente tratadas como ações pontuais, acionadas em resposta a crises ou a exigências externas, e não como componentes permanentes da agenda organizacional. O planejamento anual é o instrumento pelo qual a organização declara suas prioridades reais — e enquanto comunica-

ção e educação ética não figurarem nele com recursos, prazos e responsáveis definidos, continuarão sendo intenções sem consequência.

A revisão periódica e contínua dos conteúdos de treinamento e comunicação é igualmente indispensável. Um programa que repete os mesmos materiais ano após ano ignora dois fatos fundamentais: que o ambiente de riscos da organização muda, e que colaboradores que já assistiram ao mesmo treinamento deixam de absorvê-lo com a atenção necessária. Como advertem Chen e Soltes — cuja crítica aos programas de compliance meramente formais percorre todo esta seção —, a mensuração da efetividade é o que transforma intenção em gestão. Definir indicadores capazes de capturar não apenas o volume de treinamentos realizados, mas a real compreensão e internalização dos valores éticos pela força de trabalho, é o que permite à organização distinguir o que está funcionando do que precisa ser revisto.

Envolver as lideranças intermediárias como educadores éticos — "*tone from the middle*" — é uma recomendação que complementa e amplifica as anteriores. Gerentes, supervisores e coordenadores são os interlocutores cotidianos dos colaboradores — são eles que, na prática, interpretam e traduzem os valores da organização nas situações concretas de trabalho. Capacitá-los não apenas para cumprir, mas para ensinar e exemplificar a conduta ética esperada, é multiplicar o alcance do Programa de forma orgânica e sustentável. O assessor externo, como discutido no tópico 5, pode desempenhar papel relevante nessa capacitação, mas o protagonismo precisa ser assumido pela própria organização.

O que esta seção buscou demonstrar, em síntese, é que integridade não se decreta — ela se constrói. E ela só se consolida quando é compreendida, praticada e repetida. *Compreendida*, porque os colaboradores precisam saber não apenas o que a organização proíbe, mas por que a ética importa e como ela se expressa nas decisões do dia a dia. *Praticada*, porque nenhum treinamento substitui o exemplo — especialmente o da liderança. E *repetida*, porque valores não se internalizam em uma única exposição: eles se formam pelo acúmulo de experiências, conversas, decisões e comportamentos ao longo do tempo.

As organizações que compreenderem isso — e que tratarem comunicação e educação ética não como etapas de um *checklist*, mas como dimensões permanentes de sua estratégia de gestão — construirão algo que nenhuma sanção pode comprar e nenhuma crise pode rapidamente destruir: uma cultura de integridade que resiste porque foi genuinamente internalizada. Em um ambiente regulatório crescentemente exigente, em um mercado cada vez mais atento aos critérios de governança e em uma sociedade que cobra das organizações coerência entre o que declaram e o que praticam, essa cultura não é apenas um diferencial ético — é uma vantagem estratégica.

Referências

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *ABNT NBR ISO 37301: sistemas de gestão de compliance — requisitos com orientações para uso.* Rio de Janeiro: ABNT, 2021.

BRASIL. Controladoria-Geral da União. *Programa de Integridade:* Diretrizes para Empresas Privadas. Volume II. Brasília: CGU, 2024. Disponível em: https://www.gov.br/cgu/pt-br/assuntos/etica-e-integridade/empresa-pro-etica. Acesso em: 15 maio 2026.

BRASIL. Controladoria-Geral da União. *Programa de Integridade:* Diretrizes para Empresas Privadas. Brasília: CGU, 2015. Disponível em: https://www.gov.br/cgu/pt-br/assuntos/etica-e-integridade/empresa-pro-etica/arquivos/diretrizes_integridade_privadas.pdf. Acesso em: 15 maio 2026.

BRASIL. Decreto nº 11.129, de 11 de julho de 2022. Regulamenta a Lei nº 12.846, de 1º de agosto de 2013. *Diário Oficial da União*: seção 1, Brasília, DF, 12 jul. 2022.

BRASIL. Lei nº 12.846, de 1º de agosto de 2013. Dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira. *Diário Oficial da União:* seção 1, Brasília, DF, 2 ago. 2013.

CHEN, Hui; SOLTES, Eugene. Why Compliance Programs Fail—and How to Fix Them: the Key to Success Is Better Measurement. *Harvard Business Review*, Boston, mar./abr. 2018. Disponível em: https://hbr.org/2018/03/why-compliance-programs-fail. Acesso em: 28 abr. 2026.

COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION (COSO). *Enterprise Risk Management:* Integrating with Strategy and Performance. Durham: COSO, 2017. Disponível em: https://www.coso.org/sitepages/enterprise-risk-management.aspx. Acesso em: 15 maio 2026.

FEDERAÇÃO DAS INDÚSTRIAS DO ESTADO DO RIO DE JANEIRO (FIRJAN). *Diagnóstico de políticas de governança e estratégias de integridade, compliance e proteção de dados pessoais.* Rio de Janeiro: Firjan, 2026.

KAPTEIN, Muel. Toward Effective Codes: Testing the Relationship with Unethical Behavior. *Journal of Business Ethics*, v. 99, n. 2, p. 233-251, 2011. DOI: 10.1007/s10551-010-0652-5.

PAGANI, Luana Palmieri França (coord.). *Compliance para o Sistema Indústria:* Teoria e Prática. Brasília, DF: Serviço Social da Indústria - Conselho Nacional, 2022. Disponível em: https://www.cnsesi.com.br/admin/data/dynamic/arquivos/100/downloads/4e6e1c4f748ff763c37233c9a02166ff.pdf. Acesso em: 30 abr. 2026.

PAINE, Lynn S. Managing for organizational integrity. *Harvard Business Review*, Boston, v. 72, n. 2, p. 106-117, mar./abr. 1994. Disponível em: https://hbr.org/1994/03/managing-for-organizational-integrity. Acesso em: 10 maio 2026.

RIO DE JANEIRO (Estado). *Lei nº 7.753, de 17 de outubro de 2017.* Dispõe sobre a instituição do Programa de Integridade nas empresas que contratam com a Administração Pública do Estado do Rio de Janeiro e dá outras providências. Diário Oficial do Estado do Rio de Janeiro, Rio de Janeiro, 18 out. 2017. Disponível em: https://alerjln1.alerj.rj.gov.br/contlei.nsf/c8aa0900025feef6032564ec0060dfff/0b110d0140b3d479832581c3005b82ad?OpenDocument&Highlight=0,7753. Acesso em: 01 set 2026.

UNITED NATIONS OFFICE ON DRUGS AND CRIME (UNODC). *An Anti-Corruption Ethics and Compliance Programme for Business:* a practical guide. New York: United Nations, 2013. Disponível em: https://www.unodc.org/documents/corruption/Publications/2013/13-84498_Ebook.pdf. Acesso em: 15 maio 2026.

UNITED STATES. Department of Justice. *Evaluation of Corporate Compliance Programs.* Washington: DOJ, 2024. Disponível em: https://www.justice.gov/criminal/criminal-fraud/page/file/937501/dl?inline=. Acesso em: 15 maio 2026.

Incentivos, recompensas e consequências:

o impacto do sistema de reconhecimento na cultura ética

Jéssica Corrêa Diniz da Silva

Jéssica Corrêa Diniz da Silva é gerente de Governança, Riscos & Compliance na Volkswagen Caminhões e Ônibus, tem 35 anos e conta com mais de 15 anos de experiência em Compliance e Gestão de Riscos. Possui sólida atuação fundamentada em SOX, COSO, auditoria, investigações e programas de integridade. Atua em ambientes corporativos complexos e altamente regulados, contribuindo para o fortalecimento dos frameworks de governança e para a mitigação de riscos. Lidera iniciativas estratégicas voltadas à cultura ética, conformidade regulatória e prevenção de riscos. Apresenta perfil analítico, visão sistêmica e foco consistente em resultados sustentáveis.

Introdução

A construção de uma cultura ética organizacional não se sustenta apenas por instrumentos formais, como códigos de conduta, políticas internas ou treinamentos periódicos. Embora essenciais, tais elementos possuem alcance limitado se não forem acompanhados de práticas concretas que orientem o comportamento no dia a dia da organização.

Nesse contexto, os sistemas de incentivos, recompensas e consequências assumem papel central. São eles que, na prática, influenciam decisões, prioridades e atitudes dos colaboradores, afetando diretamente a efetividade dos programas de compliance e integridade.

No ambiente regulatório brasileiro, é particularmente relevante que os mecanismos de reconhecimento estejam alinhados não apenas às exigências legais, mas também aos valores éticos que a organização declara adotar. Este artigo analisa como incentivos, recompensas e consequências impactam a cultura ética organizacional, a partir de fundamentos comportamentais consolidados e das principais referências nacionais e internacionais sobre o tema.

1. Fundamentos comportamentais

1.1 Reforço positivo, reforço negativo e punição

A lógica dos incentivos organizacionais encontra base na psicologia comportamental, especialmente nos estudos de B. F. Skinner (1953). De acordo com essa abordagem, o comportamento humano tende a se consolidar ou a ser desencorajado a partir das consequências que o seguem.

O reforço positivo ocorre quando um comportamento desejado é seguido por uma recompensa, aumentando a probabilidade de sua repetição. No ambiente corporativo, isso se traduz, por exemplo, em reconhecimento público, promoções, avaliações positivas de desempenho, premiações ou incentivos financeiros associados à conduta ética e à observância de políticas internas.

O reforço negativo, por sua vez, não se confunde com punição. Trata-se da retirada de estímulos indesejados após a adoção do comportamento esperado. Exemplos incluem a eliminação de verificações redundantes ou controles adicionais quando a avaliação de riscos indicar que tais medidas não são mais necessárias e os processos demonstrarem adequado nível de maturidade e conformidade. Ao eliminar um fator percebido como oneroso, esse mecanismo contribui para a manutenção do comportamento desejado ao longo do tempo.

Já a punição busca reduzir comportamentos inadequados por meio de consequências negativas, como advertências, suspensões ou desligamentos. Embora indispensável para a credibilidade dos programas de compliance, a literatura aponta que seu uso excessivo ou desproporcional pode gerar efeitos adversos, como medo, silêncio organizacional e ocultação de irregularidades (Skinner, 1953).

1.2 Motivação extrínseca e intrínseca

A Teoria da Autodeterminação, desenvolvida por Deci e Ryan (1985), amplia a análise ao diferenciar motivação extrínseca e motivação intrínseca. A motivação extrínseca ocorre quando o comportamento é impulsionado por fatores externos ao indivíduo, como recompensas, reconhecimento formal ou consequências associadas ao desempenho. Ela depende de estímulos externos oferecidos ou retirados pela organização.

Já a motivação intrínseca está relacionada ao interesse e à satisfação inerentes à própria atividade. A ação é realizada pelo prazer ou interesse gerado pela atividade em si. Em contraste, comportamentos motivados pela

percepção de importância, alinhamento com valores pessoais ou senso de propósito representam formas de motivação extrínseca internalizada, que ocupam posição intermediária no *continuum* da autodeterminação.

Essa distinção é particularmente relevante para os programas de compliance. Em geral, o cumprimento de regras, políticas e controles não decorre de motivação intrínseca em sentido estrito, mas da internalização de valores éticos e organizacionais, que passam a orientar o comportamento de forma voluntária e consistente, mesmo na ausência de supervisão direta.

2. O impacto do sistema de reconhecimento na cultura ética organizacional

No Brasil, a Lei nº 12.846/2013 reforça a importância de mecanismos efetivos de integridade ao considerar, entre outros fatores, a existência e efetividade dos programas de compliance na avaliação de responsabilização das pessoas jurídicas. Nesse contexto, sistemas de incentivos, reconhecimento e medidas disciplinares coerentes contribuem para a efetividade desses programas.

O sistema de reconhecimento exerce impacto direto e estruturante sobre a cultura ética organizacional, pois atua como um sinal concreto do que é efetivamente valorizado pela empresa. Mais do que discursos institucionais, são os critérios de reconhecimento e consequência que orientam decisões em situações de pressão, ambiguidade ou conflito de interesses.

Treviño, Weaver e Reynolds (2006) destacam que colaboradores interpretam a cultura ética a partir das chamadas "mensagens éticas", transmitidas pela organização no cotidiano, principalmente por meio dos sistemas formais de gestão, como avaliação de desempenho, remuneração variável, promoções e medidas disciplinares. Na prática, tais sistemas funcionam como sinais organizacionais que comunicam aos colaboradores quais comportamentos são efetivamente valorizados, tolerados ou rejeitados. Assim, quando o sistema de reconhecimento está desalinhado com os valores corporativos declarados pela organização, há risco significativo de normalização de desvios de conduta.

Já quando comportamentos como transparência, respeito às políticas e aos processos internos, adesão aos controles internos, reporte responsável de irregularidades, cooperação com auditorias e proteção de dados pessoais são reconhecidos, a organização comunica que a ética é parte integrante do conceito de desempenho.

2.1 Riscos de sistemas de reconhecimento mal estruturados

Sistemas de reconhecimento que priorizam exclusivamente metas financeiras ou operacionais, sem considerar os meios utilizados para alcançá-las, podem atuar como indutores de condutas antiéticas. A Organização para a Cooperação e Desenvolvimento Econômico (OCDE) recomenda que os sistemas de incentivos e medidas disciplinares sejam estruturados de forma a promover o cumprimento efetivo dos programas de integridade e evitar estímulos incompatíveis com padrões éticos e legais.

Pesquisas internacionais demonstram que pressões inadequadas por resultados e incentivos desalinhados podem aumentar significativamente o risco de condutas antiéticas e violações de compliance. Esses dados reforçam que sistemas de incentivos não são neutros: quando mal calibrados, tornam-se vetores estruturais de risco ético e legal.

Além disso, a ausência de consequências claras e proporcionais para violações compromete a credibilidade do Programa de Compliance. A percepção de impunidade — especialmente quando aplicada de forma seletiva — enfraquece a confiança organizacional e desestimula o comportamento ético.

2.2 O papel da liderança no sistema de reconhecimento

A liderança é elemento central na efetividade do sistema de reconhecimento. Líderes são agentes diretos de reforço comportamental, pois distribuem *feedbacks*, oportunidades, visibilidade e consequências. Esse fenômeno é amplamente identificado na literatura e na prática como *"Tone from the Top"*, conceito que traduz a influência concreta da liderança na formação do comportamento organizacional e da cultura de compliance.

Segundo Treviño e Brown (2004), líderes éticos não apenas comunicam padrões, mas os incorporam nas decisões de reconhecimento e punição, fortalecendo a percepção de justiça organizacional. Para programas de compliance, isso significa integrar critérios éticos às avaliações de desempenho e evitar recompensar resultados obtidos por meio de práticas incompatíveis com leis e políticas corporativas.

2.3 Sustentabilidade da cultura ética

A sustentabilidade da cultura ética depende da combinação entre incentivos formais e mecanismos que promovam a internalização dos valores éticos pelos colaboradores. Formas não financeiras de reconhecimento contribuem para que a ética seja percebida como parte integrante da identidade profissional e organizacional.

Ambientes que adotam essa abordagem tendem a apresentar maior segurança psicológica, facilitando o reporte de irregularidades e a prevenção de riscos relacionados à corrupção e outras infrações legais.

Além disso, reconhecimento e consequências não são mecanismos opostos, mas complementares. Um sistema ético eficaz combina reconhecimento consistente de condutas éticas, consequências claras, proporcionais e aplicadas de forma equânime e transparência nos critérios de decisão.

Esse equilíbrio reforça a previsibilidade organizacional e fortalece a credibilidade do Programa de Integridade perante colaboradores, reguladores e demais *stakeholders* e contribuem para a ética como valor organizacional e não apenas como obrigação regulatória.

A literatura também aponta que recompensas tangíveis e excessivamente vinculadas ao comportamento podem reduzir a motivação intrínseca em determinadas circunstâncias. Por essa razão, programas de reconhecimento ético devem ser cuidadosamente estruturados para reforçar valores organizacionais sem transformar a conduta ética em mera resposta instrumental a incentivos financeiros.

Conclusão

Os sistemas de incentivos, recompensas e consequências exercem influência decisiva sobre a cultura ética organizacional. Quando alinhados aos valores institucionais e às exigências legais, fortalecem o compliance e reduzem riscos. Quando mal estruturados, podem incentivar desvios e comprometer a integridade corporativa.

À luz da legislação brasileira e das melhores práticas internacionais, a construção de uma cultura ética sustentável exige equilíbrio entre reforços positivos, consequências justas e mecanismos que promovam a internalização dos valores éticos, tornando o comportamento íntegro parte natural do cotidiano organizacional.

Referências

BRASIL. Lei nº 12.846/2013 – Lei Anticorrupção. Dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira. *Diário Oficial da União*: seção 1, Brasília, DF, 2 ago. 2013.

DECI, E. L.; RYAN, R. M. *Intrinsic Motivation and Self-Determination in Human Behavior*. New York: Plenum Press, 1985.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD). *Recommendation of the Council for Further Combating Bribery of Foreign Public Officials in International Business Transactions*. Paris: OECD Publishing, 2021.

SKINNER, B. F. *Science and Human Behavior*. New York: Macmillan, 1953.

TREVIÑO, Linda K.; BROWN, Michael E. Managing to be ethical: debunking five business ethics myths. *Academy of Management Executive*, [*S. l.*], v. 18, n. 2, p. 69-81, 2004. DOI: https://doi.org/10.5465/ame.2004.13837400.

TREVIÑO, L. K.; WEAVER, G. R.; REYNOLDS, S. J. *Behavioral Ethics in Organizations:* A review. *Journal of Management*, [*S. l.*], v. 32, n. 6, p. 951-990, 2006. DOI: https://doi.org/10.1177/014920630629425.

Compliance e integridade:

do marco legal à consolidação de uma cultura ética nas organizações com ferramentas de mitigação de riscos e sustentabilidade

Carla Gonçalves Domingues

Carla Gonçalves Domingues é executiva com 32 anos de trajetória profissional com ênfase em auditoria interna, riscos, controles internos, compliance, Due Diligence, segurança da informação, com atuação nos setores de seguros, saúde, previdência, consórcio, capitalização. Atualmente está como Gerente de Monitoramento e Gestão de Riscos da CNI, SESI/DN, SENAI/DN e IEL/NC. É mestre em Direito pelo IDP, possui MBA em Auditoria pela FGV, é graduada em Ciências Contábeis e em Direito e especialista em Segurança em Redes de Computadores pela UCB. Sua sólida experiência em governança inclui a coordenação do Comitê de Auditoria Estatutário e a participação no Comitê de Pessoas, Elegibilidade, Sucessão e Remuneração da Valec (INFRA S.A.), além da participação como membro do Comitê do Pró-Ética da CGU e da Comissão de Estudo Especial de Gestão de Riscos da ABNT.

Introdução

O termo "compliance" remete à ideia de agir em conformidade e ao cumprimento de leis, regulamentos e normas. Muito embora o compliance seja um tema discutido há décadas no Brasil e, de alguma forma, esteja presente em várias organizações privadas, públicas, estatais e de economia mista no Brasil, somente no ano de 2013, com a edição da Lei nº 12.846/13, a chamada Lei Anticorrupção, ocorreu, de fato, uma mobilização e estruturação para combater a corrupção de forma mais efetiva nas organizações. Os órgãos de regulação e fiscalização ficaram mais atentos e exigentes, orientando e, em alguns casos, determinando que as organizações adotassem um Programa de Compliance e integridade, como forma de transmitir maior credibilidade à sociedade e implementar e/ou aprimorar normas já existentes, como códigos de conduta ética, políticas, canais de denúncia, mecanismos de gestão de riscos, monitoramento e treinamentos internos, contribuindo também para o desenvolvimento da cultura organizacional.

Diante das exigências, existem muitas críticas e desentendimentos em relação à efetividade dos programas de *compliance* e integridade, visto que, pelo "holofote" que foi dado ao tema, alguns presumem que as penas são negligenciadas e que existem limitações quanto à autonomia das áreas responsáveis em atuar dentro das organizações. Um dos principais pilares para que o programa tenha sucesso é o patrocínio da alta administração, pois, sem esse apoio, o programa fica desacreditado e "vazio".

Os programas de compliance e integridade não têm a premissa de eliminar todos os riscos, mas identificar, de forma preventiva, os riscos inerentes e propor controles adequados, com intuito de minimizar os possíveis gargalos e assim resguardar os valores da organização. Com isso, busca-se demonstrar ao corpo funcional e à sociedade maior credibilidade e um efetivo trabalho de combate à corrupção e às ilicitudes, comprovando a transparência, a ética e a moral.

De forma geral, é possível perceber a evolução do combate à corrupção no país quando resgatamos, há 28 anos, a Lei nº 9.613/1998, que dispõe sobre os crimes de lavagem de dinheiro ou ocultação de bens, direitos e valores; estabelece medidas de prevenção da utilização do sistema financeiro para os ilícitos previstos e cria o Conselho de Controle de Atividades Financeiras (COAF). Outro marco foi o lançamento, em 2009, pela Controladoria-Geral da União (CGU), em parceria com o Instituto Ethos de Empresas e Responsabilidade Social e o grupo de trabalho do Pacto Empresarial pela Integridade contra a Corrupção, do manual "A responsabilidade social das organizações no combate à corrupção", que abordou a integridade das organizações, com ênfase na transparência, na responsabilidade e nas boas práticas de mercado[1].

O conceito clássico de *compliance* utilizado nas organizações consiste em garantir a conformidade com padrões éticos, normativos internos e externos, leis e regulamentos, objetivando minimizar e evitar práticas ilegais, multas, litígios e danos à imagem da organização. Em outras palavras, o *compliance* é um conjunto de regras e procedimentos éticos e legais, e até preventivos, que definem e alinham o comportamento da organização, influenciando a conduta de seus colaboradores, desenvolvendo processos internos e mitigando riscos. É assegurar que as regras vigentes para as organizações e para os colaboradores sejam cumpridas e que eventuais infrações sejam descobertas e devidamente apuradas e punidas.

Embora o conceito de *compliance* pareça ser claro para muitos, é importante discutir o seu próprio significado, visto que há autores que apresentam interpretações conceituais diferentes, a depender da amplitude que se atribui ao termo *compliance*. Para a autora brasileira Débora Motta Cardoso, o compliance é uma ferramenta da governança corporativa, que abrange o controle interno, a auditoria e o compliance e está ligada ao estabelecimento de diretrizes e princípios gerais da administração

[1] CGU. *A responsabilidade social das empresas no combate à corrupção*. Brasília: CGU: Instituto Ethos de Empresas e responsabilidade social, 2009. 66 p. E-book. Disponível em: https://www.gov.br/cgu/pt-br/centrais-de-conteudo/publicacoes/integridade/arquivos/manualrespsocialempresas_baixa.pdf. Acesso em: 25 nov. 2024

das organizações, de maneira ampla[2]. O autor Leandro Sarcedo apresenta o *compliance* como um programa que cria, implanta e fiscaliza normas e procedimentos internos, com o objetivo de criar um comportamento ético e lícito na organização, distribuindo responsabilidades para os membros da organização[3].

Na prática, os principais objetivos do compliance são prevenção, detecção e correção. No que se refere ao aspecto preventivo, o compliance busca prevenir infrações e mitigar os riscos legais e reputacionais aos quais a organização está sujeita caso essas infrações se concretizem. No que se refere ao aspecto detectivo, sua atuação se manifesta quando ocorre algum evento que demanda investigação interna, busca de evidência, preparação de eventual defesa perante autoridades regulatórias ou de aplicação da lei penal, assim como gestão do risco de escândalo que possa afetar a reputação da organização. As medidas corretivas são adotadas a partir dos ilícitos já revelados, cuja análise pode permitir a identificação de falhas e/ou da ausência de controles.

Considerando que um dos principais objetivos do compliance é o combate à corrupção, vale trazer aqui o conceito de corrupção, definida como "ato ou resultado de corromper, como a 'corruptela' (alteração). Alteração das características originais de algo, como adulteração. Degradação de valores morais ou dos costumes, associada à devassidão ou depravação. Ato ou efeito de subornar alguém, geralmente em busca de vantagens pessoais ou para terceiros. Uso de meios ilícitos, especialmente por servidores públicos, para obter informações sigilosas com o objetivo de conseguir benefícios"[4].

A evolução do compliance é marcada por uma transição de normas setoriais para um padrão global de integridade corporativa. Historicamente, um dos marcos iniciais foi a criação do Comitê da Basileia (1974), que visava à estabilidade financeira e supervisão bancária, inspirando, no Brasil, a Resolução nº 2.554/1998 do Banco Central, focada em controles internos. Contudo, a legislação considerada basilar para o compliance moderno é o Foreign Corrupt Practices Act (FCPA), de 1977, nos Estados Unidos, que proibiu o suborno de funcionários estrangeiros e impôs rígidos controles contábeis às corporações sob jurisdição americana. Posteriormente, com a promulgação das Federal Sentencing Guidelines for Organizations, em 1991, consolidou-se o entendimento de que a existência de programas de integridade efetivos poderia mitigar as sanções corporativas em até 95%. Contudo, a United States Sentencing Commission condiciona essa expressiva redução à imediata autocomunicação da irregularidade às autoridades competentes e ao não envolvimento da alta administração no ilícito.

No cenário internacional, a influência dessas diretrizes norte-americanas e de organismos como a Organização para a Cooperação e Desenvolvimento Econômico (OCDE) e a Organização das Nações Unidas (ONU) consolidou padrões globais que culminaram nas normas internacionais de padronização, com destaque para a ISO 37301, que substituiu a antiga recomendação da ISO 19600 para estabelecer os requisitos e as diretrizes de sistemas de gestão de compliance, de forma harmonizada com a ISO 37001 (sistema de gestão antissuborno). Em paralelo, países europeus também adaptaram seus ordenamentos: a Espanha (LO 1/2015) passou a isentar ou atenuar penas de empresas com programas eficazes; a Itália (Decreto nº 231/2001) buscou contornar vedações constitucionais para punir pessoas jurídicas; e o Reino Unido inovou com o UK Bribery Act de 2010 (em vigor a partir de 2011), tipificando de forma autônoma a omissão ou falha das organizações em prevenir o suborno. Na América Latina, Chile (Lei nº 20.393/2009) e Argentina (Lei nº 27.401/2017) seguiram a tendência de prever a responsabilidade penal corporativa com atenuantes para o compliance.

No Brasil, o grande divisor de águas foi a Lei nº 12.846/2013 (Lei Anticorrupção). Ela estabeleceu a responsabilidade objetiva (administrativa e civil) de empresas por atos lesivos à administração pública, prevendo multas de até 20% do faturamento bruto. A lei brasileira incentiva a autorregulação ao considerar a existência de mecanismos de integridade como fator atenuante na dosimetria das penas.

[2] CARDOSO, Débora Motta. *Criminal Compliance na perspectiva da Lei de Lavagem de Dinheiro*. São Paulo: LiberArs, 2015.

[3] SARCEDO, Leandro. *Compliance e responsabilidade penal da Pessoa Jurídica:* construção de um novo modelo de imputação baseado na culpabilidade corporativa, São Paulo: Editora Liber Ars, 2016.

[4] MICHELIS: Dicionário Brasileiro de Língua Portuguesa. São Paulo: Editora Melhoramentos, 2024. Disponível em: https://michaelis.uol.com.br/busca?id=we1w. Acesso em: 20 nov. 2024.

A regulamentação brasileira expandiu-se rapidamente para áreas específicas, trazendo a Lei nº 9.613/1998, que refere-se ao combate à lavagem de dinheiro e a criação do COAF; a Lei nº 13.303/2016 (Lei das Estatais), que exige governança e compliance para empresas públicas e de economia mista; a Lei nº 13.709/2018 (LGPD), que regula o tratamento de dados pessoais, gerando novos desafios de conformidade; e a Lei nº 14.133/2021 (Nova Lei de Licitações), que torna obrigatória a implementação de programas de integridade para empresas em contratos de grande vulto com o setor público.

Em suma, o compliance no Brasil evoluiu de uma prática restrita ao setor financeiro para um sistema robusto e multifacetado, essencial para a competitividade das organizações no mercado global e para a proteção contra riscos legais e reputacionais.

A finalidade central de um Programa de Compliance e integridade é garantir que a organização atue em conformidade com normas legais e internas, promovendo um ambiente transparente que previna, detecte e responda a condutas ilícitas. Para além da conformidade legal, a integridade foca no fortalecimento de uma cultura de honestidade e responsabilidade. Atualmente, esses programas são vistos como um diferencial competitivo essencial para empresas que buscam expansão internacional ou que interagem com o setor público, sendo muitas vezes uma exigência de mercado e de investidores.

A eficácia do programa depende da solidez de seus pilares fundamentais, que incluem o comprometimento da alta administração, a gestão de riscos, a criação de códigos de conduta, canais de denúncia seguros e treinamentos contínuos. Recentemente, as organizações têm integrado também o pilar ESG (Ambiental, Social e Governança) ao *compliance* para alinhar a conformidade aos compromissos de sustentabilidade e responsabilidade social. O processo de implementação exige um mapeamento detalhado das vulnerabilidades da empresa, seguido da criação de políticas que reflitam seus valores éticos. Os principais desafios para o sucesso dessa estrutura são a resistência cultural interna, a necessidade de investimentos em tecnologia e a manutenção de uma auditoria independente que garanta a melhoria contínua dos processos.

A função do Compliance Officer (CO) é complexa: esse profissional atua como o guardião dos padrões de comportamento da organização. No Brasil, a ausência de regulamentação específica que delimite sua responsabilidade jurídica ou o proteja de determinadas responsabilizações gera insegurança jurídica. No âmbito penal, a imputação de responsabilidade por omissão imprópria ao CO (sob a figura de garantidor prevista no artigo 13, § 2º, do Código Penal) não é automática. Essa responsabilidade criminal depende estritamente das atribuições fáticas e contratuais assumidas pelo profissional de maneira concreta na governança da corporação, bem como de sua possibilidade real e efetiva de agir para evitar a consumação do ilícito no caso concreto.

Na esfera trabalhista, o CO pode responder por práticas abusivas ou discriminatórias durante processos de Due Diligence e Background Check. Para mitigar esses riscos, é essencial que a organização estabeleça uma descrição detalhada das funções em contrato e garanta ao profissional total autonomia e independência, com acesso direto à alta gestão ou ao conselho de administração. Além disso, a adoção de boas práticas documentadas e a contratação de seguros de responsabilidade civil são mecanismos recomendados para proteger o profissional contra responsabilizações injustas. Embora a condenação penal direta de *compliance officers* ainda seja rara na jurisprudência brasileira, determinados julgados frequentemente fundamentam as discussões doutrinárias sobre a responsabilidade por omissão. É imperativo pontuar, contudo, que, no julgamento da Ação Penal 470 (caso Mensalão) pelo Supremo Tribunal Federal, não estava formalmente em questão a figura do Compliance Officer. As condenações de dirigentes da instituição financeira por condutas omissivas deram-se em virtude de suas posições estatutárias de comando, amparadas pela teoria da cegueira deliberada (*willful blindness*). Desse modo, constata-se que a jurisprudência brasileira ainda carece de um precedente consolidado e específico sobre a responsabilidade pessoal do CO por atos de omissão na supervisão corporativa, o que confere maior precisão e tecnicidade à análise jurídica do tema.

No âmbito da governança corporativa, a Due Diligence de Integridade (DDI) e o Background Check são pilares que, embora complementares, possuem escopos distintos. A DDI é um processo investigativo amplo, voltado à avaliação de risco no contexto corporativo, como fusões, aquisições e contratação de fornecedores, visando assegurar que parceiros atendam aos padrões éticos e de conformidade. Já o Background Check foca na verifica-

ção específica sobre informações de indivíduos (conexões políticas, criminais e profissionais), sendo comumente aplicado em processos de recrutamento para cargos estratégicos ou de confiança.

A aplicação dessas ferramentas fundamenta-se na Lei Anticorrupção (Lei nº 12.846/2013) e no Decreto nº 11.129/2022, que incentivam a adoção de programas de integridade como fator atenuante de sanções. Contudo, a execução deve observar rigorosamente a LGPD (Lei nº 13.709/2018), exigindo uma base legal adequada (como legítimo interesse ou cumprimento de obrigação legal) e o respeito aos princípios da finalidade e necessidade, coletando apenas os dados estritamente essenciais para a avaliação de risco. Normas internacionais como a ISO 37001 (Sistema de Gestão Antissuborno) na sua nova versão de 2025, e a ISO 37301 (Sistema de Gestão de Compliance), estabelecida em 2021, também servem como guias para estruturar esses processos de forma técnica e segura.

A gestão de riscos por meio de Due Diligence e Background Check oferece oito benefícios centrais para a sustentabilidade organizacional: prevenção de fraudes e corrupção; tomada de decisão baseada em dados concretos; conformidade regulamentar; proteção da reputação corporativa; redução de riscos financeiros; aumento da eficiência operacional; valorização do capital humano; melhoria na relação com *stakeholders*. A implementação eficaz exige passos metódicos, iniciando pelo mapeamento de riscos e pela criação de uma matriz de riscos, que permite priorizar ações mitigadoras conforme a probabilidade e o impacto de eventos adversos.

No campo das contratações públicas, embora a Lei nº 14.133/2021 não mencione expressamente a obrigatoriedade específica dos institutos da DDI e do Background Check, a fundamentação jurídica de tais deveres operacionais é extraída com precisão do artigo 57, inciso XIII, do Decreto Federal nº 11.129/2022. Esse normativo regulamentador exige expressamente a aplicação de diligências apropriadas para a contratação e supervisão de terceiros, englobando doações, patrocínios e o monitoramento de pessoas expostas politicamente (PEPs), consolidando tais rotinas como indispensáveis nas contratações públicas de elevado risco. No que tange às contratações trabalhistas, o Tribunal Superior do Trabalho (TST) consolidou o entendimento, por meio do IRR 243000-58.2013.5.13.0023, de que a exigência de antecedentes criminais em *background checks* só é lícita quando justificada pela natureza da atividade (como manuseio de dados sigilosos, armas ou valores), sob pena de configurar discriminação e gerar direito à reparação por dano moral.

Alinhando-se a essa diretriz protetiva, o Supremo Tribunal Federal (STF), no julgamento do Recurso Extraordinário (RE) 560.900 (Tema 22 da Repercussão Geral), fixou a tese de que a existência de inquéritos policiais ou de ações penais em andamento, sem trânsito em julgado, não constitui fundamento idôneo para a eliminação de candidatos em processos seletivos. Esse entendimento constitucional dialoga de forma harmônica com a tese restritiva adotada pelo TST, reforçando os limites éticos e legais do Background Check admissional e vedando o uso de dados criminais não definitivos como fator de exclusão sumária e discriminatória de candidatos.

As melhores práticas de integridade corporativa exigem que a DDI operacionalize uma triagem minuciosa em cadastros públicos nacionais e estrangeiros. Na esfera nacional, destaca-se a verificação eletrônica sistemática perante o Cadastro de Empresas Inidôneas e Suspensas (CEIS) e o Cadastro Nacional de Empresas Punidas (CNEP), ambos administrados pela Controladoria-Geral da União (CGU). Complementarmente, a governança de riscos reputacionais estende essa análise a bases de dados internacionais de restrições comerciais e financeiras, tais como as listas de sanções consolidadas do Conselho de Segurança da ONU, a lista da Office of Foreign Assets Control (OFAC) dos Estados Unidos, mídia negativa e histórico público. Esse mapeamento corporativo correlaciona-se ao monitoramento de Pessoas Expostas Politicamente (PEPs) — cuja identificação é parametrizada no ordenamento jurídico brasileiro pela Resolução COAF nº 40/2021 e pela Circular Bacen nº 3.978/2020. Sob tais diplomas, a condição de PEP estende-se por cinco anos após o encerramento do exercício de funções públicas relevantes, alcançando igualmente cônjuges, companheiros, parentes até o segundo grau e colaboradores de estreito relacionamento ("PEPs relacionados"), demandando das organizações a imposição de procedimentos adicionais de diligência e supervisão financeira proporcional ao risco.

No âmbito procedimental das análises de integridade, a autodeclaração consubstancia-se como o marco inicial dos processos de cadastramento e de triagem de

riscos de lavagem de dinheiro, corrupção e conflitos de interesse. Sob as diretrizes regulatórias nacionais — a exemplo da Circular do Banco Central do Brasil (BCB) nº 3.978/2020 e da Resolução COAF nº 40/2021 —, a coleta de fichas e questionários declaratórios assinados pelo titular é qualificada como etapa formal e obrigatória para fins de Know Your Customer (KYC) e Know Your Partner (KYP). Essa prática visa assegurar que o próprio indivíduo preste informações preliminares a respeito de sua qualificação patrimonial, da estrutura de seus beneficiários finais e de seu enquadramento na categoria de PEP. Trata-se de um instrumento basilar que fomenta o princípio da boa-fé objetiva e estabelece a responsabilidade inicial do declarante quanto à fidedignidade dos dados reportados à organização.

Contudo, as normas regulatórias e a jurisprudência administrativa dos órgãos de controle são peremptórias ao determinar que a autodeclaração não possui o condão de eximir a instituição do dever de realizar averiguações independentes. Observada à luz das melhores práticas de mercado e do dever de diligência mitigadora, a autodeclaração atua como mero filtro inicial, cujo teor deve ser obrigatoriamente cruzado, confrontado e corroborado com evidências documentadas de fontes externas e bases de dados de inteligência independentes. Esse modelo híbrido — que integra o relato subjetivo do titular à auditoria objetiva do controlador — garante o alinhamento com os preceitos de conformidade e repele tentativas de ocultação patrimonial ou fraude regulatória.

No tocante ao tratamento de dados pessoais exigido por essas rotinas investigativas de Background Check, a observância dos ditames da Lei Geral de Proteção de Dados (LGPD) impõe severas restrições metodológicas ao controlador. Quando a base legal para o processamento de dados não residir em uma obrigação regulatória explícita, mas sim no legítimo interesse da organização (artigo 7º, inciso IX, da Lei nº 13.709/2018), revela-se mandatória a elaboração do Teste de Legítimo Interesse (LIA — Legitimate Interest Assessment). Conforme as orientações da Autoridade Nacional de Proteção de Dados (ANPD), o LIA deve se estruturar rigorosamente em quatro fases de balanceamento: a aferição da legitimidade do interesse da organização (que deve ser lícito e concreto, como a prevenção a fraudes); a demonstração da necessidade e proporcionalidade estrita do tratamento (garantindo que não haja meio menos intrusivo); o teste de balanceamento propriamente dito, que considera as expectativas legítimas de privacidade do titular frente aos interesses do controlador; e, finalmente, o estabelecimento de salvaguardas contratuais e técnicas robustas (incluindo o canal para o exercício do direito de oposição e a exclusão imediata de dados desnecessários), neutralizando potenciais riscos de danos morais trabalhistas decorrentes de checagens abusivas e garantindo-se a proporcionalidade, a segurança e a conformidade ética de todo o fluxo investigativo.

Conclusão

A análise dos marcos legais e das práticas de integridade no Brasil revela que o *compliance* deixou de ser uma opção administrativa para se tornar um imperativo estratégico e de sobrevivência para as organizações privadas. O divisor de águas estabelecido pela Lei Anticorrupção (Lei nº 12.846/13) não apenas endureceu as sanções, mas inaugurou uma era em que a autorregulação e a ética institucional são valorizadas como ativos tangíveis perante o mercado e o Estado.

A implementação eficaz desses programas, contudo, transcende a mera existência de manuais e códigos de conduta. Conforme evidenciado, o sucesso de qualquer estrutura de conformidade repousa sobre o comprometimento genuíno da alta administração; sem o exemplo da liderança, o programa torna-se "vazio" e incapaz de sustentar uma cultura de integridade. Como bem ilustram os casos de insucesso de grandes corporações, a estratégia mais sofisticada sucumbe diante de uma cultura organizacional permissiva.

No campo da gestão de riscos, ferramentas como a Due Diligence de Integridade (DDI) e o Background Check consolidaram-se como instrumentos indispensáveis de prevenção. Todavia, sua aplicação exige um equilíbrio delicado entre o dever de investigar e o respeito a direitos fundamentais, como a privacidade (LGPD) e a dignidade do trabalhador (CLT). O Judiciário brasileiro, em especial o TST (no IRR 243000-58.2013.5.13.0023) e o STF (no RE 560.900), tem sinalizado que a busca pela

integridade não autoriza práticas indiscriminadas ou discriminatórias, exigindo proporcionalidade e justificativa técnica em cada verificação.

Quanto ao papel do Compliance Officer, o cenário atual apresenta um paradoxo: ao mesmo tempo em que esse profissional é o guardião dos padrões éticos, ele enfrenta uma insegurança jurídica considerável devido à ausência de regulamentação que limite sua responsabilidade penal e administrativa. A mitigação desse risco pessoal passa obrigatoriamente pela definição clara de atribuições contratuais e pela garantia de autonomia funcional dentro da governança corporativa.

O *compliance* e a integridade devem ser entendidos como processos dinâmicos e em constante evolução, consolidando-se como um diferencial competitivo e uma exigência para a sustentabilidade das empresas no comércio global. O sucesso a longo prazo depende não apenas do cumprimento de normas, mas do fortalecimento de uma cultura organizacional que valorize a transparência e a responsabilidade social. O monitoramento contínuo e a adaptação às novas tecnologias, como a inteligência artificial, integradas aos critérios ESG, são os próximos passos para a evolução desses programas no Brasil, onde a integridade passa a ser o pilar central da reputação e da sustentabilidade.

Referências

ANDRADE, A. Compliance no Brasil: Uma análise da legislação e da adoção por organizações de capital aberto. *Revista de Administração de Organizações*, v. 53, n. 6, 2013.

ANDRADE, Adriana; ROSSETTI, José Paschoal. *Governança Corporativa:* Fundamentos, Desenvolvimento e Tendências. 7. ed. São Paulo: Atlas, 2014.

ARAUJO, Marcelo Azambuja. *Investigações Empresariais*. São Paulo: LiberArs, 2019.

ARROYO ZAPATERO, Luis Alberto; NIETO MARTÍN, Adán (org.). *El Derecho Penal Económico en la Era Compliance*. Valencia: Tirant lo Blanch, 2013.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). *ABNT NBR ISO 37301:* Sistemas de gestão de compliance - Requisitos com orientações para uso. Rio de Janeiro: ABNT, 2021.

BATALHA, Sara Costa Cunha. *A responsabilidade pré-contratual por violação dos deveres de boa-fé:* a importância de uma due diligence. 2019. Dissertação (Mestrado em Direito) – Faculdade de Direito, Universidade de Lisboa, Lisboa, 2019.

BENTIVEGNA, Carlos Frederico Barbosa. *Liberdade de expressão, honra, imagem e privacidade:* os limites entre o lícito e o ilícito. Santana de Parnaíba: Manole, 2020.

BRASIL. *Decreto-Lei nº 2.848, de 7 de dezembro de 1940*. Código Penal. Brasília, DF: Presidência da República, 1940. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 18 out. 2026.

BRASIL. *Decreto-Lei nº 5.452, de 1º de maio de 1943.* Aprova a Consolidação das Leis do Trabalho. Brasília, DF: Presidência da República, 1943. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del5452compilado.htm. Acesso em: 18 out. 2026.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Brasília, DF: Presidência da República, 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709compilado.htm. Acesso em: 18 out. 2026.

BRASIL. *Decreto nº 11.129, de 11 de julho de 2022.* Regulamenta a Lei nº 12.846, de 1º de agosto de 2013, que dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira. Brasília, DF: Presidência da República, 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/decreto/d11129.htm. Acesso em: 18 out. 2026.

BRASIL. Banco Central do Brasil. *Circular nº 3.978, de 23 de janeiro de 2020.* Dispõe sobre a política, os procedimentos e os controles internos a serem adotados pelas instituições autorizadas a funcionar pelo Banco Central do Brasil visando à prevenção da utilização do sistema financeiro para a prática dos crimes de "lavagem" ou ocultação de bens, direitos e valores, de que trata a Lei nº 9.613, de 3 de março de 1998, e de financiamento do terrorismo, previsto na Lei nº 13.260, de 16 de março de 2016. Brasília, DF: Banco Central do Brasil, 2020. Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/buscanormas?tema=27. Acesso em: 18 out. 2026.

BRASIL. Conselho de Controle de Atividades Financeiras. *Resolução Coaf nº 40, de 22 de novembro de 2021.* Dispõe sobre os procedimentos a serem observados, em relação a pessoas expostas politicamente, por aqueles que se sujeitam à supervisão do Conselho de Controle de Atividades Financeiras (Coaf) na forma do § 1º do art. 14 da Lei nº 9.613, de 3 de março de 1998, e revoga a Resolução nº 29, de 7 de dezembro de 2017. Brasília, DF: Conselho de Controle de Atividades Financeiras, 2021. Disponível em: https://www.gov.br/coaf/pt-br/acesso-a-informacao/Institucional/a-atividade-de-supervisao/regulacao/supervisao/normas-1/resolucao-coaf-no-40-de-22-de-novembro-de-2021. Acesso em: 18 out. 2026.

BRASIL. *Lei nº 12.376, de 30 de dezembro de 2010.* Altera a ementa do Decreto-Lei nº 4.657, de 4 de setembro de 1942, ampliando o seu campo de aplicação. Brasília, DF: Presidência da República, 2010. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2007-2010/2010/lei/l12376.htm. Acesso em: 18 out. 2026.

BRASIL. *Lei nº 12.683, de 9 de julho de 2012.* Altera a Lei nº 9.613, de 3 de março de 1998, para tornar mais eficiente a persecução penal dos crimes de lavagem de dinheiro. Brasília, DF: Presidência da República, 2012. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12683.htm. Acesso em: 18 out. 2026.

BRASIL. *Lei nº 12.846, de 1º de agosto de 2013.* Dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira, e dá outras providências. Brasília, DF: Presidência da República, 2013. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12846.htm. Acesso em: 18 out. 2026.

BRASIL. *Lei nº 13.303, de 30 de junho de 2016.* Dispõe sobre o estatuto jurídico da empresa pública, da sociedade de economia mista e de suas subsidiárias, no âmbito da União, dos Estados, do Distrito Federal e dos Municípios. Brasília, DF: Presidência da República, 2016. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/lei/l13303.htm. Acesso em: 18 out. 2026.

BRASIL. *Lei nº 14.133, de 1º de abril de 2021.* Lei de Licitações e Contratos Administrativos. Brasília, DF: Presidência da República, 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14133.htm. Acesso em: 18 out. 2026.

BRASIL. *Lei nº 9.613, de 3 de março de 1998.* Dispõe sobre os crimes de "lavagem" ou ocultação de bens, direitos e valores; a prevenção da utilização do sistema financeiro para os ilícitos previstos nesta Lei; cria o Conselho de Controle de Atividades Financeiras (Coaf) e dá outras providências. Brasília, DF: Presidência da República, 1998. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9613compilado.htm. Acesso em: 18 out. 2026.

BRASIL. *Lei nº 13.608, de 10 de janeiro de 2018.* Dispõe sobre o serviço telefônico de recebimento de denúncias e sobre recompensa por informações que auxiliem nas investigações policiais; e altera o art. 4º da Lei nº 10.201, de 14 de fevereiro de 2001, para prover recursos do Fundo Nacional de Segurança Pública para esses fins. Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13608.htm. Acesso em: 18 out. 2026.

BRASIL. *Lei nº 8.078, de 11 de setembro de 1990.* Dispõe sobre a proteção do consumidor e dá outras providências. Brasília, DF: Presidência da República, 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 18 out. 2026.

CARDOSO, Débora Motta. *Criminal Compliance na perspectiva da Lei de Lavagem de Dinheiro*. São Paulo: LiberArs, 2015.

COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION (COSO). *Compliance risk management:* applying the COSO ERM framework. Durham: COSO, 2020.

CONTROLADORIA-GERAL DA UNIÃO (CGU). *Programa de integridade:* diretrizes para empresas privadas. Brasília: CGU, 2015.

COSTA, Henrique. *Compliance*: A nova regra do jogo. *Revista de Administração de Organizações*, v. 56, n. 3, 2016.

CRESCENTE, Paula Scarpari Carlini. *Breves considerações a respeito da Lei nº 12.846/2013 e sua relação com os contratos privados.* 2017. Monografia (Pós-graduação lato sensu em Direito) – Insper, São Paulo, 2017.

DOMINGUES, Carla Gonçalves. *Due diligence de integridade e background check como ferramentas estratégicas na prevenção de ilícitos empresariais.* 2024. Dissertação (Mestrado Profissional em Direito) – Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa, Brasília, 2024.

ESTELLITA, Heloisa. *Responsabilidade penal de dirigentes de empresas por omissão:* estudo sobre a responsabilidade omissiva imprópria de dirigentes de sociedades anônimas, limitadas e encarregados de cumprimento por crimes praticados por membros da empresa. São Paulo: Marcial Pons, 2017.

FACCINI NETO, Orlando; SÁ, Getúlio Humberto Barbosa de. Job description e *compliance* no Direito Penal Empresarial. *Revista Magister de Direito Penal e Processual Penal*, Porto Alegre, v. 17, n. 97, p. 105-120, 2020. Disponível em: https://www.tjdft.jus.br/institucional/biblioteca/conteudo-revistas-juridicas/revista-magister-de-direito-penal-e-processual-penal/2020-v-17-n-97-ago-set. Acesso em: 18 out. 2026.

FAGUNDES, M. *Compliance e Governança Corporativa*. São Paulo: Editora Atlas, 2018.

GARCIA, Luis. *Due Diligence: Direito das Sociedades*. São Paulo: Editora Saraiva, 2017.

GOMES, João. *Compliance no Brasil: Teoria e Prática*. São Paulo: Revista dos Tribunais, 2016.

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA (IBGC). *Código das melhores práticas de governança corporativa*. 5. ed. São Paulo: IBGC, 2015.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). *ISO 31000:2018:* risk management – guidelines. Geneva: ISO, 2018. Disponível em: https://www.iso.org/standard/31000. Acesso em: 18 out. 2026.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). *ISO 37001:2025:* anti-bribery management systems – requirements with guidance for use. Geneva: ISO, 2025. Disponível em: https://www.iso.org/standard/37001. Acesso em: 18 out. 2026.

LIEBL, Helena; SANTOS, Rafael Padilha dos. *Compliance* e governança corporativa: estratégias para uma gestão socioambiental. *Revista de Ciências Jurídicas e Sociais da UNIPAR*, v. 23, n. 1, p. 129-142, 2020. DOI: https://doi.org/10.25110/rcjs.v23i1.2020.8259.

MARTINS, G. *Corrupção: prevenção e combate à corrupção em organizações*. Saraiva, 2018.

ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO (OCDE). *Guia da OCDE de devida diligência para uma conduta empresarial responsável.* Paris: OECD Publishing, 2018. DOI: https://doi.org/10.1787/de-16420f-pt.

PALMA, Maria Fernanda; DIAS, Augusto Silva; MENDES, Paulo de Sousa (coord.). *Estudos sobre Law Enforcement, Compliance e Direito Penal*. 2. ed. Coimbra: Almedina, 2018.

PERES, João Roberto; BRIZOTI, Nilson. *Compliance:* corrupção e fraudes no mundo empresarial. São Paulo: Edição dos Autores, 2016.

PINOTTI, Maria Cristina (org.). *Corrupção:* Lava Jato e Mãos Limpas. São Paulo: Portfolio-Penguin, 2019.

SALGADO, Daniel de Resende; QUEIROZ, Ronaldo Pinheiro de; ARAS, Vladimir (coord.). *Corrupção:* aspectos sociológicos, criminológicos e jurídicos. Salvador: JusPodivm, 2020.

SARAIVA, Renata Machado. *Criminal compliance como instrumento de tutela ambiental*. São Paulo: LiberArs, 2018.

SARCEDO, Leandro. *Compliance e responsabilidade penal da pessoa jurídica:* construção de um novo modelo de imputação baseado na culpabilidade corporativa. São Paulo: LiberArs, 2016.

SCHÜTT, Júlia Flotes. *Desperdício do compliance penal no Brasil:* uma crítica à limitada responsabilidade penal da pessoa jurídica na legislação brasileira frente à experiência espanhola. São Paulo: Tirant lo Blanch, 2024.

SOUZA, Artur de Brito Gueiros. *Direito penal empresarial:* critérios de atribuição de responsabilidade e o papel do compliance. 2. ed. São Paulo: LiberArs, 2022.

SUPREMO TRIBUNAL FEDERAL (STF). *Ação Penal nº 470 (Mensalão)* e Recurso Extraordinário (RE) nº 650.900/DF (Tema 22 de Repercussão Geral).

TRIBUNAL DE CONTAS DA UNIÃO (TCU). *Acórdão 2622/2016 - Plenário* e *Programa Nacional de Prevenção à Corrupção (PNPC)*.

TRIBUNAL SUPERIOR DO TRABALHO (TST). *IRR 243000-58.2013.5.13.0023 (Antecedentes Criminais)* e Acórdãos nos processos *RR-176200-45.2013.5.13.0024* e *RR-17302-16.2013.5.16.0002*.

VASCONCELOS, Fernando. *Compliance: a excelência no cumprimento de normas e controles internos*. Elsevier, 2016.

VERÍSSIMO, Carla. *Compliance: incentivo à adoção de medidas anticorrupção*. 2. ed. Ed. Saraiva, 2018.

VIANA, Ana. *Corrupção: aspectos criminais e políticos*. São Paulo: JusPodivm, 2018.

ZENKNER, Marcelo. *Integridade governamental e eempresarial:* um espectro da repressão e da prevenção à corrupção no Brasil e em Portugal. Belo Horizonte: Fórum, 2019.

Capítulo 2

Governança: estruturas que sustentam a integridade corporativa

Cultura como infraestrutura da governança:

o que sustenta a integridade na prática

Roberta Codignoto

Roberta Codignoto é consultora e palestrante em compliance e integridade, com mais de 20 anos de experiência nos setores público e privado. Atua no desenvolvimento de culturas de integridade e no fortalecimento de programas de compliance. Foi conselheira da Comissão de Ética Pública da Presidência da República e membro independente do Comitê de Integridade da Petrobras. É autora e coautora de publicações sobre ética, governança e compliance e treinadora voluntária da Alliance for Integrity.

Introdução

As últimas décadas trouxeram avanços significativos na agenda de governança corporativa. Temas antes restritos a determinados fóruns especializados passaram a ocupar as agendas dos Conselhos de Administração e da alta liderança. A pauta ESG ganhou centralidade nas discussões estratégicas, programas de compliance e integridade tornaram-se mais robustos, canais de denúncia passaram a ser estruturados de forma mais independente e códigos de conduta foram progressivamente aprimorados. Matrizes de riscos, processos de *due diligence* de terceiros e sofisticados mecanismos de controle passaram a integrar a realidade de inúmeras organizações.

Paradoxalmente, escândalos corporativos continuam ocorrendo em empresas que, ao menos formalmente, possuíam todos esses mecanismos. Os casos amplamente divulgados demonstram que a existência de estruturas de governança, por si só, não é suficiente para impedir fraudes, desvios éticos ou decisões incompatíveis com os valores declarados pelas organizações.

A pergunta que emerge é inevitável: por que estruturas aparentemente sólidas falham justamente quando são mais necessárias?

A resposta pode estar em um elemento menos visível, porém decisivo: a cultura organizacional.

Embora frequentemente tratada como um conceito abstrato ou intangível, a cultura exerce influência concreta sobre a forma como decisões são tomadas, conflitos são administrados, denúncias são recebidas, riscos são reportados e consequências são aplicadas. Em outras palavras, a cultura determina se os mecanismos formais de governança serão efetivamente utilizados para proteger a integridade organizacional ou se permanecerão restritos ao campo das boas intenções e da conformidade documental.

As empresas não fracassam, em regra, por absoluta ausência de mecanismos de governança. Elas fracassam porque os mecanismos são ignorados, os desvios são racionalizados, o silêncio é recompensado, as metas superam os valores e as lideranças, muitas vezes, enviam mensagens contraditórias sobre aquilo que efetivamente importa. Em outras palavras, a cultura ocupa os espaços que as regras não conseguem alcançar.

A efetividade dos mecanismos de integridade depende da existência de um ambiente organizacional que legitime comportamentos éticos, favoreça o diálogo, estimule o questionamento responsável e sustente a coerência entre discurso e prática. Portanto, a cultura exerce um papel fundamental como infraestrutura da governança corporativa: não é a governança que cria integridade, mas sim a cultura que permite que a governança funcione.

A governança define o que deveria acontecer. A cultura determina o que realmente acontece.

1. Quando a governança existe, mas não funciona

A história recente oferece inúmeros exemplos de organizações que possuíam estruturas formais de governança e, ainda assim, enfrentaram graves crises de integridade. Escândalos corporativos envolvendo manipulação de demonstrações financeiras, fraudes, violações regulatórias e omissões deliberadas revelam que a simples existência de políticas, controles ou instâncias decisórias não garante sua efetividade.

O caso das Americanas reacendeu o debate sobre os limites das estruturas formais diante de ambientes organizacionais em que determinados comportamentos podem ser normalizados ao longo do tempo. Independentemente das responsabilidades individuais ainda discutidas em diferentes esferas, o episódio levantou questionamentos importantes sobre o funcionamento dos mecanismos de supervisão, o fluxo de informações, a qualidade do processo decisório e a disposição organizacional para questionar práticas estabelecidas.

Em âmbito internacional, o caso da Volkswagen, relacionado à manipulação de testes de emissões, e o escânda-

lo envolvendo a abertura de contas não autorizadas no Wells Fargo, evidenciaram como culturas excessivamente orientadas ao atingimento de metas, combinadas com baixa tolerância ao questionamento e reduzida abertura para a divergência, podem comprometer estruturas que, formalmente, pareciam adequadas.

O que aproxima esses casos não é a ausência de estruturas formais de governança. Em todos eles havia conselhos, políticas, processos de auditoria, sistemas de controle e mecanismos de compliance. O que se observou, contudo, foi a incapacidade de essas estruturas produzirem o comportamento esperado, seja pela normalização de determinadas práticas, pela pressão excessiva por resultados ou pela ausência de ambientes seguros para o questionamento e a divergência.

O problema, portanto, não estava apenas na governança formal, mas na cultura que determinava como essa governança era vivida na prática.

Esses exemplos não sugerem que mecanismos de governança sejam dispensáveis. Ao contrário, demonstram que sua efetividade depende de condições culturais que favoreçam sua utilização genuína.

A questão central deixa de ser apenas um *checklist* de quais estruturas existem e passa a ser um questionamento mais profundo sobre como essas estruturas são vivenciadas pelas pessoas que delas participam. O que é praticado? O que é tolerado? O que é recompensado? O que é ignorado? Essas talvez sejam algumas das perguntas mais relevantes para compreender a efetividade da governança.

2. A cultura como infraestrutura invisível da governança

Edgar Schein[1], uma das principais referências sobre cultura organizacional, define cultura como o conjunto de pressupostos básicos compartilhados por um grupo, aprendidos à medida que esse grupo resolve seus problemas de adaptação externa e integração interna.

Esses pressupostos influenciam a forma como as pessoas percebem, interpretam e respondem às situações cotidianas.

Na prática, a cultura manifesta-se por meio das decisões toleradas, dos comportamentos recompensados, das histórias contadas, das prioridades estabelecidas e dos desvios ignorados.

A análise da cultura também permite identificar um dos maiores riscos organizacionais: a distância entre os valores declarados e os comportamentos efetivamente vividos. Organizações podem afirmar possuir tolerância zero para determinadas práticas e, ao mesmo tempo, conviver com sistemas de incentivos inadequados, lideranças incoerentes ou ambientes pouco seguros para o questionamento. Nessas situações, a integridade deixa de ser um valor vivido e passa a ser apenas uma narrativa institucional. A cultura, portanto, revela menos aquilo que a organização diz ser e muito mais aquilo que ela efetivamente recompensa, tolera ou desencoraja[2].

Assim sendo, se a governança pode ser compreendida como a arquitetura formal que orienta o funcionamento da organização, a cultura representa a infraestrutura invisível que sustenta – ou fragiliza – essa arquitetura.

Da mesma forma que um edifício pode aparentar solidez enquanto suas fundações se deterioram silenciosamente, organizações podem exibir estruturas sofisticadas de governança sem que essas estruturas sejam efetivamente capazes de produzir integridade. A cultura é essa fundação invisível. Ela sustenta, enfraquece ou, em situações extremas, inviabiliza o funcionamento dos mecanismos formais.

[1] SCHEIN, Edgar H. *Organizational Culture and Leadership*. 5. ed. Hoboken: John Wiley & Sons, 2017. Edgar Schein é professor emérito da MIT Sloan School of Management e é reconhecido internacionalmente como um dos principais estudiosos da cultura organizacional.

[2] ALLIANCE FOR INTEGRITY; UN GLOBAL COMPACT NETWORK GERMANY; TRANSPARENCY INTERNATIONAL DEUTSCHLAND. *Practical guide for measuring integrity culture in companies*. [S. *l.*]: Alliance for Integrity; UN Global Compact Network Germany; Transparency International Deutschland, 2025.

A governança estabelece papéis, responsabilidades, controles e mecanismos de supervisão. A cultura, por sua vez, determina se as pessoas utilizarão essas estruturas com coragem, coerência e compromisso com a integridade.

É justamente nesse sentido que Olga Pontes, executiva com ampla experiência em governança e compliance[3], chama atenção para o fato de que estruturas robustas de governança tornam-se insuficientes quando não são ocupadas por lideranças capazes de agir com coerência ética ao longo do tempo.

Afinal, estruturas não operam sozinhas. São pessoas que interpretam regras, tomam decisões e respondem aos dilemas inerentes à vida organizacional, e que se deixam guiar pelo exemplo de seus líderes.

Portanto, sem cultura fortalecida, a governança corre o risco de transformar-se em mera formalidade.

3. Governança começa onde as regras não alcançam

Nenhuma política corporativa, por mais bem estruturada que seja, consegue antecipar todas as situações que emergem na dinâmica dos negócios. Afinal, são as pessoas que tomam decisões, e os dilemas mais complexos raramente apresentam respostas binárias ou claramente previstas em procedimentos.

Nenhuma política responde integralmente a perguntas como: Devo ignorar este conflito de interesses? Vale flexibilizar uma regra para atingir uma meta? Preciso reportar uma preocupação que pode gerar desconforto para minha liderança? Devo discordar de uma decisão que considero inadequada?

É justamente nesses espaços de ambiguidade que a cultura exerce sua maior influência.

Quando um profissional decide reportar ou silenciar diante de uma irregularidade, quando um gestor escolhe respeitar ou flexibilizar uma regra em função de uma meta ou quando uma liderança reage defensivamente a um questionamento ou acolhe perspectivas divergentes, são os elementos culturais que orientam essas escolhas.

A escritora Brené Brown, em sua obra Coragem para Liderar[4], argumenta que confiança, vulnerabilidade e coragem constituem competências essenciais para a construção de ambientes saudáveis.

Transportadas para o contexto organizacional, essas competências ajudam a compreender por que algumas empresas conseguem transformar mecanismos de governança em práticas vivas, enquanto outras permanecem presas à lógica da conformidade meramente formal.

Falar sobre riscos, admitir erros, discordar respeitosamente e fazer perguntas difíceis exige coragem. E a coragem somente prospera em culturas que oferecem segurança psicológica suficiente para que as pessoas possam se manifestar sem medo de retaliações desproporcionais.

Assim, governança não se resume ao estabelecimento de regras. Ela começa, justamente, onde as regras deixam de oferecer respostas prontas.

[3] Declaração proferida em entrevista concedida ao portal SEGS, em 2022, ao discutir os desafios da efetividade dos programas de integridade. Olga Pontes é executiva com ampla experiência em compliance e integridade corporativa, tendo atuado em posições de liderança em grandes organizações brasileiras.

[4] BROWN, Brené. *Coragem para Liderar:* trabalho duro, conversas difíceis, corações plenos. Rio de Janeiro: Sextante, 2019. Brené Brown é pesquisadora e professora da Universidade de Houston, com atuação voltada ao estudo da vulnerabilidade, coragem, confiança e liderança.

4. Os elementos culturais que sustentam a governança

A efetividade das estruturas de governança depende de alguns elementos culturais fundamentais, e o primeiro deles é a coerência da liderança.

A forma como líderes tomam decisões, reconhecem erros, lidam com dilemas e respondem a desvios, comunica, de maneira muito mais poderosa do que qualquer código de conduta, quais comportamentos são efetivamente esperados.

Outro aspecto relevante refere-se à segurança psicológica. Ambientes em que as pessoas sentem que podem expressar preocupações, levantar questionamentos ou discordar construtivamente tendem a identificar riscos mais precocemente[5].

A ausência de segurança psicológica produz um efeito silencioso e extremamente perigoso para a governança: as pessoas passam a saber dos riscos, mas deixam de compartilhá-los. Os problemas deixam de ser reportados, as preocupações deixam de ser verbalizadas e os sinais de alerta deixam de circular. Nesse contexto, as estruturas permanecem formalmente íntegras, mas tornam-se progressivamente cegas.

Estudos recentes indicam que ambientes psicologicamente seguros apresentam maior propensão ao reporte de preocupações éticas e irregularidades, justamente porque as pessoas percebem que podem se manifestar sem receio de retaliações ou de prejuízos à sua reputação profissional. Em contextos marcados pelo medo, pela culpabilização ou pela excessiva hierarquização das relações, os problemas deixam de ser comunicados e os riscos permanecem invisíveis às estruturas de supervisão, tornando a governança progressivamente menos capaz de cumprir sua função preventiva[6].

A existência de canais de denúncia também merece destaque. Um canal de denúncia não é apenas um mecanismo de recebimento de relatos. Ele é, sobretudo, um termômetro da confiança organizacional. Sua existência formal pouco significa se as pessoas acreditam que falar produzirá retaliações ou que nada acontecerá após o reporte.

A construção de uma cultura de integridade pressupõe, além da existência de canais, a capacidade de ouvir, de forma estruturada, a percepção das pessoas sobre o ambiente ético da organização. Pesquisas de percepção, grupos focais, entrevistas e outros instrumentos de escuta ampliam a capacidade da governança de identificar incoerências entre valores declarados e práticas efetivamente vividas[7].

Ao incorporar a experiência dos colaboradores na avaliação da cultura, a governança torna-se mais participativa e menos dependente de percepções exclusivamente hierárquicas, fortalecendo sua capacidade de identificar riscos e promover relações de confiança.

Da mesma forma, a aplicação consistente de consequências contribui para fortalecer a percepção de justiça organizacional. Quando regras são flexibilizadas em função da posição hierárquica ou dos resultados entregues, a credibilidade dos mecanismos de governança é comprometida.

A integridade é profundamente influenciada pela percepção de justiça. Quando determinados resultados justificam exceções ou quando determinadas pessoas são percebidas como "imunes às consequências", a mensagem transmitida à organização é de que as regras são negociáveis.

[5] EDMONDSON, Amy C. *The Fearless Organization:* Creating Psychological Safety in the Workplace for Learning, Innovation, and Growth. Hoboken: John Wiley & Sons, 2019. Amy Edmondson é professora da Harvard Business School e referência internacional nos estudos sobre segurança psicológica no ambiente de trabalho.

[6] LRN Corporation. *Benchmark of Ethical Culture 2024: Unveiling the Link Between Company Culture, Misconduct and Risk*. New York: LRN Corporation, 2024.

[7] ALLIANCE FOR INTEGRITY; UN GLOBAL COMPACT NETWORK GERMANY; TRANSPARENCY INTERNATIONAL DEUTSCHLAND. *Practical guide for measuring integrity culture in companies.* [*S. l.*]: Alliance for Integrity; UN Global Compact Network Germany; Transparency International Deutschland, 2025.

Por fim, merece atenção o papel das lideranças intermediárias.

Durante muito tempo, a literatura enfatizou a importância do *tone at the top*. Embora esse aspecto permaneça relevante, cresce o reconhecimento da influência exercida pelo chamado *tone at the middle*. São as lideranças intermediárias que transformam princípios abstratos em práticas concretas. São elas que decidem quais urgências justificam exceções, quais comportamentos serão tolerados e quais mensagens serão efetivamente reforçadas no cotidiano das equipes.

Pequenas racionalizações nesse nível possuem enorme potencial de multiplicação e influenciam diretamente a percepção de integridade da organização.

5. Cultura e governança: uma relação de complementaridade

Defender o papel central da cultura não significa minimizar a importância das estruturas formais. A governança continua sendo essencial para estabelecer limites, definir responsabilidades e assegurar mecanismos adequados de supervisão.

Da mesma forma, uma cultura positiva não substitui controles internos, auditorias ou programas de integridade. A relação entre cultura e governança é, portanto, de complementaridade.

A governança oferece direção; a cultura oferece sustentação.

A governança estabelece expectativas; a cultura legitima comportamentos.

A governança cria mecanismos; a cultura determina se esses mecanismos serão efetivamente utilizados.

Em outras palavras, a governança define estruturas, enquanto a cultura define significados; a governança formaliza decisões, enquanto a cultura influencia comportamentos; a governança determina o que deveria acontecer, enquanto a cultura determina aquilo que, de fato, acontece.

A integridade organizacional emerge precisamente do encontro entre essas duas dimensões. Se a cultura é capaz de fortalecer ou inviabilizar a efetividade das estruturas de governança, ela deixa de ser apenas um atributo organizacional e passa a constituir um fator de risco.

A cultura influencia a forma como decisões são tomadas, como controles são percebidos, como preocupações são reportadas e como as pessoas respondem aos dilemas éticos do cotidiano. Por essa razão, cresce internacionalmente o entendimento de que a cultura de integridade deve ser observada, monitorada e gerida de maneira tão diligente quanto outros riscos organizacionais, uma vez que sua deterioração pode comprometer a própria capacidade de funcionamento dos mecanismos formais de governança[8].

[8] ALLIANCE FOR INTEGRITY; UN GLOBAL COMPACT NETWORK GERMANY; TRANSPARENCY INTERNATIONAL DEUTSCHLAND. *Practical guide for measuring integrity culture in companies*. [*S. l.*]: Alliance for Integrity; UN Global Compact Network Germany; Transparency International Deutschland, 2025.

Considerações finais

As organizações continuarão investindo em estruturas cada vez mais sofisticadas de governança. Conselhos serão fortalecidos, controles serão aprimorados e novas tecnologias serão incorporadas aos processos de supervisão e monitoramento.

Entretanto, a efetividade desses mecanismos continuará dependendo da cultura que lhes dá vida, porque a governança define o caminho, mas é a cultura que determina se as pessoas terão coragem para percorrê-lo.

Conselhos deliberam. Políticas orientam. Controles monitoram. Canais recebem relatos. Mas são as pessoas que escolhem falar ou silenciar, agir ou omitir, cumprir ou relativizar.

Afinal, a cultura não se decreta nem se impõe. Ela é construída diariamente, em todas as decisões tomadas, no que é tolerado, no que é incentivado e no que é, efetivamente, praticado.

Os modelos de maturidade em integridade demonstram que a cultura organizacional tende a evoluir de uma postura predominantemente reativa para estágios de maior integração e internalização, até que os valores sejam efetivamente vividos no cotidiano.

Por isso, a integridade, entendida como inteireza organizacional, não nasce exclusivamente da governança. Ela nasce da interação entre estruturas consistentes e uma cultura capaz de legitimar seu funcionamento.

Sem cultura, a governança transforma-se em formalidade; com cultura, ela se torna prática cotidiana.

Ao final, não é a governança que cria integridade. Ela cria estruturas, e estruturas sustentam processos. É a cultura que determina se essas estruturas serão utilizadas para proteger ou comprometer a integridade organizacional.

Em última análise, são as culturas que sustentam as escolhas. Portanto, a construção de uma cultura de integridade não constitui um estado permanente nem um destino alcançável de forma definitiva. Trata-se de um processo contínuo de aprendizagem, adaptação e aperfeiçoamento, que exige monitoramento constante, abertura ao diálogo e capacidade de revisar práticas e comportamentos à luz dos riscos e das transformações do ambiente de negócios.

Referências

ALLIANCE FOR INTEGRITY; UN GLOBAL COMPACT NETWORK GERMANY; TRANSPARENCY INTERNATIONAL DEUTSCHLAND. *Practical guide for measuring integrity culture in companies*. [*S. l.*]: Alliance for Integrity; UN Global Compact Network Germany; Transparency International Deutschland, 2025.

BROWN, Brené. *A coragem para liderar:* trabalho duro, conversas difíceis, corações plenos. Rio de Janeiro: Sextante, 2019.

DENARDIN, Sandra. Ex-líder de compliance da Odebrecht fala pela primeira vez após desligamento da empresa. *SEGS*, 4 nov. 2021. Disponível em: https://www.segs.com.br/demais/317689-ex-lider-de-compliance-da-odebrecht-fala-pela-primeira-vez-apos-desligamento-da-empresa. Acesso em: 27 jun. 2026.

EDMONDSON, Amy C. *The Fearless Organization:* Creating Psychological Safety in the Workplace for Learning, Innovation, and Growth. Hoboken: John Wiley & Sons, 2019.

LRN CORPORATION. *Benchmark of Ethical Culture 2024:* Unveiling the Link Between Company Culture, Misconduct and Risk. New York: LRN Corporation, 2024.

SCHEIN, Edgar H. *Organizational Culture and Leadership*. 5. ed. Hoboken: John Wiley & Sons, 2017.

O compliance como pilar estratégico da governança corporativa

Andreia Marques

Andreia Marques é profissional com formação multidisciplinar em Ciências da Computação e Direito, complementada por especializações em Logística, Compliance, Proteção de Dados e Inteligência Artificial. Possui 33 anos de experiência profissional, sendo quase 15 anos dedicados à área jurídica, com atuação estratégica em Tecnologia da Informação, Recursos Humanos, Jurídico, Compliance e Proteção de Dados.

Ao longo da carreira, liderou projetos internacionais na América do Sul e desenvolveu expertise em contratos, Direito do Trabalho, Previdenciário, Ambiental e governança corporativa. Atualmente, responde pelas áreas de Compliance, Gestão da Linha Ética e Proteção de Dados (DPO) da Michelin na América do Sul, conduzindo iniciativas voltadas à ética, ESG, combate à corrupção, direitos humanos, privacidade de dados e sustentabilidade corporativa. Além disso, atua como Coordenadora da Câmara de Governança da Firjan, contribuindo para o fortalecimento das melhores práticas de governança e integridade corporativa.

1. Fundamentos e evolução do *compliance* na governança corporativa

A evolução da governança corporativa ao longo das últimas décadas evidencia uma transição relevante: de um modelo centrado no controle acionário e financeiro para uma abordagem sistêmica baseada em transparência, ética, responsabilidade e criação de valor sustentável. Nesse contexto, o compliance emerge como um elemento central dessa transformação, deixando de ser apenas um instrumento jurídico de conformidade para assumir um papel estratégico dentro das organizações.

Historicamente, a governança corporativa foi estruturada a partir da necessidade de mitigar conflitos entre proprietários e gestores, conforme discutido por autores clássicos como Berle e Means (1932). Com a intensificação da globalização, da regulação e da pressão social por maior integridade corporativa, o conceito foi ampliado, incorporando práticas voltadas à responsabilidade social e à sustentabilidade.

O compliance surge, portanto, como resposta direta ao aumento das exigências legais e regulatórias, especialmente nas áreas de combate à corrupção, lavagem de dinheiro e proteção de dados. A disseminação de legislações como o Foreign Corrupt Practices Act (EUA), o UK Bribery Act e, no Brasil, a Lei nº 12.846/2013, consolidou a necessidade de mecanismos estruturados de integridade nas empresas.

Essa evolução não deve ser compreendida apenas como uma resposta externa à pressão regulatória, mas como uma transformação interna das organizações. O compliance consolida-se como um sistema de integridade organizacional, capaz de conectar regras formais à cultura empresarial. Estudos apontam que o compliance deixou de ser apenas um mecanismo defensivo e passou a ser compreendido como elemento essencial de governança, capaz de reduzir riscos, fortalecer a reputação e gerar vantagens competitivas. Essa visão converge com diretrizes internacionais, como as da Organização para a Cooperação e Desenvolvimento Econômico (OCDE), que tratam a integridade corporativa como fator determinante para o desenvolvimento econômico sustentável.

O diferencial de um Programa de Compliance efetivo não está apenas em sua existência formal, mas na sua capacidade de promover transformação comportamental, influenciando decisões e atitudes no cotidiano empresarial. Dessa forma, o compliance assume caráter dinâmico, evolutivo e multidimensional, alinhado às melhores práticas internacionais.

2. O compliance como instrumento estratégico de criação de valor

A concepção contemporânea do compliance o posiciona como um vetor estratégico dentro das organizações. Não se trata mais apenas de evitar sanções, mas de contribuir para a geração de valor e para o fortalecimento da governança corporativa.

Pesquisas globais indicam que empresas que integram o compliance às suas estratégias conseguem alinhar melhor seus objetivos de negócio com expectativas regulatórias e sociais, aumentando a confiança de investidores e *stakeholders*. A confiança, nesse sentido, torna-se um ativo intangível fundamental.

O compliance deve ser visto como um instrumento de gestão estratégica, e não como função isolada. Programas de integridade eficazes são aqueles que se conectam diretamente à estratégia empresarial e às decisões da alta administração, influenciando inclusive a forma como riscos são compreendidos e tratados.

Além disso, o compliance estratégico atua em três dimensões principais:

- **Mitigação de riscos corporativos**, incluindo riscos legais, reputacionais e operacionais.
- **Aprimoramento da tomada de decisão**, com base em critérios éticos e de transparência.
- **Fortalecimento da cultura organizacional**, promovendo ou fortalecendo valores alinhados à integridade.

A criação de valor pelo compliance está diretamente associada à sua capacidade de gerar confiança institucionalizada, ou seja, confiança baseada não apenas em reputação, mas em estruturas sólidas de governança que garantem previsibilidade e segurança nas relações empresariais.

No Brasil, essa transformação é impulsionada por fatores como a maturação da Lei Anticorrupção e a crescente atuação de órgãos reguladores, que incentivam a adoção de programas de integridade como diferencial competitivo.

No âmbito acadêmico brasileiro, autores como Andrade e Rossetti (2012) destacam que a governança eficaz depende da integração entre mecanismos formais (regras, controles) e informais (cultura e ética), sendo o compliance o elo que conecta essas dimensões.

Nesse sentido, a consolidação do compliance como função estratégica exige sua integração a estruturas formais de governança, com responsabilidades claramente definidas e instâncias de supervisão ativas. Sua efetividade depende da coordenação entre compliance, gestão de riscos, auditoria e jurídico, evitando lacunas e sobreposições. Nesse contexto, a alta administração e os órgãos de governança desempenham papel central ao garantir diretrizes, recursos e a sustentação contínua do Programa de Integridade como elemento estrutural da estratégia organizacional.

3. Tendências globais: ESG, tecnologia e regulação

O cenário atual global reforça ainda mais o papel estratégico do *compliance*. Três grandes tendências moldam essa evolução, como demonstrando a seguir.:

3.1 Integração com ESG

A agenda ESG tornou-se central nas estratégias corporativas internacionais. Reguladores e investidores exigem maior transparência e responsabilidade, fazendo com que o compliance amplie seu escopo para além das obrigações legais.

Atualmente, compliance e ESG são indissociáveis: programas de integridade precisam contemplar temas como direitos humanos, diversidade, sustentabilidade e impacto social.

Essa integração representa uma evolução natural do compliance, que passa a incorporar dimensões éticas mais amplas. O compliance deixa de ser apenas uma função de controle para assumir papel ativo na sustentabilidade corporativa.

3.2 Intensificação regulatória e *enforcement* global

O ambiente regulatório tornou-se mais complexo e interconectado, com forte cooperação internacional entre autoridades. Isso exige das empresas programas de compliance capazes de atuar de forma integrada em múltiplas jurisdições.

Nesse cenário, a governança deve ser acompanhada de mecanismos de compliance capazes de garantir uniformidade de princípios, mesmo diante de legislações distintas. Trata-se de um desafio que exige padronização ética com adaptação local.

3.3 Transformação digital e uso de tecnologia

O avanço tecnológico impacta profundamente o compliance. Ferramentas de análise de dados, inteligência artificial e automação aumentam a eficiência dos controles, mas também ampliam os riscos.

A tecnologia não substitui o compliance, mas exige sua evolução. O profissional da área deve assumir papel mais analítico e estratégico, utilizando dados para antecipar riscos e apoiar decisões organizacionais, atuando como facilitador da inovação com responsabilidade.

4. A perspectiva brasileira: avanços e desafios

No Brasil, o desenvolvimento do compliance está diretamente ligado ao combate à corrupção e ao fortalecimento das instituições. A Lei nº 12.846/2013 marcou um ponto de inflexão ao estabelecer a responsabilização objetiva das empresas por atos ilícitos.

A legislação brasileira avançou significativamente ao incorporar conceitos internacionais de integridade, alinhando-se às diretrizes da OCDE. Contudo, ressalta que a simples existência de normas não garante a efetividade do compliance.

Ademais, eventos como a Operação Lava Jato ampliaram a conscientização sobre a importância da ética empresarial e da transparência, intensificando a demanda por práticas robustas de governança.

Uma pesquisa recente da Grant Thornton Brasil apontou a "oportunidade" como o principal motivador de fraudes corporativas, sendo citada por (90%) dos respondentes como facilitada pela deficiência ou ausência de controles e monitoramento.

É necessária a customização dos programas de integridade, considerando as especificidades culturais, sociais e regulatórias de cada organização. No contexto brasileiro — marcado por desafios institucionais e diversidade regional — essa adaptação é fundamental.

Entre os principais desafios no Brasil, destacam-se:

- necessidade de amadurecimento da cultura ética nas organizações;
- dificuldade de integração entre as áreas (jurídica, compliance, auditoria e gestão);
- tendência de tratar o compliance como obrigação formal, e não como valor estratégico.

Além disso, existe uma preocupação por parte das empresas com a redução de despesas, para melhorar a rentabilidade do negócio e o cumprimento de metas, garantindo sustentabilidade econômica. Nesse contexto, fica difícil falar de compliance, uma atividade que demanda recursos e cria novos procedimentos dentro da empresa. É, de fato, desafiador. No entanto, como uma empresa poderá se sustentar ao longo dos anos, caso venha a sofrer impactos financeiros significativos e não previstos, com aplicações de multas e sanções legais, ou até mesmo com sua reputação abalada?

Um Programa de Compliance bem desenvolvido, adequadamente implementado e comunicado com eficácia, funciona como uma ferramenta de sustentabilidade corporativa, porque ajuda a empresa a mapear seus riscos, prevenir fraudes e evitar punições por descumprimento da legislação aplicável ao negócio.

O verdadeiro avanço no Brasil ocorrerá quando o compliance for plenamente incorporado ao modelo mental da alta e média liderança, tornando-se parte da identidade organizacional, parte dos seus valores.

Não é mais possível acreditar que o "*tone at the top*" é suficiente, porque se o topo inspira e o meio executa, é necessário investir também onde a cultura de fato se sustenta. Tratar o "*tone at the middle*" é tratar da camada em que se concentra o maior risco reputacional, até porque a maioria dos desvios ocorre a partir de decisões operacionais repetidas, justificadas por urgência, metas agressivas ou cultura de tolerância. São os gestores intermediários que, via de regra, sufocam o canal de denúncia. Pequenos sinais como ignorar um conflito de interesse ou suavizar uma regra, têm efeito multiplicador sobre a equipe, muito mais do que qualquer comunicado corporativo.

5. *Compliance* e o futuro da governança corporativa

O futuro da governança corporativa está intrinsecamente ligado à evolução do compliance como função estratégica. As organizações que conseguirem integrar plenamente a conformidade aos seus modelos de decisão estarão mais preparadas para enfrentar um ambiente de negócios caracterizado por incerteza e alta complexidade.

O futuro do compliance está na sua capacidade de transformar-se em um mecanismo de governança ética permanente, indo além de controles formais para promover alinhamento entre propósito empresarial e comportamento organizacional.

O compliance do futuro tende a apresentar características como:

- **proatividade**, com foco em prevenção e não apenas reação;
- **integração com a alta gestão**, influenciando decisões estratégicas;
- **uso intensivo de dados e tecnologia**, com análise preditiva;
- **centralidade na cultura organizacional**, promovendo ética como valor estruturante.

A construção de uma cultura de integridade exige consistência, liderança exemplar e comunicação contínua. Não se trata de um projeto pontual, mas de um processo contínuo de evolução institucional.

Assim, o compliance deixa de ser um requisito regulatório e consolida-se como um dos pilares centrais da governança corporativa moderna, sendo essencial para a legitimidade das organizações, a sustentabilidade dos negócios e a construção de confiança no longo prazo.

Referências

ANDRADE, Adriana; ROSSETTI, José Paschoal. *Governança Corporativa:* fundamentos, desenvolvimento e tendências. São Paulo: Atlas, 2012.

ALLIANCE FOR INTEGRITY; GRUPO DE TRABALHO ANTICORRUPÇÃO DA REDE BRASIL DO PACTO GLOBAL DA ONU. *Prevenção à corrupção: um guia para empresas.* [*S. l.*]: Alliance for Integrity; Rede Brasil do Pacto Global da ONU, 2016. Disponível em: https://www.allianceforintegrity.org/wAssets/docs/publications/pt/programa-de-compliance/Prevencao-a-Corrupcao_Um-Guia-para-Empresas.pdf. Acesso em: 18 out. 2026.

BERLE, Adolf A.; MEANS, Gardiner C. *The modern corporation and private property.* New York: Macmillan, 1932.

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA (IBGC). *Código das melhores práticas de governança corporativa.* 6. ed. São Paulo: IBGC, 2023.

BASTOS, Marcella Blok. *Compliance e Governança Corporativa*. 4. ed. Rio de Janeiro: Freitas Bastos, 2023.

ZENKNER, Marcelo. *Tone at the Top, descanse em paz. Artigo, LinkedIn*

Fontes recentes e estudos complementares

PWC. *PwC's Global Compliance Survey 2025:* moving faster — reinventing compliance to speed up, not trip up. [S. l.]: PwC, 2025. Disponível em: https://www.pwc.com/gx/en/issues/risk-regulation/pwc-global-compliance-study-2025.pdf. Acesso em: 19 maio 2026.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD). *Corporate governance.* Paris: OECD. Disponível em: https://www.oecd.org/en/topics/corporate-governance.html. Acesso em: 19 maio 2026.

ESG trends: looking back on 2024 and outlook for 2025. Disponível em: (https://www.dilitrust.com/esg-trends-2025/). Disponível em: 19 maio 2026

Grant Thornton. Tendências e perspectivas de compliance para 2025. Disponível em: (https://www.grantthornton.com.br/insights/artigos-e-publicacoes/pesquisas/). Acesso em: 19 de maio de 2026.

Um ambiente de negócios íntegro não é possível sem os pequenos negócios

Gabriel Nogueira Portella Nunes Pinto Bravo

Gabriel Nogueira Portella Nunes Pinto Bravo é gerente das Unidades de Integridade Corporativa e da Ouvidoria do Sebrae Nacional; conselheiro titular no Conselho Deliberativo do Sebrae Rondônia e coordenador do Comitê de Compliance no mesmo conselho; membro titular no Comitê do Pró-Ética e no Conselho de Transparência, Integridade e Combate à Corrupção (CTICC), da Controladoria-Geral da União.

Advogado, especialista em Direito e Gestão de Serviços Sociais Autônomos pelo IDP. Possui mais de 19 anos de experiência no Sistema Sebrae, com atuação destacada nas áreas jurídica, de integridade, de ouvidoria e de governança.

Ao longo de sua trajetória, foi advogado e, posteriormente, gerente jurídico do Sebrae/RJ por uma década, tendo exercido também a função de gerente da Ouvidoria da instituição. Atualmente acumula a gerência das Unidades de Integridade Corporativa e Ouvidoria do Sebrae Nacional, com foco em governança, gestão de riscos, investigações internas, integridade e aprimoramento de mecanismos de controle institucional.

No âmbito institucional e representativo, atuou em diversas comissões da Ordem dos Advogados do Brasil, incluindo o exercício do cargo de conselheiro suplente na OAB/RJ e de ouvidor adjunto. Também participou de comissões voltadas à advocacia corporativa na OAB/RJ e ao apoio jurídico a micro e pequenas empresas no Conselho Federal da OAB, tendo exercido, nesse contexto, as funções de vice-presidente e secretário executivo.

Introdução

Quando comecei a estudar compliance ou integridade corporativa, expressão que considero mais adequada por sua maior amplitude e aderência ao conceito contemporâneo, eu já atuava no Sebrae. Naquele contexto, há pouco mais de doze anos, uma questão começou a me acompanhar: em que medida as micro e pequenas empresas brasileiras seriam impactadas por essa agenda?

A pergunta fazia sentido diante da dimensão dos pequenos negócios na economia brasileira. Em 2014, segundo dados divulgados pelo Sebrae, o país contava com cerca de nove milhões de micro e pequenas empresas, que representavam aproximadamente 99% dos empreendimentos brasileiros, respondiam por cerca de 27% do Produto Interno Bruto (PIB) e empregavam 52% da mão de obra formal no setor privado.

Mais de uma década depois, sua relevância permanece evidente. Atualmente, os pequenos negócios representam cerca de 97% das empresas brasileiras e respondem por 26,5% do PIB nacional. No mercado de trabalho, dados baseados na Relação Anual de Informações Sociais (RAIS) 2024 indicam que as micro e pequenas empresas concentravam 19,8 milhões de vínculos formais, superando, em estoque de empregos, as médias e grandes empresas.

Foi justamente nesse universo que entrou em vigor a Lei nº 12.846/2013, conhecida como Lei Anticorrupção. Ao responsabilizar pessoas jurídicas pela prática de atos lesivos contra a Administração Pública, nacional ou estrangeira, e valorizar a existência de mecanismos de integridade, a legislação contribuiu para impulsionar uma nova agenda de responsabilidade empresarial no país.

Diante disso, minha inquietação era relativamente simples: como essa agenda chegaria aos pequenos negócios, responsáveis pela quase totalidade dos empreendimentos brasileiros?

A estrutura tradicionalmente associada a um Programa de Compliance parecia ampla, complexa e, muitas vezes, distante da realidade de uma pequena empresa. A própria linguagem utilizada à época em materiais especializados revelava essa distância. Expressões como *tone at the top*, *due diligence* e *background check*, entre tantas outras, circulavam em um vocabulário técnico, pouco acessível e, em certa medida, elitizado.

Ainda que esses conceitos fossem traduzidos para o português, avanço que se consolidou ao longo dos anos, parte da distância permaneceria. Falar em "alta administração", por exemplo, pode fazer sentido em grandes organizações, mas soa pouco aderente à realidade de um pequeno negócio no qual o proprietário frequentemente concentra funções administrativas, comerciais, financeiras e operacionais.

O risco, portanto, sempre foi o de que o pequeno empreendedor enxergasse a integridade como algo necessário e positivo, porém pertencente a outra realidade: a das grandes corporações, multinacionais ou organizações com estruturas empresariais mais sofisticadas.

1. Da adaptação regulatória ao diagnóstico das MPEs

Essa distância entre o modelo tradicional de integridade e a realidade dos pequenos negócios, contudo, não passou despercebida pelo próprio marco regulatório. A regulamentação da Lei nº 12.846/2013 procurou reconhecer as diferenças de porte, estrutura e capacidade operacional das empresas, abrindo espaço para uma aplicação mais proporcional dos mecanismos de integridade às microempresas e empresas de pequeno porte.

Embora a Lei Anticorrupção não tenha estabelecido originalmente um modelo específico de Programa de Integridade para microempresas e empresas de pequeno porte, seu artigo 7º abriu espaço para que a regulamentação considerasse características como quantidade de funcionários, complexidade da estrutura interna e utilização de terceiros.

Em 2015, o Decreto nº 8.420/2015, então responsável pela regulamentação da lei, avançou nessa direção ao reduzir formalidades na avaliação dos programas de integridade das microempresas e empresas de pequeno porte.

Com base nessa possibilidade de tratamento diferenciado, foi editada, ainda naquele ano, a Portaria Conjunta CGU/SMPE nº 2.279/2015. A norma detalhou medidas de

integridade aplicáveis às Micro e Pequenas Empresas (MPEs) e buscou estabelecer parâmetros mais simples e compatíveis com a realidade desses negócios.

Na prática, a regulamentação permitiu reconhecer a integridade por meio de instrumentos proporcionais à estrutura das pequenas empresas: códigos de conduta simplificados, orientações diretas do proprietário aos empregados, treinamentos, controles sobre pagamentos e contratações, mecanismos para comunicação de irregularidades, verificações de fornecedores e adoção de medidas corretivas.

O ponto central dessa abordagem era importante: integridade não deveria significar necessariamente a reprodução, em menor escala, das estruturas existentes em grandes corporações. O foco poderia estar na adoção efetiva de práticas de prevenção, detecção e correção de irregularidades compatíveis com os riscos, o porte e a capacidade operacional de cada negócio.

Em 2017, Sebrae e Controladoria-Geral da União (CGU) avançaram nessa aproximação ao desenvolver conjuntamente uma cartilha de orientações práticas destinada a sensibilizar e auxiliar os pequenos negócios na implementação de medidas de integridade.

Posteriormente, o Decreto nº 11.129/2022, que substituiu o Decreto nº 8.420/2015 na regulamentação da Lei Anticorrupção, manteve a possibilidade de tratamento diferenciado para microempresas e empresas de pequeno porte. É verdade que a Portaria Conjunta CGU/SMPE nº 2.279/2015 demanda atualização diante das transformações normativas, tecnológicas e conceituais ocorridas desde sua edição. Ainda assim, é preciso reconhecer que ela representou um avanço importante na tentativa de aproximar a agenda de integridade da realidade das MPEs.

Mas essa evolução leva a uma questão ainda mais relevante: passados mais de dez anos desde as primeiras iniciativas voltadas à adaptação dessa agenda às MPEs, em que medida a integridade foi efetivamente incorporada à realidade dos pequenos negócios e quais fatores ainda podem dificultar esse processo?

Responder a essa pergunta é fundamental. Afinal, se a integridade pretende contribuir para um ambiente de negócios mais ético, transparente e responsável, essa agenda precisa alcançar justamente quem representa a maior parte dos empreendimentos brasileiros.

Mais de uma década depois das inquietações que deram origem a essa reflexão, passamos a dispor de dados que ajudam a compreender melhor essa realidade.

Em julho de 2026, o Sebrae Nacional, por meio da Unidade de Integridade Corporativa, e a Controladoria-Geral da União, por meio da Secretaria de Integridade Privada, realizaram uma pesquisa com micro e pequenas empresas para medir seu grau de maturidade em integridade, identificar práticas já adotadas e compreender os principais obstáculos à implementação de programas adequados a esse segmento.

Do ponto de vista metodológico, o levantamento foi realizado por meio de pesquisa on-line (*web survey*), com questionário enviado por e-mail a empreendedores de microempresas e empresas de pequeno porte e respondido na plataforma SurveyMonkey. A coleta ocorreu entre 13 e 20 de julho de 2026 e reuniu 649 respostas completas, com nível de confiança de 95% e margem de erro de aproximadamente quatro pontos percentuais.

Os resultados confirmam parte relevante das inquietações que motivaram esta reflexão.

Antes da apresentação do tema, o nível médio de conhecimento dos respondentes sobre programas de integridade era de apenas 3,8 em uma escala de 1 a 10. Além disso, 80% declararam não possuir um Programa de Integridade ou não saber informar se a empresa possuía um.

À primeira vista, os números poderiam indicar simplesmente uma baixa adoção de práticas de integridade. Mas os demais resultados revelam uma realidade mais interessante.

Quando questionadas sobre práticas específicas, muitas empresas demonstraram já adotar medidas diretamente relacionadas à integridade, ainda que não necessariamente as reconhecessem como componentes de um programa estruturado.

O registro contábil preciso, por exemplo, foi indicado por 79% dos respondentes; a divulgação de informações claras sobre produtos e serviços, por 69%; e a existência de algum meio para relatar irregularidades, por 61%. Em contraste, apenas 36% declararam possuir código de ética formal, e o mesmo percentual afirmou que os sócios já formalizaram e divulgaram uma declaração de valores e compromisso com a integridade.

Esse contraste talvez seja um dos achados mais importantes da pesquisa. Ele sugere que o desafio não consiste apenas em criar estruturas ou instrumentos. Em muitos casos, é necessário ajudar o pequeno empreendedor a reconhecer, organizar e aprimorar práticas que já fazem

parte de sua rotina, transformando condutas dispersas em um sistema mínimo, proporcional e compreensível de integridade.

Em outras palavras, talvez o primeiro passo não seja simplesmente ensinar a pequena empresa a "ter compliance", mas mostrar que integridade pode começar por práticas de boa gestão que ela já conhece: manter registros confiáveis, definir responsabilidades, controlar pagamentos, conhecer fornecedores, cumprir compromissos, tratar adequadamente irregularidades e deixar claros os valores que orientam o negócio.

Os dados também sugerem que a baixa adoção não deve ser interpretada necessariamente como resistência ao tema.

A maioria dos respondentes, 55%, declarou interesse em receber apoio para construir ou desenvolver um programa de integridade, enquanto 66% afirmaram desejar que suas empresas fossem reconhecidas no mercado por possuir um programa próprio.

Após conhecerem melhor o tema, os participantes atribuíram grau médio de importância de 7,2, em uma escala de 0 a 10, à existência de um programa de integridade, sendo que 37% atribuíram notas 9 ou 10.

Há, portanto, espaço concreto para avançar.

A principal dificuldade apontada pelos respondentes foi justamente a falta de conhecimento ou de orientação especializada, mencionada por 32%, seguida pela falta de tempo ou pelo impacto na rotina operacional, pelos custos financeiros e pela baixa percepção dos benefícios que a integridade pode proporcionar ao negócio.

Outro aspecto relevante é o desconhecimento sobre os incentivos e as consequências associados à adoção de práticas de integridade. Apenas 41% dos respondentes sabiam que grandes empresas e o governo têm exigido de seus fornecedores a adoção de programas de integridade. Somente 22% conheciam a previsão da Lei nº 14.133/2021 que admite o desenvolvimento de programa de integridade como critério de desempate em licitações. Além disso, apenas 25% sabiam que a existência de um programa de integridade pode ampliar oportunidades comerciais e ser considerada na aplicação de penalidades previstas na Lei nº 12.846/2013.

2. Caminhos para aproximar a integridade dos pequenos negócios

Esses achados apontam para uma mudança necessária na forma de apresentar o tema.

Os resultados da pesquisa demonstram que as políticas públicas levadas a cabo nos últimos anos ainda não foram capazes de atrair de forma ampla e efetiva os pequenos negócios para a agenda da integridade corporativa. A persistência do baixo nível de conhecimento sobre o tema, a limitada percepção de seus benefícios concretos e a reduzida adesão a programas estruturados indicam que os instrumentos até aqui utilizados não foram suficientes para transformar a integridade em prática cotidiana e acessível para a maioria das micro e pequenas empresas.

Para os pequenos negócios, integridade não pode ser comunicada apenas como agenda de prevenção de ilícitos ou atendimento a exigências legais. Ela também precisa ser compreendida como instrumento de gestão, mitigação de riscos, fortalecimento da confiança e acesso a mercados.

Isso significa preparar as MPEs para participar de cadeias de fornecimento cada vez mais qualificadas, disputar contratações públicas em ambientes mais íntegros, construir relações comerciais mais confiáveis e atender às exigências crescentes de clientes, parceiros e grandes empresas.

Se o diagnóstico aponta para baixo conhecimento, práticas dispersas e interesse em avançar, a resposta precisa combinar pelo menos três movimentos: simplificar, demonstrar valor e ampliar o acesso.

Simplificar significa traduzir conceitos e oferecer ferramentas proporcionais ao porte, aos riscos e à capacidade operacional das empresas. Uma pequena empresa não precisa reproduzir a estrutura de compliance de uma multinacional para demonstrar compromisso com a integridade.

Demonstrar valor significa conectar a integridade aos problemas concretos do empreendedor: reduzir riscos, evitar perdas, melhorar controles, fortalecer a reputação,

conquistar clientes e fornecedores, participar de compras públicas e acessar novas oportunidades de mercado.

E ampliar o acesso significa disponibilizar conhecimento e ferramentas de maneira simples e escalável. A própria pesquisa oferece uma indicação importante nesse sentido: vídeos e textos na internet aparecem entre os meios preferidos pelos respondentes para acessar conhecimento, indicando espaço para soluções digitais de baixo custo, complementadas, quando necessário, por capacitações e orientações mais direcionadas.

Mais do que comprovar a baixa maturidade atual, portanto, a pesquisa evidencia uma oportunidade: transformar a integridade em uma linguagem de gestão para os pequenos negócios.

Isso exige abandonar modelos excessivamente formais, aproximar conceitos jurídicos e corporativos da rotina do empreendedor e construir uma trilha progressiva, na qual cada empresa possa avançar de acordo com seu porte, seus riscos, seu mercado e sua capacidade operacional.

O Sebrae tem papel relevante nesse processo. A instituição foi um dos primeiros apoiadores institucionais do Pacto Brasil pela Integridade Empresarial, iniciativa da CGU voltada à sensibilização, mobilização e promoção da integridade no setor privado. A partir de sua capilaridade e de sua relação direta com empreendedores e parceiros estratégicos, o Sebrae tem buscado contribuir para aproximar essa agenda dos pequenos negócios e demonstrar seus benefícios em termos de crescimento, acesso a mercados, mitigação de riscos e competitividade.

Mas essa responsabilidade não deve ser apenas do Sebrae e da CGU. O próprio mercado de integridade corporativa precisa enxergar os pequenos negócios como parte fundamental dessa agenda e desenvolver produtos, serviços, metodologias e ferramentas mais simples, acessíveis e adequados à sua realidade.

A pesquisa ajuda, assim, a responder à pergunta que me acompanhava desde o início dessa trajetória. A baixa incorporação da agenda de integridade pelos pequenos negócios não parece decorrer simplesmente de falta de interesse. Os resultados apontam para uma combinação de baixo conhecimento, dificuldade de orientação, limitações operacionais e pouca percepção dos benefícios concretos, ao mesmo tempo em que revelam práticas já existentes e disposição para avançar.

O desafio dos próximos anos é reduzir essa distância, o que passa tanto pelo aumento da efetividade das políticas públicas voltadas à disseminação da integridade entre os pequenos negócios quanto pela apropriação dessa agenda pelo próprio mercado, com o desenvolvimento de soluções simples, acessíveis e adequadas às MPEs, um campo ainda pouco explorado e com significativo potencial de geração de valor econômico.

Se quisermos que a integridade deixe de ser percebida como uma pauta restrita às grandes corporações e se transforme efetivamente em parte da cultura empresarial brasileira, precisaremos torná-la simples, útil, proporcional e acessível.

Afinal, um ambiente de negócios verdadeiramente íntegro só será possível quando essa agenda alcançar também aqueles que representam a imensa maioria das empresas do país. Sem os pequenos negócios, não haverá ambiente de negócios íntegro no Brasil.

Referências

BRASIL. *Decreto nº 8.420, de 18 de março de 2015.* Regulamenta a Lei nº 12.846, de 1º de agosto de 2013, e dá outras providências. Brasília, DF: Presidência da República, 2015. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/decreto/d8420.htm. Acesso em: 1 set. 2026.

BRASIL. *Decreto nº 11.129, de 11 de julho de 2022.* Regulamenta a Lei nº 12.846, de 1º de agosto de 2013. Brasília, DF: Presidência da República, 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/decreto/d11129.htm. Acesso em: 1 set. 2026.

BRASIL. *Lei nº 12.846, de 1º de agosto de 2013.* Dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira, e dá outras providências. Brasília, DF: Presidência da República, 2013. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12846.htm. Acesso em: 1 set. 2026.

BRASIL. *Lei nº 14.133, de 1º de abril de 2021.* Lei de Licitações e Contratos Administrativos. Brasília, DF: Presidência da República, 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14133.htm. Acesso em: 1 set. 2026.

BRASIL. Controladoria-Geral da União. *Pacto Brasil pela Integridade Empresarial*. Brasília, DF: CGU, [2024]. Disponível em: https://www.gov.br/cgu/pt-br/assuntos/integridade-privada/pacto-brasil. Acesso em: 1 set. 2026.

BRASIL. Controladoria-Geral da União; Secretaria da Micro e Pequena Empresa. *Portaria Conjunta CGU/SMPE nº 2.279, de 9 de setembro de 2015*. Dispõe sobre a avaliação de programas de integridade de microempresa e de empresa de pequeno porte. Brasília, DF: CGU; SMPE, 2015. Disponível em: https://www.gov.br/cgu/pt-br/assuntos/integridade-privada/avaliacao-e-promocao-da-integridade-privada/legislacao. Acesso em: 1 set. 2026.

BRASIL. Controladoria-Geral da União; SERVIÇO BRASILEIRO DE APOIO ÀS MICRO E PEQUENAS EMPRESAS. *Integridade para pequenos negócios: construa o país que desejamos a partir da sua empresa*. Brasília, DF: CGU; Sebrae, 2015. Disponível em: https://bis.sebrae.com.br/bis/download.zhtml?t=D&uid=c49af50a24136d157320e9fee-e9c96a9. Acesso em: 1 set. 2026.

BRASIL. Ministério do Trabalho e Emprego. *Relação Anual de Informações Sociais (RAIS)*: ano-base 2024: sumário executivo. Brasília, DF: Ministério do Trabalho e Emprego, 2026. Disponível em: https://www.gov.br/trabalho-e-emprego/pt-br/acesso-a-informacao/acoes-e-programas/programas-projetos-acoes-obras-e-atividades/estatisticas-trabalho/rais/rais-2024/rais-2024-1/sumario-executivo_rais-2024-1.pdf/view. Acesso em: 1 set. 2026.

SERVIÇO BRASILEIRO DE APOIO ÀS MICRO E PEQUENAS EMPRESAS. *Participação das micro e pequenas empresas na economia brasileira*. Brasília, DF: Sebrae, 2014. Disponível em: https://meuatendimento.sebrae.com.br/Sebrae/Portal%20Sebrae/Estudos%20e%20Pesquisas/Participacao%20das%20micro%20e%20pequenas%20empresas.pdf. Acesso em: 1 set. 2026.

SERVIÇO BRASILEIRO DE APOIO ÀS MICRO E PEQUENAS EMPRESAS. Unidade de Estratégia e Transformação; Unidade de Integridade Corporativa. *Pesquisa maturidade em integridade nas MPE 2026*. Brasília, DF: Sebrae Nacional, jul. 2026.

O papel do compliance na governança das empresas estratégicas de defesa

Adriana da Rosa Silva

Adriana da Rosa Silva é coordenadora de Compliance e Integridade do SENAI CETIQT, com certificação CPC-A. Advogada, mestre em Direito Econômico pela Universidade de Coimbra e pós-graduanda em Direito do Estado pela UERJ.

Diogo de Souza e Mello

Diogo de Souza e Mello é advogado do SENAI CETIQT, master in Business Innovation em Indústria 4.0., pós-graduado em Direito Digital, membro da Comissão de Defesa do Consumidor da OAB-RJ, pós-graduado em Direito Processual Civil e em Direito do Trabalho e Legislação Social.

Thiago Felipe da Silva Carlos

Thiago Felipe da Silva Carlos é advogado do SENAI CETIQT, pós-graduado em Direito dos Contratos pela PUC-Rio.

Introdução

O arcabouço regulatório que estruturou a Indústria de Defesa no Brasil foi concebido a partir da Base Industrial de Defesa (BID) com a criação de leis específicas, abrangendo regras de continuidade, incentivos fiscais e fomento estatal, tendo como objetivo principal garantir a autonomia tecnológica e a soberania nacional.

Nesse contexto, surgiram os conceitos de Empresa Estratégica de Defesa (EED), Produto Estratégico de Defesa (PED) e Produto de Defesa (PRODE). Sob esse arcabouço legal, as EEDs, pessoas jurídicas credenciadas pelo Ministério da Defesa, tornaram-se beneficiárias de um regime especial tributário, linhas de fomento e regras exclusivas de licitação, sujeitando-se, contudo, a critérios rigorosos de credenciamento e descredenciamento.

As EEDs operam em um ambiente de alta sensibilidade, no qual o descumprimento de requisitos legais e regulatórios pode acarretar severas consequências, desde perdas financeiras e reputacionais até a nulidade de atos societários e desfazimento de bens, podendo o seu descredenciamento comprometer, inclusive, a segurança nacional, o que dá ao compliance um papel de enorme responsabilidade.

A redação atual da Lei nº 14.459/2022[1] destaca a importância conferida às EEDs para a segurança nacional, conforme expresso no artigo 1º-A:

> Art. 1º-A. As Empresas Estratégicas de Defesa (EEDs) são *essenciais* para a promoção do desenvolvimento científico e tecnológico brasileiro e *fundamentais* para a preservação da segurança e da defesa nacional contra ameaças externas (grifo dos autores)

Com a finalidade de mitigar situações que contrariem a legislação específica e que possam configurar ameaças diretas à soberania, a referida lei estabeleceu mecanismos rigorosos de contenção, garantindo assim que os interesses comerciais privados das EEDs não se sobreponham à segurança e à autonomia tecnológica nacional, incluindo:

- Obrigação de Continuidade Produtiva mesmo após o descredenciamento (Art. 2º-A, § 2º)
- Poder de Veto do Ministro da Defesa ao pedido de descredenciamento (Art. 2º-A, § 3º)
- Permanência Compulsória como EED por até 5 anos (Art. 2º-A, § 4º)
- Nulidade de alterações Societárias e Venda de Bens sem o consentimento do Ministro da Defesa (Art. 2º-A, § 5º)

O regime jurídico aplicável às EEDs estabelece uma relação de proporcionalidade entre os incentivos recebidos e as exigências estatais. Consequentemente, a posição privilegiada no mercado de defesa acarreta limitações à autonomia de gestão e eleva os riscos de conformidade, tornando os programas de integridade indispensáveis para a viabilidade e a continuidade dessas empresas.

A atuação no setor de defesa impõe às EEDs o desafio de atuar em um ambiente complexo e cheio de contradições. Por um lado, a eficiência na gestão de vultosos recursos públicos e a magnitude das contratações estratégicas exigem o mais alto grau de transparência e prestação de contas à sociedade. Por outro, a natureza sensível das tecnologias desenvolvidas e a imperativa proteção à soberania nacional demandam um regime de sigilo absoluto. Os principais desafios dessas organizações nascem justamente dessa dupla exigência. Nesse ambiente de tensão constante, a estratégia de uma EED não pode ignorar as regras do setor: é preciso um alinhamento contínuo para garantir a manutenção do credenciamento e a conformidade regulatória.

Ademais, o expressivo volume financeiro do setor, somado ao véu de confidencialidade que o encobre, cria um ambiente de alto risco para desvios éticos. Este artigo propõe-se a refletir sobre os possíveis atritos operacionais e regulatórios enfrentados pelas EEDs, evidenciando a necessidade premente de uma cultura de integridade corporativa que responda com eficácia às legislações anticorrupção nacionais e transnacionais. Nesse contexto, o papel exercido pela área de compliance transcende a mera observância legal; ele se consolida como o principal alicerce da governança corporativa.

[1] BRASIL. Lei nº 14.459, de 21 de setembro de 2022. Altera a Lei nº 12.598, de 21 de março de 2012.

1. Equilíbrio entre transparência e sigilo

Um dos maiores desafios para as EEDs reside no delicado equilíbrio entre a necessidade de transparência no uso dos recursos[2], diante da obrigatoriedade de prestar contas, e a imperatividade do sigilo imposto pela segurança nacional.

A Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação – LAI)[3], estabelece como regra geral a publicidade dos atos e informações governamentais. Contudo, a própria legislação excepciona essa regra nos casos em que a divulgação tiver potencial de colocar em risco a defesa e a soberania nacional ou as relações internacionais do País.

Embora muitas EEDs possuam capital estritamente privado e, em tese, não se submetam às obrigações de publicidade da LAI, é importante lembrar que as informações inerentes aos projetos de defesa não pertencem às EEDs, mas sim, ao Estado brasileiro e, por isso, precisam ser classificadas utilizando os critérios da própria LAI e do Decreto nº 7.845/2012[4].

Consequentemente, as EEDs precisam controlar e monitorar sua comunicação externa, a fim de mitigar o risco de exposição não autorizada de dados estratégicos em peças publicitárias e materiais de marketing, por exemplo. Para tanto, deve-se cumprir rigorosamente as cláusulas de confidencialidade e a observância de autorização prévia e expressa do órgão contratante antes de qualquer divulgação.

A clareza e observância à classificação das informações circulantes nos projetos de defesa é requisito vital que sustenta, são requisitos vitais que sustentam não apenas a atuação da EED no mercado de defesa, mas também sua integridade. Vale ressaltar que a inobservância a qualquer desses pontos pode impactar e fragilizar a segurança nacional do país.

Outro aspecto a ser considerado é que a criação das EEDs, e de todo o arcabouço regulatório, teve o propósito de reter o conhecimento e fortalecer a Base Industrial de Defesa, para mitigar a dependência externa em setores críticos. Por isso, qualquer vazamento de dados ou informações ou transferência de conhecimento científico e tecnológico não autorizada compromete a autonomia tecnológica nacional, atinge a Estratégia Nacional de Defesa e compromete a capacidade do Estado Brasileiro de se proteger frente aos complexos cenários geopolíticos.

A ausência de mecanismos de integridade e controle expõe a organização a consequências graves. A transferência indevida de documentos ou informações classificadas como secretas ou ultrassecretas transborda a esfera das sanções administrativas, como o descredenciamento de ofício, e adentra na seara criminal, podendo ser caracterizado como crime contra a soberania nacional, nos termos da lei[5].

O cenário torna-se ainda mais crítico caso a transferência tecnológica seja facilitada pelo pagamento de vantagens indevidas a agentes públicos, sejam eles nacionais ou estrangeiros. Nessas hipóteses a EED atrai para si a Lei Anticorrupção[6], cujas sanções englobam elevadas multas pecuniárias, proibição de contratar com o governo e, em última instância, dissolução compulsória da empresa, podendo inclusive sofrer sanções transnacionais, caso o agente público seja de Estado estrangeiro.

[2] BRASIL. [Constituição (1988)]. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da República, [2026]. Art. 70, parágrafo único.

[3] BRASIL. Lei nº 12.527, de 18 de novembro de 2011.

[4] BRASIL. Decreto nº 7.845, de 14 de novembro de 2012.

[5] O Código Penal que estabelece como crime passível de reclusão de 3 (três) a 12 (doze) anos: "Entregar a governo estrangeiro, a seus agentes, ou a organização criminosa estrangeira, em desacordo com determinação legal ou regulamentar, documento ou informação classificados como secretos ou ultrassecretos nos termos da lei, cuja revelação possa colocar em perigo a preservação da ordem constitucional ou a soberania nacional". BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Código Penal. Art. 359-K. Incluído pela Lei nº 14.197, de 2021. e BRASIL e BRASIL. Lei nº 9.279, de 14 de maio de 1996

[6] BRASIL. Lei nº 12.846, de 1º de agosto de 2013.

Para evitar esse cenário, o Programa de Integridade atua como o principal mecanismo de calibração entre o dever de informar e o dever de proteger. Cabe às instâncias de compliance da EED estabelecer protocolos rígidos que permitam o atendimento às exigências de auditoria e *due diligence* inerentes à comprovação de conformidade exigida pelo Decreto nº 11.129/2022, sem que isso resulte na exposição de dados técnicos classificados. Assim, assegura-se que a transparência corporativa não se converta em uma vulnerabilidade para a retenção do conhecimento tecnológico no País, requisito essencial da Lei nº 12.598/2012.

A efetividade do Programa de Integridade é o pilar que sustenta a viabilidade da EED, mitigando riscos que ameaçam tanto a continuidade corporativa quanto a soberania nacional.

2. Alinhamento entre planejamento estratégico e manutenção do status de empresa estratégica de defesa

A Lei nº 12.598/2012, alterada pela Lei nº 14.459/2022, estabeleceu regras de descredenciamento mais rigorosas tornando a conformidade regulatória o pilar central da estratégia corporativa dessas organizações.

O planejamento estratégico de uma EED precisa estar alinhado às condições que a levaram ao credenciamento. Nesse sentido, a manutenção das condições definidas em lei[7] deve fazer parte do monitoramento dos programas de *compliance* formando uma barreira estratégica para evitar a perda de confiança ou falhas graves de segurança da informação.

Embora muitas EEDs sejam pessoas jurídicas de direito privado, suas decisões corporativas precisam estar alinhadas às condicionantes que lhes permitiram usufruir de condições especiais de tributação, contratação, dentre outras. O descumprimento dos requisitos para se beneficiar do Regime Especial Tributário para a Indústria de Defesa (RETID)[8], como, por exemplo, a não manutenção do *status* de "preponderantemente fornecedora", a irregularidade fiscal em relação aos impostos e contribuições administrados pela Secretaria da Receita Federal e o uso indevido da desoneração em produtos não estratégicos, pode gerar o descredenciamento.

Nesse sentido, a aplicação da isenção do RETID a produtos de uso comum, que não foram formalmente classificados, por meio da Portaria do Ministério da Defesa, como PRODE ou PED, pode acarretar exclusão do regime especial, multas altas e obrigatoriedade de devolução aos cofres públicos dos impostos não pagos. Esses são alguns exemplos que podem levar ao descredenciamento, comprometer a saúde da empresa, o nível de confiança do mercado, bem como levar à aplicação das sanções previstas na lei.

Os programas de integridade das EEDs, alinhados ao planejamento corporativo, pavimentam o caminho para uma avaliação segura de oportunidades, levando em consideração o panorama de projetos do setor e o peso estratégico de cada decisão.

A complexidade dessa avaliação estratégica é corroborada pelo recente entendimento do Tribunal de Contas

[7] BRASIL, 2022, art. 2º IV e XII parágrafo único.

[8] BRASIL, 2022, art 8º §1º e 2º e § 5º.

[9] TCU Acórdão 1918/2024 – Plenário: "(...) 9.1. conhecer da consulta, para responder ao Ministro de estado da defesa que, nas normas vigentes aplicáveis à aquisição, pelo Brasil, de produtos ou sistemas de defesa (Lei 12.598/2012, Decreto 9.607/2018 e Decreto 11.173/2022 – Tratado sobre o Comércio de Armas), não há restrição relativa a fornecedor que tenha sua sede em país em situação de conflito armado, seja quanto à sua participação em licitação, seja quanto à celebração ou a manutenção de contrato. (...)"

da União[9]. A Corte firmou a tese de que, pelas normas vigentes de aquisição de defesa, não há restrição automática para a contratação de fornecedores sediados em países em situação de conflito armado. Essa ausência de vedação prévia do Estado transfere para as EEDs a responsabilidade de realização de uma *due diligence* internacional exaustiva a fim de garantir que parcerias com empresas em zonas de conflito não violem as diretrizes de política externa e os compromissos internacionais ratificados pelo Brasil na área de defesa, sanções internacionais, embargos ou que exponham a segurança nacional a riscos geopolíticos que o próprio processo licitatório não filtrou.

3. Riscos de corrupção e a necessidade de integridade corporativa

As contratações no setor de defesa caracterizam-se por três aspectos: (I) pelo alto valor agregado; (II) pela complexidade tecnológica; e (III) pelo frequente envolvimento em negociações internacionais, fatores que elevam substancialmente a exposição a riscos de corrupção. Diante do avanço do arcabouço legal brasileiro no combate a esses ilícitos, o alinhamento das EEDs a essas normativas tornou-se essencial.

O Decreto nº 11.129, de 11 de julho de 2022, que regulamenta a Lei Anticorrupção, consolida a responsabilização objetiva administrativa e civil de pessoas jurídicas por atos lesivos contra a Administração Pública nacional ou estrangeira. Estabelece ainda rigorosos parâmetros para a aplicação de sanções e o cálculo de multas, além de definir os requisitos para a avaliação de programas de integridade, os quais podem servir como atenuantes legais.

Para que o Programa de Integridade se consolide como mecanismo de defesa e salvaguarda corporativa, o Capítulo V do Decreto nº 11.129/2022 exige que ele ultrapasse a barreira documental. É mandatório o comprometimento irrestrito da alta direção, a realização de análises de riscos periódicas e, fundamentalmente, a aplicação de diligências prévias rigorosas na contratação de terceiros, despachantes e representantes. No setor de defesa, no qual a cadeia de suprimentos é complexa e internacionalizada, essa diligência em relação a terceiros é o principal filtro contra a contaminação da EED por ilícitos alheios.

Destaca-se, ainda, que a legislação brasileira também alcança os atos lesivos praticados contra a administração pública estrangeira, ainda que cometidos no exterior. No mesmo sentido, as EEDs estão sujeitas ao alcance de rigorosas leis internacionais de combate à corrupção transnacional.

A natureza jurídica da EED, seja ela constituída com ou sem fins lucrativos[10], não oferece qualquer imunidade frente à legislação anticorrupção ou às sanções impostas por descredenciamento.

A inobservância das legislações nacionais ou estrangeiras sobre o tema e a ausência de um Programa de Integridade efetivo podem resultar em severas sanções, comprometendo a credibilidade da EED perante o Estado e inviabilizando sua continuidade operacional.

[10] BRASIL. Ministério da Defesa. Gabinete do Ministro. Portaria GM-MD nº 5.179, de 15 de dezembro de 2021. Credencia o Centro de Tecnologia da Indústria Química e Têxtil – SENAI CETIQT como Empresa Estratégica de Defesa (EED).

Conclusão

As reflexões aqui tratadas demonstram que a conformidade no âmbito das Empresas Estratégicas de Defesa (EEDs) transcende a visão tradicional baseada em conformidade legal para consolidar-se como o alicerce da governança corporativa e a salvaguarda da própria soberania nacional.

O ecossistema de riscos enfrentado por essas organizações, caracterizadas pela alta complexidade dos negócios envolvidos, constante tensão entre o dever de transparência e a imperatividade do sigilo, bem como necessidade de rigorosa prevenção a ilícitos e de observância do arcabouço regulatório, exige que a integridade esteja incorporada nas instâncias de decisão e nos mecanismos de supervisão. Ao converter a conformidade em um ativo estratégico que protege ativos críticos e sustenta a legitimidade institucional, as EEDs deixam de encarar o compliance como um ônus administrativo para assumi-lo como um investimento vital.

Eventuais falhas de integridade podem produzir repercussões severas, com potencial para desestabilizar a proteção dos interesses estratégicos do país. Por conseguinte, o aporte de recursos em programas de integridade robustos, aderentes às particularidades do setor de defesa, contribui para antecipar vulnerabilidades, promover a *accountability* perante os órgãos de controle e alinhar estratégia, integridade e interesse público. Essas medidas ratificam a confiabilidade das EEDs perante o poder público, além de atuarem como vetor essencial para a edificação de uma Base Industrial de Defesa ética e capacitada a responder aos imperativos da segurança nacional e a preservar a soberania nacional.

Referências

BRASIL. *Lei nº 14.459, de 21 de setembro de 2022*. Altera a Lei nº 12.598, de 21 de março de 2012, para estabelecer normas especiais para o descredenciamento de Empresas Estratégicas de Defesa (EED). Brasília, DF: Presidência da República, 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/lei/l14459.htm. Acesso em: 27 abr. 2026.

BRASIL. [Constituição (1988)] Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da República, [2023]. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 27 abr. 2026.

BRASIL. *Lei nº 12.527, de 18 de novembro de 2011*. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal. Brasília, DF: Presidência da República, 2011. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 18 out. 2026.

BRASIL. *Decreto nº 7.845, de 14 de novembro de 2012*. Regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento. Brasília, DF: Presidência da República, 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/decreto/d7845.htm. Acesso em: 27 abr. 2026.

BRASIL. *Decreto-Lei nº 2.848, de 7 de dezembro de 1940*. Código Penal. Brasília, DF: Presidência da República, 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 27 abr. 2026 e BRASIL.

BRASIL. *Lei nº 9.279, de 14 de maio de 1996*. Regula direitos e obrigações relativos à propriedade industrial. Brasília, DF: Presidência da República, 1996. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9279.htm. Acesso em: 27 abr. 2026.

BRASIL. *Lei nº 12.846, de 1º de agosto de 2013*. Dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira, e dá outras providências. Brasília, DF: Presidência da República, 2013. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12846.htm. Acesso em: 27 abr. 2026.

BRASIL. Tribunal de Contas da União (Plenário). *Acórdão nº 1918/2024*. Consulta sobre restrições a fornecedores sediados em países em conflito armado. Relator: Ministro Walton Alencar Rodrigues. Brasília, DF, 11 de setembro de 2024. Disponível em: https://pesquisa.apps.tcu.gov.br/. Acesso em: 27 abr. 2026.

BRASIL. *Decreto nº 11.129, de 11 de julho de 2022*. Regulamenta a Lei nº 12.846, de 1º de agosto de 2013, que dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira. Brasília, DF: Presidência da República, 2022. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/decreto/d11129.htm. Acesso em: 27 abr. 2026.

BRASIL. Ministério da Defesa. Gabinete do Ministro. *Portaria GM-MD nº 5.179, de 15 de dezembro de 2021*. Credencia o Centro de Tecnologia da Indústria Química e Têxtil – SENAI CETIQT como Empresa Estratégica de Defesa (EED). Brasília, DF: Ministério da Defesa, 2021. Disponível em: https://www.in.gov.br/web/dou/-/portaria-gm-md-n-5.179-de-15-de-dezembro-de-2021-368143456. Acesso em: 27 abr. 2026.

Ética na tomada de decisão:

como levar valores para as escolhas do dia a dia

Bárbara da Silva Barbosa

Bárbara da Silva Barbosa é profissional com experiência na área de Compliance, com atuação estratégica voltada à promoção da cultura de ética, integridade e aderência às normas e políticas corporativas. Possui trajetória consistente na estruturação, implementação e fortalecimento de Programas de Compliance, com foco em prevenção de riscos, disseminação de valores éticos e suporte à governança corporativa.

Atualmente atua como especialista de Compliance em uma das concessionárias de energia elétrica, com atuação na cidade do Rio de Janeiro, na implementação e monitoramento de controles internos, condução de avaliações de riscos, desenvolvimento de treinamentos e apoio a investigações internas. Possui MBA em Business Process pela Fundação Getulio Vargas (FGV), e é bacharel em Engenharia de Produção pelo Centro Federal de Educação Tecnológica Celso Suckow da Fonseca.

Michelle Moreira

Michelle Moreira é executiva em Compliance, Integridade e Investigações Corporativas, com mais de 15 anos de experiência em empresas multinacionais de diferentes segmentos. Possui sólida atuação na estruturação, implementação e monitoramento de Programas de Compliance, com foco em gestão de riscos, integridade corporativa e prevenção a fraudes. Recentemente, atuou como gerente de Compliance em uma concessionária de energia elétrica no Rio de Janeiro, liderando iniciativas voltadas ao fortalecimento da cultura ética e da conformidade regulatória. É graduada em Administração de Empresas e Ciências Contábeis, com pós-graduação em Auditoria e Controladoria. Atua como professora convidada em cursos de pós-graduação, é membro do Compliance Women Committee e membro independente do Comitê de Ética do Instituto Clima e Sociedade (iCS), além de disseminar conteúdo técnico por meio de seu canal no LinkedIn.

Introdução

Apresentação do problema

Em um cenário global de alta competitividade e dinâmicas complexas de mercado, a tomada de decisão corporativa é frequentemente confrontada com dilemas que desafiam os padrões éticos e morais. O ponto central deste artigo reside no desafio de alinhar os valores pessoais e a cultura de integridade organizacional com as escolhas práticas do cotidiano, sob a constante pressão por resultados.

Diante disso, busca-se compreender quais fatores efetivamente influenciam a tomada de decisão ética e como a cultura organizacional, reforçada por suas lideranças, pode traduzir as diretrizes teóricas de compliance em comportamentos práticos e íntegros no exercício das atividades laborais, no dia a dia.

Além disso, programas de compliance desempenham papel essencial na promoção da ética corporativa. De acordo com a Controladoria-Geral da União (2015), a efetividade desses programas está associada à atuação integrada de políticas, controles internos e ações voltadas à promoção da cultura de integridade nas organizações.

Objetivo geral

O objetivo deste artigo é analisar como os valores pessoais e os mecanismos de gestão ética corporativa moldam a tomada de decisão ética dos profissionais. Para tanto, exploram-se as práticas estruturantes necessárias para converter diretrizes de integridade em atitudes concretas, incorporando os valores éticos às escolhas estratégicas e operacionais do cotidiano nos negócios.

Objetivos específicos

- Explorar situações práticas do cotidiano empresarial que configuram dilemas éticos, com foco em áreas como gestão de riscos, compliance e relacionamento com terceiros.
- Discutir o papel dos códigos de ética corporativos e dos programas de compliance na orientação da tomada de decisão ética.
- Identificar as contribuições e limitações dos princípios éticos para a tomada de decisão nas organizações.

Justificativa

A relevância estratégica deste tema não se restringe ao ecossistema corporativo, mas se estende ao impacto que poderá ter na transformação da sociedade. No cenário contemporâneo, a maturidade ética direciona a tomada de decisão, tornando indispensável a preservação de padrões de conduta que assegurem a excelência e a dignidade nas relações de trabalho. Sob essa ótica, este artigo justifica-se pela oportunidade de oferecer aos profissionais de compliance e a outros grupos reflexões práticas e fundamentadas. O objetivo é potencializar alavancas de integridade para a construção de um ambiente de negócios mais funcional, sustentável e justo. Afinal, a consciência dos valores individuais e a consolidação de uma cultura ética corporativa são pilares fundamentais para mitigar riscos de desvios de conduta, ambições desmedidas e práticas ilícitas.

1. Desenvolvimento

1.1. Tomada de decisão ética no dia a dia

De acordo com Mauro, Cabral Capanema e Ramos (2021), que citam a nomenclatura "*arquitetura da decisão*", concepção construída por Thaler e Sunstein, grande parte das nossas decisões é realizada de forma rápida, automática e inconsciente; portanto, pequenas mudanças no contexto têm tudo para fazer a diferença. Imagine um cenário: você responde à um censo que autoriza sua família a doar seus órgãos em caso de alguma fatalidade. Suponha que sua família, infelizmente, teve que tomar a decisão de doar ou não os seus órgãos, porém não sabia quem seria o beneficiário por motivo de confidencialidade e de preservação de dados. Sua resposta seria a mesma caso soubesse que o beneficiário dos órgãos a serem doados fosse um criminoso e que esse criminoso também tivesse sido responsável pela morte de um ente da sua família? Percebem como pequenas mudanças no contexto podem interferir em nossas ações?

Fazendo um paralelo com o ambiente profissional, a eficácia da ética corporativa na tomada de decisão ética está intrinsecamente ligada à construção e à disseminação de valores no cerne da cultura organizacional. Conforme destaca o Instituto Brasileiro de Governança Corporativa (IBGC) (2023), a efetividade da governança corporativa depende da incorporação dos princípios éticos às práticas organizacionais, de modo que orientem efetivamente o comportamento dos colaboradores. Sendo assim, não é suficiente a mera formalização de normas e padrões de conduta, faz-se necessário investir em treinamentos contínuos, mecanismos eficazes de controle e aplicar, de forma consistente, sanções aos profissionais que violem os princípios éticos da organização.

Quando esses princípios são cocriados coletivamente ou estruturados por programas de integridade consistentes, amparados por mecanismos que estimulam o debate transparente de dilemas éticos em todos os níveis hierárquicos, o código de conduta deixa de ser um documento estático e passa a orientar, de fato, as decisões estratégicas e operacionais. Nessa perspectiva, Srour (2013) ressalta que a ética organizacional se consolida quando há coerência entre discurso institucional e práticas efetivas, sendo influenciada pelas estruturas de poder e pelos padrões culturais internos.

Nesse contexto, a área responsável por compliance atua como a principal guardiã da cultura, desempenhando um papel estratégico tanto na prevenção de inconformidades quanto na promoção de um ambiente seguro, íntegro e confiável. A seguir, são apresentadas situações práticas do cotidiano empresarial, extraídas de situações reais que podem ser vivenciadas no ambiente corporativo, as quais ilustram os desafios e as oportunidades para amadurecer a prática ética nas organizações.

1.2 Dilemas de vendas e metas

A pressão pelo atingimento de metas pode comprometer a integridade das decisões organizacionais, especialmente quando o desempenho é priorizado em detrimento de princípios éticos. De acordo com o IBGC (2023), a ausência de alinhamento entre resultados e valores organizacionais pode fragilizar a cultura de integridade. Nesse contexto, metas excessivas tendem a tornar difusa a linha entre práticas legítimas e inadequadas.

Um reflexo prático desse desafio manifesta-se em relatos de 'manobras operacionais' para inflar artificialmente os indicadores de performance. Um exemplo comum é a situação em que, diante do receio de descontinuidade do vínculo empregatício, o colaborador pode praticar atos que culminam em fraudes operacionais, como a manipulação de reversões de cancelamentos e a utilização indevida de dados de terceiros (como CPFs de familiares) para simular novas vendas. Nesse cenário, a tomada de decisão ética exige do profissional um raciocínio crítico rigoroso para discernir a legalidade e a moralidade de suas ações, compreendendo que a pressão institucional não exime o indivíduo da responsabilidade por sua conduta. A responsabilidade pela decisão ética permanece com o indivíduo, sendo indispensável o desenvolvimento de um raciocínio crítico capaz de distinguir legalidade e

legitimidade moral, mesmo em contextos adversos.

Diante desse contexto, cabe às organizações estruturar ambientes que incentivem a integridade, assegurando que o cumprimento de metas não se sobreponha aos princípios éticos. Conforme orienta a Controladoria-Geral da União (2015), programas de integridade eficazes devem alinhar incentivos, controles e cultura organizacional, promovendo não apenas a prevenção de irregularidades, mas também a valorização de comportamentos éticos.

Assim, práticas inadequadas devem ser prevenidas por meio de controles internos robustos, monitoramento contínuo e treinamentos regulares, bem como corrigidas mediante a aplicação consistente de sanções. Além disso, a responsabilização efetiva, incluindo medidas disciplinares e, quando necessário, o desligamento de colaboradores, mostra-se essencial para a preservação da confiança, da reputação institucional e da sustentabilidade dos negócios.

1.3 Favorecimento e conflitos de interesse

Usualmente, a área de compras das organizações demanda alto grau de governança e discernimento. O conflito de interesses e o consequente dilema ético manifestam-se quando ambições pessoais ou o favorecimento de terceiros sobrepõem-se aos princípios de isonomia, transparência e busca pela melhor proposta para a organização.

Segundo o IBGC (2023), a adequada gestão de conflitos de interesse está associada ao fortalecimento das práticas de governança, especialmente por meio da transparência, da equidade e da responsabilização nos processos decisórios. Adicionalmente, a CGU (2015) reforça a importância da *due diligence* e da responsabilização, como forma de a empresa agir proativamente na identificação de potenciais conflitos.

Um caso emblemático que pode ser citado como exemplo é uma situação que evidencia indícios substanciais de direcionamento e favorecimento em processos concorrenciais. O *modus operandi* consistia no vazamento de informações estratégicas de custos e orçamentos de obras por parte de uma colaboradora interna a um fornecedor específico. Tal dinâmica resultava em benefícios financeiros indevidos para as partes envolvidas, caracterizando um cenário típico de conluio, prática frequentemente associada a falhas nos mecanismos de governança e controle.

Sob a perspectiva de compliance, essa conduta configura um caso de corrupção privada, na medida em que compromete a imparcialidade dos processos decisórios e viola princípios fundamentais de integridade, transparência e equidade. De acordo com a Controladoria-Geral da União (2015), situações dessa natureza evidenciam fragilidades nos mecanismos de integridade organizacional, especialmente quando inexistem controles eficazes ou quando há falhas na supervisão. Ademais, conforme argumenta Srour (2013), práticas dessa natureza tendem a emergir em contextos organizacionais nos quais interesses individuais se sobrepõem às diretrizes institucionais, refletindo distorções na cultura e no exercício do poder.

Diante desse contexto, a atuação da função de compliance deve ser pautada pela condução de investigações rigorosas, com adequada coleta, análise e documentação de evidências, assegurando a consistência e a rastreabilidade das conclusões. Paralelamente, torna-se imperativo fortalecer instrumentos preventivos, como processos estruturados de *due diligence* de terceiros, a adequada segregação de funções e a implementação de controles internos capazes de mitigar conflitos de interesse. Nesse sentido, o IBGC (2023) destaca que a efetividade da governança corporativa depende diretamente da qualidade dos mecanismos de controle e da responsabilização dos agentes envolvidos nos processos decisórios.

Por fim, a aplicação consistente de medidas disciplinares, incluindo, quando cabível, o afastamento de colaboradores, é essencial para preservar a credibilidade institucional e reforçar uma cultura organizacional orientada à integridade. Nesse sentido, a Controladoria-Geral da União (2015) destaca que a efetividade dos programas de integridade depende da adequada responsabilização em casos de desvios, enquanto o IBGC (2023) reforça que a credibilidade das práticas de governança está diretamente associada à consistência na aplicação de regras e na responsabilização dos agentes envolvidos.

1.4 Gestão de recursos e desvios éticos

No último reporte "Occupational Fraud 2026", da instituição internacional Association of Certified Fraud Examiners (ACFE), 90% dos casos reportados associados aos atos antiéticos se referiam à prática de apropriação indébita de ativos, indicando uma perda financeira, em média de, 100 mil dólares.

Por isso, destacamos que a gestão de despesas corporativas e a transparência no uso de recursos institucionais constituem testes diários para a tomada de decisão ética. Desvios de conduta nessa frente exemplificam como a fragilidade dos valores individuais pode se traduzir em fraudes operacionais severas contra o patrimônio da organização.

Esses comportamentos, além de gerar perdas financeiras, contribuem para a deterioração da cultura organizacional, criando um ambiente permissivo a irregularidades (IBGC, 2023).

Um outro exemplo típico é que, em auditorias de reembolsos de despesas de viagens corporativas, são frequentemente identificadas não conformidades críticas, como gastos desproporcionais com hospedagens de luxo e alimentação, além da emissão de passagens aéreas cujos itinerários e calendários coincidem sistematicamente com finais de semana e feriados, sem justificativa de negócios. A gravidade desses cenários costuma ser amplificada pelo envolvimento ou pela conivência de lideranças que, ao aprovarem relatórios financeiros inconsistentes ou lastreados em documentação inidônea, falham em seu dever de supervisão, comprometendo os controles internos para encobrir as irregularidades.

Nesses casos, a tomada de decisão ética do indivíduo é corrompida pela busca por vantagens financeiras ilícitas, resultando em prejuízos financeiros significativos e na degradação do ambiente de controle.

Com base em pesquisa realizada pela Grant Thornton, "Diagnósticos das fraudes no Brasil" ([2024?]), 94% dos respondentes indicam a oportunidade como principal fator que influência ocorrências de fraude. Ressalta-se a importância de reforçar os mecanismos internos para combater a ocorrência de fraudes e evitar repetições no futuro. Diante desse fato, é prudente implementar ações, tais como realização de auditorias-surpresa, revisão/supervisão efetiva da gestão e monitoramento e análise de dados de forma proativa.

Conclusão

A análise desenvolvida evidencia que a tomada de decisão ética no ambiente corporativo é influenciada por múltiplos fatores interdependentes, incluindo valores individuais, cultura organizacional, liderança e mecanismos de controle.

Embora os programas de compliance sejam fundamentais, sua eficácia depende da internalização dos valores éticos e do alinhamento entre incentivos organizacionais e princípios de integridade. Ambientes marcados por pressão excessiva por resultados, falhas de governança e fragilidade cultural tendem a aumentar o risco de desvios.

Dessa forma, conclui-se que a construção de uma cultura ética sólida exige atuação integrada entre liderança, políticas corporativas e mecanismos de controle. Organizações que promovem ambientes seguros para decisões éticas tendem a apresentar maior sustentabilidade e resiliência.

Referências

ASSOCIATION OF CERTIFIED FRAUD EXAMINERS (ACFE). *Occupational fraud 2026*: a report to the nations. [*S. l.*]: ACFE, 2026. Disponível em: https://www.acfe.com/-/media/files/acfe/pdfs/rttn/2026/2026-report-to-the-nations.pdf. Acesso em: 22 maio 2026.

BRASIL. Controladoria-Geral da União. Programa de integridade: diretrizes para empresas privadas. Brasília, DF: CGU, 2015. Disponível em: https://www.gov.br/cgu/pt-br/centrais-de-conteudo/publicacoes/integridade/arquivos/programa-de-integridade-diretrizes-para-empresas-privadas.pdf. Acesso em: 10 out. 2026.

GRANT THORNTON BRASIL. Diagnóstico das fraudes no Brasil. [*S. l.*]: Grant Thornton Brasil, [2024?]. Disponível em: https://www.grantthornton.com.br/insights/diagnostico-de-fraudes-no-brasil/. Acesso em: 21 jun. 2026.

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA (IBGC). *Código das melhores práticas de governança corporativa*. 6. ed. São Paulo: IBGC, 2023.

MAURO, Carlos; CABRAL, Gabriel; CAPANEMA, Renato; RAMOS, Tânia. MUITOS: Como as ciências comportamentais podem tornar os programas de compliance anticorrupção mais efetivos? [*S. l.*]: Editora Brasileira; World Observatory, 2021.

SROUR, Robert Henry. *Ética empresarial*. Rio de Janeiro: Elsevier, 2013.

Governança e compliance tributário no novo cenário fiscal:

caminhos para segurança jurídica e competitividade empresarial

Gisela Gadelha

Gisela Gadelha é diretora da Federação das Indústrias do Estado do Rio de Janeiro (Firjan). Conselheira da Turma Ordinária 3401, especialista em Direito Aduaneiro, da 3ª Seção de Julgamento do Conselho Administrativo de Recursos Fiscais (CARF). Membro do Conselho de Representantes do Centro Brasileiro de Mediação e Arbitragem (CBMA). Professora convidada da FGV – Rio. Mestre em Ciências Jurídicas pela Universidade Autônoma de Lisboa. Possui diversos artigos publicados. Ex-vice-presidente do Conselho de Contribuintes do Estado do Rio de Janeiro.

Introdução

O sistema tributário brasileiro é amplamente reconhecido por sua complexidade e constante mutabilidade, impondo desafios significativos às organizações. Nesse contexto, a governança e o compliance tributário emergem como instrumentos fundamentais para assegurar o cumprimento das obrigações fiscais e mitigar riscos associados à não conformidade.

Há décadas discute-se a necessidade de aprimoramento do sistema tributário nacional. A complexidade do modelo federativo, a distribuição desproporcional da carga tributária entre os diversos setores da economia, bem como as distorções e privilégios criados pelo sistema vigente, tornaram a reforma tributária um tema de difícil solução política.

De acordo com dados do Banco Mundial[1], enquanto entre 2009 e 2019, o PIB do Brasil cresceu, em média, apenas 1,3% ao ano, o restante do mundo teve crescimento médio de 2,8% ao ano[2]. São muitas as causas dessa perda de produtividade da economia brasileira, mas o tamanho e a complexidade do sistema tributário nacional certamente têm um papel importante.

Em que pese a dificuldade de reorganizar um sistema fortemente constritivo no qual, desde a promulgação da Constituição de 1988, foram editadas, em média, 2,21 normas tributárias por hora de dia útil, o Congresso Nacional aprovou as tão celebradas Emenda Constitucional nº 132/2023 e a Lei Complementar nº 214/2025.

A promulgação da Emenda Constitucional nº 132 de 2023 instituiu uma profunda reformulação desse modelo ao prever a substituição gradual desses tributos por dois novos impostos sobre valor agregado: a Contribuição sobre Bens e Serviços (CBS) e o Imposto sobre Bens e Serviços (IBS).

Gabriela Conca[3] traz uma visão ampla das mudanças introduzidas pela reforma tributária:

> As mudanças propostas pelo novo modelo de tributação do consumo consiste essencialmente, na instituição de: (i) tributos com base ampla de incidência, que englobe a prestação de serviços operações com bens tangíveis e intangíveis; (ii) alíquotas uniformes que deverão ser aplicadas indistintamente a todas as operações; (iii) tributação no destino, deslocando a competência ativa para o ente onde se concretiza o consumo; e (iv)não cumulatividade plena, permitindo-se a tomada de créditos de forma ampla, com exceção de créditos decorrentes de operações envolvendo bens de uso e consumo pessoal. Estas mudanças prometem pôr fim à guerra fiscal entre Estados e Municípios, bem como eliminar uma série de disputas relativas à qualificação jurídica da operação, alíquota aplicável e formação de resíduos tributários (Conca, 2025, p. 261-284).

A Reforma Tributária, ao instituir o Imposto sobre Valor Agregado (IVA) dual — composto pela Contribuição sobre Bens e Serviços (CBS) e pelo Imposto sobre Bens e Serviços (IBS) —, promove avanços relevantes em termos de simplificação, neutralidade, transparência e isonomia entre os setores econômicos.

Como ensinam Cristiane Mcnaughton e Charles Mcnaughton[4]:

> A ideia de neutralidade exprime a noção de que a tributação não deveria interferir no modo em que os agentes econômicos atuam.
>
> A neutralidade se manifesta no IBS e na CBS de diversas maneiras. A primeira delas é a "não-cumulatividade", prevista no inciso VII do §1º do art. 156-A do Texto Maior. A não cumulatividade exige que tributos plurifásicos, como o IBS e a CBS, não criem distintas cargas tributárias em razão do nú-

[1] BANCO MUNDIAL. *World Development Indicators*: GDP growth (annual %). Washington, DC: World Bank, [2026?]. Disponível em: https://data.worldbank.org/indicator/NY.GDP.MKTP.KD.ZG. Acesso em: 15 maio 2026.

[2] Federação das Indústrias do Estado do Rio de Janeiro (FIRJAN). *Reforma tributária*: um marco para a indústria e para o desenvolvimento econômico do Brasil. Rio de Janeiro: Firjan, 2025. Disponível em: https://www.firjan.com.br/data/files/E0/A7/37/A7/CDD87910734FAA69D8284EA8/Cartilha%20Reforma%20Tributaria_DIGITAL_vF.pdf. Acesso em: 18 out. 2026.

[3] CONCA, Gabriela. Os novos tributos sobre o consumo no Brasil: contornos do fato gerador do IBS e da CBS. *In*: DE SANTI, Eurico Marcos Diniz (org.). *Análise e comentários sobre a reforma tributária do Brasil*: EC 132/2023 e LC 214/2025. São Paulo: Editora JusPodivm, 2025. p. 261-284.

[4] MCNAUGHTON, Cristiane Pires; MCNAUGHTON, Charles William. *Curso de IBS e CBS*: de acordo com a EC 132/2023 e com a LC 214/2025. 1. ed. São Paulo: Noeses, 2025. p. 17-18.

> mero de etapas em um ciclo econômico. Ou seja, se certo bem ou serviço for alienado ou prestado uma única vez, a carga tributária deve ser exatamente a mesma do que se houvesse diversas vendas. (...) A própria exceção da não cumulatividade, que é o uso e consumo pessoal, também foi concebida buscando a neutralidade, evitando que pessoas jurídicas sejam constituídas para permitir o consumo final sem a oneração dos gravames (Mcnaughton; Mcnaughton, 2025, p. 17-18)

Por meio da Emenda Constitucional nº 132/2023 e da Lei Complementar nº 214/2025, foram estabelecidas regras específicas para a implementação do novo sistema. O novo regime terá início em 2026, com conclusão prevista para 2033. Durante esse período de transição, as empresas deverão conviver com dois regimes distintos, nos quais os novos tributos serão gradualmente introduzidos, em concomitância com aqueles que serão extintos.

A crescente digitalização da administração tributária, aliada ao fortalecimento dos mecanismos de fiscalização, exige das empresas maior rigor na gestão de suas informações fiscais. Nesse cenário, torna-se imprescindível a adoção de práticas estruturadas que integrem processos, pessoas e tecnologia.

O presente artigo tem como objetivo analisar a importância da governança e do compliance tributário no novo cenário fiscal, especialmente durante o período de transição da reforma tributária, previsto até 2033, destacando seus impactos na segurança jurídica e na competitividade empresarial.

1. O novo cenário fiscal

O ambiente fiscal contemporâneo é marcado por profundas transformações decorrentes de reformas legislativas e avanços tecnológicos. A implementação de sistemas digitais de controle, como o Sistema Público de Escrituração Digital (SPED), e a futura adoção do mecanismo de *split payment*[5] ampliam significativamente a capacidade de fiscalização do Estado. Paralelamente, a intensificação da transparência e do intercâmbio de informações entre as administrações tributárias contribui para a redução de práticas evasivas e para o aumento dos níveis de conformidade fiscal.

Nesse contexto, as propostas de simplificação tributária e de reestruturação da tributação sobre o consumo sinalizam mudanças relevantes no modelo vigente, tendo como uma de suas principais diretrizes a neutralidade tributária, materializada, entre outros aspectos, pela adoção da tributação no destino. Essas transformações exigem das empresas maior capacidade de adaptação, bem como a revisão de suas estratégias fiscais, operacionais e de conformidade regulatória.

Diante desse cenário, a governança tributária assume papel central como instrumento de gestão estratégica. Mais do que assegurar o cumprimento das obrigações fiscais, ela compreende um conjunto de práticas voltadas à definição de responsabilidades, gestão de riscos, estabelecimento de políticas internas, transparência e monitoramento contínuo das atividades tributárias. Sob essa perspectiva, a tributação deixa de ser tratada apenas como uma função operacional e passa a integrar o processo decisório das organizações, influenciando aspectos relacionados à segurança jurídica, à reputação institucional e à sustentabilidade dos negócios.

O compliance tributário, por sua vez, refere-se à observância das normas fiscais vigentes, abrangendo tanto as obrigações principais quanto as acessórias. Sua implementação envolve a adoção de controles internos, auditorias periódicas, capacitação de profissionais e utilização de tecnologias capazes de aprimorar a gestão das obrigações fiscais e reduzir falhas operacionais. Tais medidas tornam-se ainda mais relevantes diante

[5] *Split payment* é um mecanismo de liquidação financeira em que o valor de uma transação é automaticamente dividido entre duas ou mais partes no momento do pagamento, seguindo regras pré-definidas. Em vez de o valor total ser creditado a um único recebedor e posteriormente redistribuído, o sistema direciona cada parcela diretamente aos respectivos beneficiários

das exigências introduzidas pela reforma tributária, que demandam maior integração de sistemas, rastreabilidade das operações, gerenciamento de dados em tempo real e adaptação a novos procedimentos de apuração e cumprimento das obrigações tributárias.

As alterações promovidas pela reforma tributária também reforçam a importância da não cumulatividade como instrumento de neutralidade econômica e eficiência produtiva. Nesse sentido, Sérgio Wulff Gobetti destaca que a tributação em cascata gera distorções alocativas ao incentivar a internalização de atividades produtivas em detrimento da formação de cadeias de fornecedores mais eficientes. Segundo o autor, além de comprometer a neutralidade tributária, a cumulatividade reduz a produtividade e o potencial de crescimento econômico, razão pela qual a reforma buscou fortalecer a não cumulatividade mediante a ampliação do direito ao crédito financeiro, a adoção de uma base tributária mais ampla e a consolidação do princípio do destino como critério de tributação. Nesse sentido, Sérgio Wulff Gobetti[6] ressalta:

> Para as cadeias produtivas mais sofisticadas, inclusive no setor de serviços, a cumulatividade é um grave problema. Quando a tributação incide em cascata, as empresas são induzidas a internalizar atividades produtivas e assim economizar no pagamento de impostos, ao invés de se organizar em arranjos produtivos com cadeias de fornecedores mais eficientes. Não se trata, portanto, de meramente ferir um dos princípios básicos da boa tributação, que é a neutralidade, mas também de introduzir ineficiências que reduzem a produtividade e o potencial de crescimento da economia como um todo. Problema este que tende a se agravar no futuro, na medida em que os setores econômicos intensifiquem o uso de serviços. Infelizmente, mesmo os tributos brasileiros concebidos sob o princípio da não cumulatividade são imperfeitamente "não cumulativos", e a reforma tributária enfrentou tal deficiência, garantindo crédito financeiro irrestrito, evoluindo para uma base tributária ampla e adotando o princípio do destino, medidas fundamentais para viabilizar a plena não cumulatividade sistêmica. Em relação ao cenário atual em que a fragmentação da base tributária gera "cumulatividade" cruzada, e o princípio da origem no ICMS cria dificuldades operacionais para o pleno aproveitamento do crédito (Gobetti, 2025, p. 211-212).

Sob essa perspectiva, o planejamento tributário assume relevância ainda maior no ambiente pós-reforma. A possibilidade de empresas optantes pelo Simples Nacional escolherem o regime regular de apuração da CBS e do IBS, permanecendo no regime simplificado em relação ao IRPJ, à CSLL e à CPP, evidencia a necessidade de avaliações tributárias mais sofisticadas e alinhadas aos objetivos empresariais. A decisão deverá considerar fatores como a estrutura de custos da empresa, seu posicionamento na cadeia de valor, a capacidade de aproveitamento de créditos tributários e os impactos concorrenciais decorrentes da sistemática de creditamento.

A gestão eficiente da carga tributária produz reflexos diretos sobre a rentabilidade das operações, a formação de preços, a capacidade de investimento e a competitividade empresarial. Custos tributários excessivos ou inadequadamente administrados podem comprometer a lucratividade e limitar oportunidades de expansão, ao passo que uma estrutura tributária adequadamente planejada pode gerar ganhos de eficiência econômica e vantagens competitivas sustentáveis. Além disso, organizações que demonstram elevado grau de conformidade tendem a reduzir sua exposição a autuações e litígios fiscais, fortalecer a segurança jurídica de suas operações e consolidar sua credibilidade perante investidores, parceiros comerciais e órgãos reguladores.

Para assegurar maior eficiência na gestão tributária e conformidade com as exigências regulatórias, recomenda-se a adoção de diretrizes estruturadas de governança e compliance, dentre as quais se destacam: (i) o engajamento da alta administração na definição de estratégias e na promoção de uma cultura organizacional voltada à integridade e à conformidade tributária; (ii) o investimento em tecnologia e sistemas de automação capazes de aprimorar o controle, a apuração e o monitoramento das

[6] GOBETTI, Sérgio Wulff. As diferentes dimensões econômicas dos impactos positivos da reforma tributária. *In*: SANTI, Eurico Marcos de (coord.). *Análise e comentários sobre a reforma tributária do Brasil*: EC 132/2023 e LC 214/2025. São Paulo: JusPodivm, 2025. p. 209-222.

obrigações fiscais; (iii) a capacitação contínua dos profissionais envolvidos, de modo que se assegure atualização permanente diante das frequentes alterações legislativas e regulatórias; (iv) o acompanhamento sistemático da legislação e da jurisprudência tributária, permitindo a identificação tempestiva de riscos e oportunidades; e (v) a implementação de controles internos eficazes, voltados à prevenção de inconsistências, à mitigação de riscos fiscais e ao fortalecimento da segurança jurídica das operações empresariais.

Conclusão

A governança e o compliance tributário consolidam-se como elementos essenciais no atual cenário fiscal brasileiro. Mais do que instrumentos de atendimento às exigências legais, configuram-se como pilares da gestão estratégica, integrando dimensões operacionais, financeiras, reputacionais e de sustentabilidade.

Ao incorporar mecanismos de supervisão, gestão de riscos, transparência e tomada de decisão estruturada, a governança tributária eleva o tema fiscal ao nível estratégico das organizações. Nesse contexto, empresas que investem nessas práticas mostram-se mais preparadas para enfrentar a complexidade do sistema tributário, adaptar-se às mudanças legislativas e explorar oportunidades de forma ética, eficiente e sustentável.

Além disso, o compliance tributário revela-se relevante fator de competitividade empresarial. Organizações que demonstram elevado grau de conformidade tendem a fortalecer sua reputação perante investidores, parceiros comerciais e autoridades fiscais, ampliando a confiança do mercado e criando condições mais favoráveis para expansão de negócios e atração de investimentos.

Sob essa perspectiva, observa-se que o planejamento tributário, aliado às boas práticas de governança e compliance, deixa de ter caráter meramente operacional e passa a integrar a estratégia corporativa das empresas. As novas possibilidades introduzidas pela reforma tributária, especialmente no que se refere à sistemática de creditamento da CBS e do IBS, evidenciam a necessidade de análises técnicas e estratégicas capazes de identificar oportunidades legítimas de otimização fiscal e aumento da competitividade.

Portanto, empresas que investem em governança e compliance tributário encontram-se mais preparadas para enfrentar os desafios do sistema tributário contemporâneo, explorando oportunidades de crescimento de forma sustentável, ética e alinhada às exigências regulatórias. Por conseguinte, se tornam mais competitivas e asseguram sua perenidade em um ambiente de crescente complexidade fiscal.

Referências

BRASIL. *Constituição (1988)*. Constituição da República Federativa do Brasil. Brasília, DF: Senado Federal, 1988.

BRASIL. Lei nº 5.172, de 25 de outubro de 1966. Código Tributário Nacional. *Diário Oficial da União*: seção 1, Brasília, DF, 27 out. 1966.

GOBETTI, Sérgio Wulff. As diferentes dimensões econômicas dos impactos positivos da reforma tributária. *In*: SANTI, Eurico Marcos de (coord.). *Análise e comentários sobre a reforma tributária do Brasil*: EC 132/2023 e LC 214/2025. São Paulo: JusPodivm, 2025. p. 209-222.

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA (IBGC). *Código das melhores práticas de governança corporativa*. São Paulo: IBGC, 2015.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD). *Tax compliance by design*: achieving improved SME tax compliance by adopting a system perspective. Paris: OECD Publishing, 2014. DOI: https://doi.org/10.1787/9789264223219-en.

SILVA, José Afonso da. *Curso de direito constitucional positivo*. 37. ed. São Paulo: Malheiros, 2014.

TORRES, Heleno Taveira. *Direito tributário e governança fiscal*. São Paulo: Revista dos Tribunais, 2018.

A cultura da integridade como diferencial estratégico:

o impacto do marco legal e de iniciativas de fomento na governança empresarial

Cristine Köhler Ganzenmüller

Cristine Köhler Ganzenmüller é auditora Federal da Controladoria-Geral da União – CGU desde 2006, onde ocupa atualmente a função de diretora de Promoção e Avaliação de Integridade Privada. Na CGU também atuou coordenadora de Promoção de Integridade, chefe na Coordenação de Negociação de Acordos de Leniência, chefe de Núcleo de Auditoria e Fiscalização e ainda corregedora dos Ministérios da Cultura e do Esporte. Possui experiência como advogada corporativa em período anterior ao ingresso na CGU. É graduada em Direito pela Universidade Federal do Paraná (UFPR) e tem MBA em Direito Econômico e Empresarial pela Fundação Getúlio Vargas (FGV) e certificação CPC-A pela LEC.

Monique Cerqueira Zuidema

Monique Cerqueira Zuidema é auditora Federal de Finanças e Controle da CGU desde 2022. Atualmente, ocupa o cargo de coordenadora-geral de Promoção de Integridade Privada. Atuou anteriormente na Coordenação-Geral de Programas de Integridade da Secretaria de Integridade Pública da CGU, desenvolvendo projetos junto a organismos internacionais. Possui graduação em Engenharia Naval e Oceânica pela Universidade Federal do Rio de Janeiro (UFRJ).

1. A mudança de paradigma: a integridade como vetor de competitividade e sustentabilidade

A ideia de sucesso empresarial sempre esteve intrinsecamente ligada à maximização de lucros e à eficiência produtiva, muitas vezes operando em uma lógica na qual um ambiente ético e uma cultura íntegra eram vistos como elementos secundários ou sem retorno efetivo.

No entanto, as transformações sociais ocorridas nas últimas décadas trouxeram uma nova realidade: em um mundo hiperconectado e de vigilância social constante, com a evolução legislativa para a responsabilização empresarial, a integridade deixou a de ser um tema secundário para se tornar um elemento central na governança das empresas. A confiança e a reputação passaram a ser algumas das moedas mais valiosas do mercado, seja para a imagem reputacional, seja para a proteção da própria organização. Quando uma empresa negligencia seus pilares éticos, ela não coloca em risco apenas sua reputação, mas sua própria viabilidade existencial. Nesse cenário, a integridade corporativa deve ser compreendida não como um conjunto de restrições e dificuldades, mas como uma diretriz estratégica que orienta a inovação, a segurança jurídica e a perenidade existencial da própria organização.

Essa percepção de que a ética traz retorno para a empresa é corroborada por evidências robustas. Dados do Ethisphere Institute revelam que as empresas reconhecidas como as mais éticas do mundo superam consistentemente o desempenho financeiro das listadas no índice S&P 500, demonstrando que a integridade atua como um acelerador de valor no longo prazo. Esse impacto reflete-se com igual intensidade no capital humano. De acordo com o relatório "State of the Global Workplace 2025", da Gallup, organizações que adotam as melhores práticas de governança e transparência alcançam um índice de engajamento de 70%, em contraste com a média global de apenas 21%. Além disso, a integridade se tornou um divisor de águas na "guerra por talentos": pesquisas da Deloitte indicam que 44% dos profissionais das gerações mais jovens já rejeitaram propostas de trabalho por discordarem dos valores éticos da organização, e um terço dos colaboradores consideraria deixar seu emprego atual se a empresa não demonstrasse um compromisso claro com valores sustentáveis e íntegros. Além disso, inúmeras empresas reconhecidas pelo Programa "Pró-Ética" da CGU relatam ter se diferenciado em termos de imagem nas escolhas feitas pelos seus parceiros comerciais e investidores do negócio, em razão de possuírem o selo.

2. Conformidade que gera valor: o papel da integridade empresarial no cenário regulatório brasileiro

Acompanhando essa mudança de paradigma global, o Brasil introduziu a temática da integridade corporativa em seu panorama jurídico com a promulgação da Lei nº 12.846/2013 (a Lei Anticorrupção). Este diploma legal foi responsável por institucionalizar o conceito de "Programa de Integridade" no cotidiano corporativo nacional. Ao estabelecer a responsabilidade objetiva das pessoas jurídicas, a lei reforçou o dever de monitoramento e controle por parte dos dirigentes, já que agora, a empresa responde por atos lesivos contra a administração pública, nacional ou estrangeira, independentemente da comprovação de dolo ou culpa de seus gestores. A legislação e regulamentação correspondente também buscaram incentivar as empresas a implementarem ou aperfeiçoarem mecanismos internos de integridade, oferecendo redução no valor de multas aplicáveis no âmbito dos processos de responsabilização e de acordos de leniência. Ademais, é de se apontar o aspecto preventivo,

no qual se nota que as empresas que possuem um programa de integridade estruturado possuem condições mais efetivas para se proteger e para responder tempestivamente a eventuais intercorrências reputacionais e envolvimento em irregularidades, para além do aspecto meramente corretivo.

Mais recentemente, a temática da integridade empresarial no Brasil passou por outra importante evolução com a publicação da Nova Lei de Licitações e Contratos (NLLC - Lei nº 14.133/2021). Esse normativo exige que, para contratações de grande vulto (no momento, acima de R$ 260 milhões), a adoção de programas de integridade seja obrigatória. Essa obrigação esta também se aplica aos entes subnacionais, para além da esfera federal. Complementarmente, o normativo estabelece incentivos reais: a implantação de programas de integridade atua como critério de desempate entre propostas e configura requisito para a reabilitação de empresas penalizadas por irregularidades.

Esse cenário regulatório, somado à crescente pressão da sociedade por condutas mais éticas e transparentes nas relações público-privado, transformou a integridade em um ativo estratégico. Diante de um mercado que pune reputações manchadas e exige transparência e boas práticas, as empresas passaram a demonstrar um interesse crescente na implementação de programas de integridade.

3. Iniciativas da CGU como instrumentos de apoio para a implementação de programas de integridade efetivos

Antecipando-se a esses movimentos legislativos, a Controladoria-Geral da União (CGU) já atuava na vanguarda do fomento à integridade com o programa Empresa Pró-Ética. Com o objetivo de reconhecer as melhores práticas em programas de integridade, em 2010, por ocasião do Dia Internacional de Combate à Corrupção foi apresentado o Pró-Ética, em parceria com o Instituto Ethos. O Pró-Ética é uma iniciativa única na América Latina, muito respeitada dentro e fora do país, que busca fomentar a adoção voluntária de medidas de integridade pelas empresas, por meio do reconhecimento público daquelas que, independentemente do porte e do ramo de atuação, mostram-se comprometidas em implementar medidas voltadas a prevenção, detecção e remediação de atos relacionados a corrupção, fraude, violação socioambiental e desrespeito aos direitos humanos. A iniciativa permite que as empresas tenham seus programas de integridade avaliados pela CGU, de acordo com metodologia e diretrizes definidas pelo órgão, não se limitando a uma análise burocrática e teórica, exigindo-se evidências de que as medidas de integridade são efetivas e apresentam efeitos na prática diária da empresa. Adicionalmente, as empresas inscritas recebem um relatório com a avaliação detalhada de seu Programa de Integridade, realizada e revisada por auditores da CGU, indicando os pontos que não obtiveram desempenho adequado e contendo recomendações de melhoria e aperfeiçoamento.

Essa iniciativa foi muito bem aceita pelo mercado nacional, sendo também reconhecida internacionalmente: a Organização de Estados Americanos (OEA) classifica o Pró-Ética como uma "excelente prática" adotada pelo Brasil; a Organização para a Cooperação e Desenvolvimento Econômico (OCDE) reconhece-o como 'um esforço positivo do governo brasileiro' na área de fomento à integridade. A United Nations Office on Drugs and Crime (UNODC) afirma que é um dos melhores exemplos internacionais de incentivos voluntários à integridade corporativa. A Sociedade de Integridade e Ética Corporativa dos Estados Unidos (SCCE) premiou a CGU pelo trabalho do Pró-Ética, tendo sido o primeiro órgão governamental da América Latina a receber essa distinção.

Até esta última edição (2025-2026), o Pró-Ética contou com aproximadamente 1.300 candidaturas inscritas ao prêmio e mais de 400 empresas premiadas e reconhecidas publicamente pela CGU. Atualmente é sinônimo de excelência em integridade empresarial, servindo como um indutor para a implementação e o aperfeiçoamento de boas práticas em centenas de empresas, inclusive as empresas estatais.

A experiência acumulada pela CGU em suas diversas frentes de atuação relacionadas à integridade no setor privado, seja em processos de responsabilização ou iniciativas de fomento, como o Pró-Ética, permitiu ao órgão perceber que o tema ainda era tratado de forma incipiente ou nem era tratado pela grande maioria das empresas e entidades privadas brasileiras. A lista de empresas contempladas com o Pró-Ética, em sua maioria, era composta de empresas de grande porte, geralmente com setores de compliance bem estruturados e dedicados a isso. Sabendo que essa amostra não reflete necessariamente a realidade da maioria das empresas brasileiras, o órgão entendeu que, para promover mudanças significativas no ambiente de negócios do país, seria necessário engajar uma gama maior de entidades privadas, como pequenas e médias empresas, associações, Organizações da Sociedade Civil (OSCs) ou até mesmo grandes corporações que, até o momento, ainda não haviam pautado a temática internamente.

Complementando esse ecossistema, no ano de 2024, a CGU disponibilizou à sociedade o Pacto Brasil pela Integridade Empresarial, que consiste num grande movimento coletivo que convida empresas e entidades privadas que atuam no país a assumirem, voluntariamente, um compromisso público com a ética e com um ambiente de negócios mais íntegro e sustentável. O principal benefício do programa é que ele disponibiliza às empresas e entidades aderentes uma ferramenta gratuita de autoavaliação, que indica se aquela instituição dispõe das medidas mínimas de um Programa de Integridade. Essa ferramenta é dividida em dez áreas e permite que a aderente veja quais áreas ela já apresenta maior maturidade em integridade e quais ainda precisa fortalecer e, mais importante, a aderente passa a conhecer as medidas que poderia implementar para aprimorar seu Programa de Integridade. Esse diagnóstico é fundamental para o planejamento das próximas ações a serem desempenhadas pela empresa.

Entre as demais vantagens trazidas pelo Pacto Brasil, ressalta-se a visibilidade institucional, já que, ao aderir ao programa, a empresa passa a ser incluída na lista de aderentes constante no painel público do Pacto Brasil, e a instituição ganha o direito de utilizar a marca de empresa ou entidade participante do programa, publicizando a seus clientes, funcionários e parceiros de negócio que está de fato comprometida com a temática da integridade empresarial.

Além disso, o Pacto Brasil conta com um site próprio e painel BI, nos quais é dada transparência ativa a todas as entidades privadas aderentes, bem como aos apoiadores institucionais da iniciativa, que operam como verdadeiros "embaixadores" da estratégia de promoção da integridade, levando ao seu público de relações a mensagem sobre a importância da adoção de mecanismos mínimos de integridade corporativa. Aqui, como exemplo, inúmeras entidades do Sistema S, diga-se, que dentre elas, a Federação de Indústrias do Estado do Rio de Janeiro (Firjan), estão atuando como apoiadoras institucionais do Pacto Brasil, disseminando o programa em parceria com a CGU, de modo que consolidem uma ação coletiva em prol da integridade nas empresas e da melhoria nas relações entre a esfera pública e o setor privado.

Adicionalmente, a Portaria Normativa CGU nº 226/2025 estabeleceu que a autoavaliação do Pacto Brasil realizada pelas empresas – desde que demonstrada a implementação de determinadas medidas mínimas – será uma das formas que as empresas terão de comprovar a implementação de seus programas de integridade para fins de desempate em licitações, conforme previsto no artigo 60 da Lei nº 14.133/2021.

4. Mitigando o risco de fragmentação normativa: a harmonização dos critérios de avaliação de programas de integridade

No contexto das exigências estabelecidas pela Lei nº 14.133/2021 quanto aos programas de integridade, a competência de estados e municípios para regulamentar a norma impõe o desafio de evitar a fragmentação normativa, que poderia gerar um cenário de incerteza, submetendo as empresas a critérios de avaliação heterogêneos e variados em cada ente federativo. Para mitigar esse risco, a CGU desenvolveu uma metodologia de avaliação, criada no âmbito da Rede Nacional de Promoção da Integridade Privada, fórum colaborativo de articulação institucional, composto pela CGU e pelas áreas e unidades competentes para a aplicação da Lei Anticorrupção e da Lei de Licitações nos entes subnacionais. Essa metodologia, portanto, se materializa como o resultado de um esforço coletivo, que incorporou contribuições provenientes dos três níveis da federação, sendo capaz de atender às diferentes realidades regionais.

Embora a adoção dessa metodologia por estados e municípios seja opcional, ela é fortemente recomendada para garantir previsibilidade e segurança jurídica às empresas e evitar que essas precisem se adaptar a uma pluralidade de parâmetros e critérios de avaliação, o que pode acarretar aumento no custo de conformidade. Paralelamente, a medida otimiza o uso dos recursos públicos, uma vez que, se o Programa de Integridade de um licitante já tiver sido avaliado pela União ou por qualquer ente que compartilhe a mesma base metodológica, dispensa-se a necessidade de novas avaliações. Esse modelo busca evitar o retrabalho e instituir um contexto de negócios ágil e previsível em todo o território nacional, trazendo maior segurança jurídica e previsibilidade aos agentes envolvidos.

Conclusão

Ao longo dos últimos anos, verificou-se que a consolidação de uma cultura de integridade no Brasil deixou de ser uma mera exigência burocrática para se posicionar como um pilar indispensável de proteção, sustentabilidade e diferenciação competitiva no mercado. O avanço do arcabouço regulatório nacional, impulsionado pela Lei Anticorrupção e pelas exigências estratégicas da Lei de Licitações e Contratos, estabeleceu um novo patamar de governança corporativa. Esse cenário transformou a conformidade em um ativo gerador de valor, capaz de blindar reputações, mitigar riscos jurídicos e atrair novos investimentos e talentos.

Nesse processo de amadurecimento institucional, a atuação da Controladoria-Geral da União (CGU), com iniciativas de vanguarda, tais como o Empresa Pró-Ética e o Pacto Brasil pela Integridade Empresarial, além da disponibilização de guias e manuais orientativos, tem sido fundamental para estimular a adoção de programas de integridade, reconhecer as empresas que buscam "fazer o certo" e democratizar o acesso a ferramentas de compliance, permitindo que organizações de diferentes portes realizem diagnósticos precisos e assumam compromissos voluntários com a ética empresarial, a transparência e a responsabilidade socioambiental, em prol do fortalecimento da política pública da integridade privada em todo o país.

Em um mercado no qual a reputação pode ser volátil e o escrutínio social é imediato, o setor privado é chamado a deixar a posição de espectador e assumir o protagonismo dessa transformação, de forma conjunta com o Poder Público. Engajar-se ativamente em iniciativas como o Pacto Brasil e o Pró-Ética não significa apenas assinar um termo de compromisso ou cumprir uma lista de tarefas; significa proteger o futuro das operações, atrair os melhores talentos e parceiros comerciais, ampliar a confiança da sociedade, além de fixar a bandeira da sua marca no lado certo da história dos negócios no país.

Por isso, diferentemente de ser apenas um suporte jurídico contra penalidades, um Programa de Integridade robusto e efetivo funciona como um motor estratégico de inovação e de fortalecimento da governança da instituição, que visa consolidar a sustentabilidade das empresas e a cultura organizacional brasileira.

Governança corporativa do amanhã:

integridade, confiança e criação de valor sustentável

A governança só cria valor quando deixa de ser arquitetura institucional e passa a ser disciplina de gestão

Agradecimentos: As autoras registram seu agradecimento aos colegas da Coordenação do Capítulo Rio do IBGC — Leonardo Zylberman, João Laudo de Camargo e Patricia Garcia — e à colega Silvia Maura Rodrigues Pereira, pela leitura crítica das versões preliminares deste artigo e pelas valiosas contribuições oferecidas. Os comentários e sugestões recebidos contribuíram para o amadurecimento das reflexões e para o aprimoramento deste trabalho.

Tiana Marzullo dos Santos

Tiana Marzullo dos Santos é conselheira certificada pelo IBGC e Celint, Membro da Comissão Estratégia e Inovação do IBGC e coordenadora do IBGC RJ. Possui experiência internacional de 34 anos em cargos de alta gestão como Head Global e Regional de business development, soluções, parcerias, consultoria e estratégia em empresas multinacionais de tecnologia como Nokia, Ericsson, Logicalis, Ciena, Nortel EUA, TIM Italia, HK-Real Time China, A.T.Kearney e Accenture, atuando em 26 países na Europa, LATAM, NAM e Asia.
Possui MBA em Gestão de Tecnologia e Gestão Global pela Haas U.C. Berkeley e SDA Bocconi. É engenheira elétrica de Telecom e Produção pela PUC-Rio.
É membro de conselhos com foco em inovação, governança, estratégia, business development, portfolio e parcerias - atualmente, na Hipermation, EcoCreator e Coleta.me; anteriormente, e anteriormente na THS, Zimobi, Briquedo Livre, Rauter e ABMEN.

Vanessa Pina

Vanessa Pina é conselheira certificada pelo IBGC e membro de Conselhos Consultivos. Coordenadora do IBGC Rio e da Comissão Temática de Pessoas do Instituto. Sócia-fundadora da Faros, onde apoia CEOs, conselhos e lideranças a transformar estratégia em capacidade organizacional, conectando cultura, desenho organizacional, liderança e governança. Mais de 30 anos de experiência profissional, com passagem por posições C-Level em organizações nacionais e multinacionais, de capital aberto e fechado, e ampla vivência em empresas familiares. Atuou em empresas como Grupo Globo, SulAmérica, British American Tobacco/Souza Cruz e SC Johnson Professional.
Psicóloga, com pós-graduação em Marketing e MBA em Gestão Empresarial pela Fundação Dom Cabral.

Introdução

A definição oficial de governança corporativa, segundo a 6ª edição do Código das Melhores Práticas do Instituto Brasileiro de Governança Corporativa (IBGC) é:

Governança corporativa é um sistema formado por princípios, regras, estruturas e processos pelo qual as organizações são dirigidas e monitoradas, com vistas à geração de valor sustentável para a organização, para seus sócios e para a sociedade em geral. Esse sistema baliza a atuação dos agentes de governança e demais indivíduos de uma organização na busca pelo equilíbrio entre os interesses de todas as partes, contribuindo positivamente para a sociedade e para o meio ambiente (IBGC, 2023).

Essa definição desloca a governança de uma visão meramente formal para uma compreensão sistêmica. Ela reúne princípios, regras, estruturas e processos, mas também explicita que sua finalidade é gerar valor sustentável para a organização, seus sócios e a sociedade. Ao enfatizar o equilíbrio entre interesses, a atuação ética e responsável e a tomada de decisão orientada para o longo prazo, o Código do IBGC reforça que governança não se limita à conformidade: ela se concretiza na forma como as organizações decidem, priorizam, prestam contas e respondem aos impactos que produzem sobre suas partes interessadas.

A governança corporativa vem passando por uma transformação relevante nos últimos anos. Se, durante muito tempo, seu amadurecimento esteve associado principalmente à criação de estruturas formais de supervisão, controle e prestação de contas, o contexto atual amplia significativamente as expectativas sobre seu papel dentro das organizações.

Conselhos de administração, conselho fiscal, auditorias, comitês, políticas corporativas, controles internos e mecanismos de compliance continuam fundamentais. Entretanto, o ambiente empresarial contemporâneo tornou mais evidente uma limitação importante dessa lógica: estruturas formais, isoladamente, não garantem a qualidade das decisões organizacionais.

Em situações concretas, organizações podem apresentar elevado grau de formalização institucional e, ainda assim, conviver com crises reputacionais, incentivos desalinhados, baixa capacidade de antecipação de riscos, conflitos de interesse, fragilidade cultural e destruição de valor no longo prazo.

Esse movimento altera a própria compreensão sobre governança corporativa. A governança do amanhã tende a ser menos associada à simples existência de estruturas institucionais e mais relacionada à cultura e à capacidade efetiva de produzir decisões íntegras, transparentes e sustentáveis em ambientes marcados por pressão, ambiguidade, transformação tecnológica e crescente escrutínio social.

Em outras palavras, governança passa a atuar como disciplina de gestão: um sistema integrado de princípios, regras, estruturas e processos capaz de orientar decisões, sustentar direcionamento estratégico e fortalecer disciplina administrativa.

Essa disciplina influencia a forma como riscos são arbitrados, incentivos são desenhados, conflitos são tratados, prioridades são definidas e consequências são aplicadas quando os princípios organizacionais são colocados à prova.

A agenda dos conselhos de administração e da alta liderança, portanto, amplia seu foco estratégico. Já não basta supervisionar controles ou acompanhar indicadores financeiros. Cresce a expectativa de que a governança seja capaz de integrar estratégia, riscos, cultura organizacional, sustentabilidade, transformação digital, gestão de pessoas, inovação e legitimidade institucional em uma lógica coerente de tomada de decisão.

Nesse contexto, três dimensões ajudam a organizar a discussão sobre a governança corporativa do amanhã, em linha com a 6ª edição do Código das Melhores Práticas do IBGC. A integridade deve ser compreendida não apenas como aderência normativa ou existência de programas de compliance, mas como coerência entre discurso institucional, incentivos, cultura organizacional e prática decisória. A confiança, por sua vez, não deve ser tratada como ativo reputacional abstrato, mas como consequência de práticas verificáveis relacionadas à transparência, qualidade da informação, *accountability*, governança de dados e maturidade de resposta institucional. Por fim, a criação de valor sustentável não se reduz a uma narrativa genérica associada ao ESG; ela se expressa

na capacidade de sustentar competitividade, resiliência e legitimidade ao longo do tempo, equilibrando retorno econômico-financeiro, responsabilidade social, adaptação estratégica e gestão de riscos.

Ao mesmo tempo, novas agendas ampliam a complexidade da atuação dos conselhos e da liderança executiva. A rápida disseminação da inteligência artificial, por exemplo, introduz desafios relacionados à governança de dados, vieses algorítmicos, privacidade, segurança da informação, *accountability* e supervisão humana sobre decisões automatizadas.

Nesse cenário, a governança corporativa do amanhã exige mais do que estruturas formais bem desenhadas. Exige capacidade institucional de transformar princípios em decisões, estratégia em execução e discurso em coerência organizacional.

A partir dessa perspectiva, este texto está estruturado em seis partes:

- Quando a governança amadurece e atua como capacidade de decisão
- Integridade: o que sustenta a governança quando a regra não alcança
- Confiança: o ativo invisível da governança
- Criação de valor sustentável: governança como disciplina de perenidade
- Inteligência artificial e o novo teste da maturidade da governança
- Da arquitetura à prática: governança como capacidade organizacional

1. Desenvolvimento

1.1 Quando governança amadurece e atua como capacidade de decisão

Um dos principais desafios da governança corporativa contemporânea é superar a tendência de tratá-la apenas como estrutura formal.

Durante décadas, o avanço da governança esteve associado principalmente à consolidação de mecanismos institucionais voltados à supervisão, mitigação de conflitos de interesse, transparência e prestação de contas. Conselhos de administração, conselho fiscal, auditorias, controles internos, comitês e políticas corporativas passaram a compor a infraestrutura básica das organizações modernas.

Esses elementos continuam indispensáveis.

No entanto, a experiência prática demonstra que apenas a existência formal dessas estruturas não assegura qualidade das decisões, coerência organizacional ou sustentabilidade no longo prazo.

É justamente nesse ponto que a governança corporativa do amanhã demonstra sua evolução: ao amadurecer para exercer, de fato, seu papel mais amplo na produção de decisões íntegras, transparentes e sustentáveis, no direcionamento estratégico e na disciplina administrativa.

Mais do que ampliar controles, cresce a necessidade de fortalecer a capacidade institucional de tomada de decisão em ambientes marcados por ambiguidade, inovação acelerada, riscos interdependentes, transformação tecnológica e pressão simultânea por crescimento, eficiência, reputação e sustentabilidade organizacional.

À luz da 6ª edição do Código das Melhores Práticas de Governança Corporativa do IBGC, os princípios de integridade, transparência, equidade, responsabilização e sustentabilidade devem permanecer no centro da governança corporativa, não apenas como diretrizes normativas, mas como critérios efetivos de orientação da estratégia, da supervisão e da tomada de decisão.

A atualização dos G20/OECD Principles of Corporate Governance (2023), por exemplo, reforça o papel da governança não apenas como mecanismo de proteção e conformidade, mas também como elemento associado à sustentabilidade, resiliência e supervisão estratégica de riscos emergentes.

No contexto da gestão de riscos, o modelo das três linhas de defesa ajuda a distribuir responsabilidades, reforçar controles e dar clareza às funções de supervisão dentro da organização:

- 1ª linha de defesa — a gestão: responsável por executar processos, gerir riscos no dia a dia e entregar resultados.

- 2ª linha de defesa — riscos, compliance, controles internos, segurança da informação e privacidade: responsável por estabelecer diretrizes, apoiar, monitorar aderência e supervisionar a gestão dos riscos.
- 3ª linha de defesa — auditoria interna: responsável por avaliar, de forma independente, se o desenho e a execução dos controles e mecanismos de gestão de riscos são adequados e efetivos (IIA, 2020).

O conselho de administração, com apoio de seus comitês, supervisiona o sistema, garantindo foco nos riscos materiais, independência, recursos e qualidade das informações. O conselho fiscal, quando instalado, exerce papel próprio de fiscalização, nos termos da legislação e das melhores práticas aplicáveis.

Para que esse arranjo funcione, é crucial que cada linha saiba com precisão o que decide, o que aprova e o que apenas recomenda, evitando tanto a captura do sistema pela gestão quanto a burocratização excessiva. Elementos relevantes são:

- Políticas críticas: aprovadas pelo conselho e revisadas periodicamente.
- Riscos materiais e apetite a risco: definidos ou validados pelo conselho, com KRIs e limites operacionais.
- Grandes investimentos e aquisições: sustentados por *business case*, cenários, análise de sensibilidade e plano de integração.
- Controles e garantias: acompanhados por relatórios de auditoria, testes de controles, apurações de denúncias e planos de ação com prazos.

A arquitetura acima continua válida e ainda mais indispensável como sustentação de uma governança que enfrenta desafios crescentes. Além das responsabilidades fiduciárias tradicionais, a demanda atual requer que o conselho seja capaz de:

- interagir de forma eficaz com a liderança;
- questionar pressupostos estratégicos;
- testar a coerência entre incentivos e comportamento organizacional;
- ampliar a qualidade do contraditório;
- supervisionar riscos emergentes;
- assegurar alinhamento entre discurso institucional, cultura e prática decisória.

Governança do amanhã, portanto, não significa apenas mais controle. Significa maior capacidade institucional de decidir bem, especialmente quando as escolhas se tornam mais difíceis, ambíguas e pressionadas, inclusive em momentos de crise.

1.2 Integridade: o que sustenta a governança quando a regra não alcança

Integridade organizacional costuma ser tratada de forma predominantemente normativa.

Códigos de conduta, treinamentos, canais de denúncia e políticas corporativas são fundamentais. Mas tornam-se insuficientes quando desconectados das decisões reais que moldam o comportamento organizacional.

Na prática, a integridade é testada menos nos discursos institucionais e mais nos momentos de tensão — pressão comercial; crescimento acelerado; conflitos de interesse; crises reputacionais; disputas de poder.

Nessas situações, a governança revela sua efetividade.

A governança do amanhã exige uma compreensão de integridade não apenas como aderência normativa, mas como coerência entre discurso institucional, critérios de decisão, incentivos organizacionais, conduta da gestão e consequências aplicadas.

Referências nacionais e internacionais reforçam esse movimento. O Código das Melhores Práticas de Governança Corporativa do IBGC (6ª edição) destaca que controles e mecanismos formais tendem a perder efetividade quando não existe alinhamento entre cultura, liderança e incentivos organizacionais.

Embora as normas sejam insuficientes, a integridade precisa ser traduzida em um programa com responsabilidades, rotinas, registros e mecanismos de aprendizado. Na prática, agentes externos — auditoria, reguladores, investidores e parceiros — buscam evidências de que a empresa não apenas "tem um código", mas previne, detecta e responde aos riscos. Isso exige mensagens consistentes da liderança, avaliação periódica dos riscos de integridade, controles proporcionais sobre terceiros, canais de denúncia confiáveis, procedimentos documentados de investigação e remediação, além de treinamentos adaptados aos diferentes públicos. Em nossa experiência, é justamente nessa passagem dos documentos para as rotinas que muitas organizações brasileiras encon-

tram maior dificuldade: há políticas bem redigidas, mas nem sempre há cadência, evidência e consequência suficientes para que elas orientem comportamentos quando a pressão por resultado aumenta.

Um exemplo recorrente ocorre em áreas comerciais submetidas a metas agressivas de crescimento. Quando bônus, promoções e reconhecimento estão vinculados apenas ao volume de vendas, sem indicadores de qualidade, conduta e satisfação do cliente, a organização pode estimular práticas incompatíveis com seus próprios valores. A governança se materializa, nesse caso, ao exigir que os incentivos sejam redesenhados, que exceções sejam monitoradas e que a liderança comunique, por decisões concretas, que resultado sem integridade não é resultado aceitável.

Nesse cenário, a cultura organizacional deixa de ocupar posição periférica e passa a representar mecanismo central de governança.

A cultura influencia comportamentos ao definir aquilo que a organização efetivamente recompensa, tolera, ignora ou corrige.

Em outras palavras, cultura funciona como mecanismo de controle e governança. Quando desalinhada, pode neutralizar controles formais, estimular atalhos e gerar impactos adversos sobre pessoas — como assédio, discriminação, jornadas inseguras, metas inexequíveis, práticas comerciais abusivas, violações de privacidade ou decisões automatizadas injustas.

Para a governança do amanhã, tratar pessoas apenas como "público afetado" é insuficiente: colaboradores e demais partes interessadas são também vetores de viabilidade do negócio. Clima organizacional, segurança psicológica, ética, engajamento e legitimidade social impactam diretamente qualidade de execução, continuidade operacional, inovação e resiliência.

Os impactos nas pessoas devem ser integrados a decisões de estratégia, riscos e alocação de capital, com critérios claros de priorização, mitigação e remediação. Isso significa levar ao conselho temas como cultura, sucessão, saúde e segurança, diversidade, relações trabalhistas, impactos em clientes e comunidades, mecanismos de escuta, diligência devida em direitos humanos, capacitação para novas tecnologias e métricas conectadas a incentivos. Também exige atenção às transações com partes relacionadas, que devem observar critérios de mercado, aprovação adequada e transparência. Quando esses temas permanecem dispersos em áreas funcionais, perdem força estratégica; quando são tratados como parte da governança, passam a orientar escolhas sobre crescimento, reputação, produtividade e continuidade do negócio.

1.3 Confiança: o ativo invisível da governança

Confiança frequentemente surge como conceito abstrato nas discussões sobre governança corporativa. Na prática, porém, seus efeitos são profundamente concretos.

A confiança influencia acesso a capital, qualidade das relações institucionais, velocidade decisória, retenção de talentos, capacidade de atravessar crises e legitimidade social.

Empresas percebidas como confiáveis tendem a operar com menor fricção institucional e maior capacidade de sustentar relações de longo prazo com investidores, colaboradores, clientes, parceiros e sociedade.

Esse ativo, contudo, não nasce apenas de narrativa reputacional. É construído — e permanentemente testado — por meio de práticas de:

- transparência;
- equidade;
- prestação de contas;
- responsabilidade corporativa.

O Código do IBGC e os Princípios do G20/OCDE destacam que informação de qualidade e freios e contrapesos reduzem assimetrias e riscos de agência (IBGC, 2023; OECD, 2023).

No Brasil, a Resolução CVM nº 59/2021 fortaleceu o regime informacional ao atualizar regras de divulgação e incorporar, em formato "pratique-ou-explique", o reporte de informações e indicadores ESG em relatório anual ou documento específico, incluindo metodologia, padrão seguido e eventual asseguração por terceiro independente (CVM, 2021).

Embora o alcance obrigatório dependa do tipo de emissor e de seu enquadramento regulatório, a direção é clara: ampliar transparência para permitir decisões mais informadas por investidores e credores. Em um ambiente de transformação digital acelerada, baixa qualidade informacional pode destruir confiança em questão de horas.

Nesse sentido, confiança deixa de ser apenas consequência reputacional da governança e passa a funcionar como um de seus ativos mais estratégicos.

Contudo, transparência não significa "divulgar tudo", mas divulgar tempestivamente o que é relevante, com qualidade e comparabilidade: temas capazes de afetar desempenho, risco, custo de capital e reputação (IFRS Foundation, 2017). Na prática, a falta de materialidade produz dois extremos igualmente problemáticos: relatórios extensos e pouco úteis ou comunicação seletiva, com assimetria informacional e risco de *greenwashing*.

Algumas práticas tornam essa confiança mais verificável. Indicadores financeiros e não financeiros precisam ter responsáveis definidos, controles de origem, metodologia de cálculo e trilha de evidências que permitam reprocessar números e justificar premissas. Metas devem ter linha de base, consistência metodológica e conexão com riscos, *trade-offs* e limitações. Do mesmo modo, a agenda anual do conselho deve reservar tempo adequado para temas como integridade, sustentabilidade, inovação, segurança da informação e qualidade do reporte. Regras de confidencialidade e divulgação, avaliações formais do conselho e da diretoria, relatórios integrados e, quando aplicável, asseguração independente completam esse conjunto de práticas que transformam confiança em algo observável, e não apenas declarado.

Um exemplo simples ilustra esse ponto: uma companhia que anuncia metas climáticas ambiciosas, mas não consegue demonstrar inventário de emissões, metodologia, responsáveis internos e plano de investimento, fragiliza sua credibilidade. Já uma organização que explicita premissas, reconhece limitações, informa avanços e revisa metas com transparência tende a fortalecer a confiança mesmo quando ainda não alcançou todos os resultados pretendidos.

1.4 Criação de valor sustentável: governança como disciplina de perenidade

A criação de valor sustentável talvez seja uma das agendas mais mal compreendidas da governança contemporânea. Na prática, significa a capacidade de manter competitividade, resiliência e legitimidade ao longo do tempo. Pressupõe reconhecer que riscos e oportunidades socioambientais afetam fluxos de caixa, acesso a financiamento e custo de capital. A sustentabilidade, então, migra de "agenda paralela" para o centro da estratégia. O próprio G20/OCDE incorporou, em 2023, um capítulo específico de sustentabilidade e resiliência, reforçando a supervisão do conselho sobre temas materiais que impactam a perenidade.

Um marco recente é a emissão, pelo International Sustainability Standards Board (ISSB), das normas IFRS S1 e IFRS S2 (2023), que estabelecem uma linha de base global para divulgações de sustentabilidade e clima voltadas ao mercado de capitais (IFRS Foundation/ISSB, 2023). As normas organizam as divulgações em quatro pilares — governança, estratégia, gestão de riscos e métricas e metas — e incorporam recomendações do TCFD (IFRS Foundation, [202-]). O movimento leva o tema para a agenda do conselho: quem supervisiona, como decide, como integra riscos climáticos ao ERM e como acompanha metas e desempenho.

Além do reporte, cresce a expectativa por diligência devida em cadeias de valor. A União Europeia, por exemplo, colocou em vigor em 2024 a Corporate Sustainability Due Diligence Directive, estabelecendo deveres para identificar e endereçar impactos adversos em direitos humanos e meio ambiente nas operações próprias, subsidiárias e parceiros da cadeia, além de exigir plano de transição climática (European Commission, 2024). Mesmo para empresas fora do bloco, o efeito tende a ser extraterritorial por meio de requisitos de clientes, financiadores e investidores globais.

Para que ESG não se torne apenas narrativa, o conselho de administração precisa arbitrar *trade-offs* reais: investimentos, prazos, retorno esperado, riscos residuais e impactos para diferentes públicos. Isso demanda materialidade e governança de execução: donos de processos, recursos, metas e monitoramento. Sem esse encadeamento, aumenta o risco de *greenwashing*, com declarações genéricas não sustentadas por evidências, métricas e controles (OECD, 2026).

Nessa arbitragem, é fundamental tornar explícito quem é impactado e como. Efeitos sobre condições de trabalho, saúde e segurança, privacidade, qualidade do produto ou serviço e impactos em comunidades precisam ser

avaliados, mitigados e, quando necessário, remediados como parte da estratégia e da gestão de riscos.

Nesse sentido, sustentabilidade precisa ser tratada como disciplina de execução e alocação de capital. O guia "Boas práticas para uma agenda ESG nas organizações" (IBGC, 2022) enfatiza que a alta gestão deve direcionar recursos financeiros e não financeiros para a agenda, integrando temas materiais à estratégia, à gestão de riscos e ao ciclo de definição de objetivos, metas e indicadores.

Na prática, isso significa avaliar e governar um portfólio de iniciativas — descarbonização, eficiência, rastreabilidade, cadeia de fornecedores, tecnologia, dados, inteligência artificial e conformidade — equilibrando três perspectivas:

- Retorno econômico-financeiro.
- Posicionamento futuro.
- Responsabilidade social.

1.5 Inteligência artificial e o novo teste da maturidade da governança

Poucos temas revelam tão claramente os desafios da governança contemporânea quanto a Inteligência Artificial (IA).

A rápida disseminação da IA — especialmente IA generativa — vem ampliando ganhos de eficiência, automação e capacidade analítica. Ao mesmo tempo, introduz novas camadas de risco relacionadas à privacidade, segurança da informação, vieses algorítmicos, explicabilidade, *accountability* e confiabilidade da informação. A governança da inteligência artificial tornou-se, assim, um teste concreto da capacidade das organizações de equilibrar inovação, velocidade, responsabilidade e supervisão.

O desafio central não é apenas tecnológico. É institucional.

O fenômeno do *shadow AI* — utilização descentralizada de ferramentas de IA sem supervisão adequada — reforça essa complexidade. Muitas organizações já convivem com uso disseminado de inteligência artificial fora dos mecanismos tradicionais de controle, elevando riscos relacionados a vazamento de dados, decisões não rastreáveis e inconsistência regulatória.

Nesse cenário, referências como *o* NIST AI Risk Management Framework (AI RMF 1.0) ajudam a criar uma linguagem comum entre áreas técnicas, risco, compliance e liderança (NIST, 2023). O framework organiza a gestão do risco em quatro macrofunções — *Govern, Map, Measure e Manage* — e consolida atributos associados à IA confiável, como segurança, resiliência, privacidade, transparência, explicabilidade e mitigação de vieses.

Algumas perguntas tornam essa governança mais concreta. Antes de escalar soluções de IA, a organização precisa definir em quais processos a tecnologia é requisito competitivo, quais decisões críticas serão apoiadas por modelos, quais dados serão utilizados e sob quais bases legais, como vieses, robustez e degradação de desempenho serão testados, quais responsabilidades cabem a fornecedores e quais usos exigem supervisão humana. A pergunta central, portanto, não é apenas se a empresa deve usar IA, mas se possui maturidade para governar seus usos, limites, evidências e consequências.

No cotidiano, esse desafio aparece quando uma área passa a utilizar ferramentas de IA generativa para resumir contratos, analisar currículos ou responder clientes sem política clara de uso, validação humana ou proteção de dados. O ganho de produtividade pode ser real, mas a ausência de governança expõe a organização a vazamentos, discriminação involuntária, decisões pouco rastreáveis e perda de confiança. A maturidade está em permitir inovação com critérios, e não em bloquear a tecnologia ou adotá-la sem supervisão.

No Brasil, o debate regulatório também evolui: o PL 2338/2023 (Brasil, 2023), aprovado pelo Senado e remetido à Câmara, reforça a tendência de abordagens baseadas em risco, com deveres proporcionais ao potencial de dano.

O verdadeiro desafio da governança do amanhã não será apenas adotar IA. Será construir capacidade institucional para decidir onde utilizar; como supervisionar; quais riscos aceitar; quais limites não podem ser ultrapassados.

1.6 Da arquitetura à prática: governança como capacidade organizacional

A governança corporativa do amanhã exige traduzir estratégia em execução, riscos em critérios de decisão, indicadores em mecanismos de aprendizado e *accountability* em consequência efetiva. Pela velocidade das mudanças, amplia-se também o papel dos conselhos de administração e das lideranças.

É cada vez maior a expectativa de que o conselho contribua para elevar a qualidade das decisões organizacionais, ampliar a capacidade de antecipação de riscos e fortalecer a coerência institucional.

Temas relacionados a tecnologia, inteligência artificial, riscos cibernéticos e governança de dados ampliam significativamente a complexidade das decisões estratégicas.

Na prática, organizações mais maduras tendem a fortalecer clareza de papéis e alçadas, qualidade dos fóruns decisórios, governança de dados, mecanismos de supervisão, processos de avaliação e capacidade de integração entre estratégia, riscos, cultura e execução. Essa maturidade raramente surge de uma única iniciativa. Ela é construída por repetição, aprendizado e coerência: reuniões com informações melhores, decisões com critérios mais explícitos, riscos discutidos antes de se materializarem e consequências aplicadas de forma consistente.

A resiliência organizacional depende da capacidade de elaborar, manter e rever planos de continuidade de negócios e planos de contingência e recuperação coerentes com o apetite a risco e testados por exercícios.

Essa integração permite que incidentes cibernéticos, falhas de fornecedores, indisponibilidade de sistemas ou crises operacionais sejam tratados com prioridades, tempos de recuperação, responsabilidades e comunicação definidos. Frameworks e normas como ISO 22301, NIST Cybersecurity Framework 2.0 e NIST SP 800-34 oferecem referências consolidadas para estruturar governança, papéis, preparação, resposta e recuperação (ISO, 2019; NIST, 2024; NIST, 2010).

Do ponto de vista de controles, importante enfatizar que a lógica das três linhas de defesa continua relevante, como descrito no item 2.1.

Com relação à disciplina de execução, a estratégia só se torna perene quando é traduzida em objetivos claros, metas e KPIs/KRIs mensuráveis — com linha de base, metodologia, responsáveis, cadência de revisão e consequências. Sem esse encadeamento, a organização perde capacidade de priorizar, monitorar riscos materiais e aprender. Com ele, o conselho melhora a qualidade do acompanhamento e a empresa sustenta desempenho no longo prazo.

Abordagens como o COBIT 2019 reforçam a importância de conectar necessidades das partes interessadas a objetivos corporativos e, a partir daí, a objetivos de alinhamento e métricas operacionais (ISACA, 2019).

Nesse contexto, exemplos de métricas e sinais que podem compor um painel do conselho incluem:

- Integridade: incidentes, tempo de apuração, qualidade de denúncias, due diligence de terceiros, treinamento e aderência a políticas críticas.
- Confiança e transparência: tempestividade de divulgações, qualidade de controles sobre informações, asseguração, incidentes de segurança da informação e conformidade com políticas de divulgação.
- Valor sustentável: indicadores climáticos e sociais materiais, exposição a riscos físicos e de transição, progresso de planos de transição, cadeia de valor e eficiência obtida com automação ou IA.
- Governança de IA: inventário de modelos, incidência de *shadow AI*, taxas de erro ou alucinação, indicadores de viés, monitoramento de *drift*, incidentes de privacidade e supervisão humana.
- Governança do conselho: presença, preparação, avaliação anual, educação continuada, composição, diversidade de competências e acompanhamento de deliberações.
- Sustentabilidade econômico-financeira: retorno sobre capital, geração de caixa, liquidez, produtividade, exposição a concentrações e performance do portfólio de projetos, incluindo CAPEX aprovado versus executado, realização de benefícios, *payback*, NPV e IRR quando aplicáveis.

Ou seja, não há governança do amanhã sem acompanhamento da evolução do mercado, que se traduz em evolução de competências. O IBGC recomenda educação continuada e avaliação do conselho e dos conselheiros, além de planejamento sucessório.

Conclusão

A governança corporativa do amanhã tende a ser julgada menos pela existência de estruturas formais e mais pela efetiva capacidade de produzir decisões íntegras, transparentes e sustentáveis em ambientes de crescente complexidade.

Integridade, confiança e criação de valor sustentável deixam de ocupar agendas paralelas para formar um mesmo sistema de gestão. Da interação entre essas três dimensões emerge uma governança capaz de reduzir desvios, fortalecer a legitimidade institucional e sustentar a competitividade no longo prazo.

Nenhum desses elementos, porém, se sustenta apenas por arquitetura institucional.

Eles dependem da capacidade de transformar princípios de governança em prática cotidiana de gestão:

- Como decisões são tomadas;
- Como incentivos são desenhados;
- Como riscos são arbitrados;
- Como conflitos são tratados;
- Como responsabilidades são exercidas.

Essa passagem da arquitetura à prática exige escolhas concretas. Como recomendações finais, destacam-se:

(i) Fortalecer a cultura e os incentivos alinhados à ética e ao desempenho, com programas de integridade efetivos e mensuráveis;

(ii) Incorporar, na agenda do conselho, a visão sobre pessoas — cultura, clima, saúde e segurança, capacitação, diversidade e impactos nas partes interessadas — com mecanismos de escuta, diligência devida e métricas que orientem decisões e remediações;

(iii) Elevar a qualidade da informação e do reporte, incluindo aspectos ESG materiais, com governança de dados e, quando aplicável, asseguração independente;

(iv) Integrar sustentabilidade, resiliência e sustentabilidade econômico-financeira ao planejamento estratégico, à alocação de capital e ao gerenciamento de riscos;

(v) Endereçar governança de IA com políticas, controles, supervisão humana e métricas;

(vi) Investir na capacidade do conselho — composição, educação continuada, avaliação e sucessão — para acompanhar riscos emergentes e orientar a transformação.

A governança corporativa do amanhã exige menos preocupação em parecer bem governada e mais capacidade de efetivamente governar.

Referências

INSTITUTE OF INTERNAL AUDITORS (IIA). *The IIA's Three Lines Model*: an update of the Three Lines of Defense. Lake Mary, FL: IIA, 2020. Disponível em: https://www.theiia.org/en/content/guidance/position-papers/three-lines-model/. Acesso em: 18 out. 2026.

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA (IBGC). *Boas práticas para uma agenda ESG nas organizações*. São Paulo: IBGC, 2022. Disponível em: https://www.ibgc.org.br/. Acesso em: 18 out. 2026.

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA (IBGC). *Caderno 9*: boas práticas para reuniões do conselho de administração. São Paulo: IBGC, 2010. Disponível em: https://www.ibgc.org.br/. Acesso em: 18 out. 2026.

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA (IBGC). *Código das melhores práticas de governança corporativa*. 6. ed. São Paulo: IBGC, 2023. Disponível em: https://www.ibgc.org.br/. Acesso em: 18 out. 2026.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). *ISO 22301:2019*: security and resilience — business continuity management systems — requirements. Geneva: ISO, 2019. Disponível em: https://www.iso.org/standard/75106.html. Acesso em: 18 out. 2026.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). *ISO 26000:2010*: guidance on social responsibility. Geneva: ISO, 2010. Disponível em: https://www.iso.org/iso-26000-social-responsibility.html. Acesso em: 18 out. 2026.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). *ISO 30414:2018*: human resource management — guidelines for internal and external human capital reporting. Geneva: ISO, 2018. Disponível em: https://www.iso.org/standard/69338.html. Acesso em: 18 out. 2026

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). *ISO/IEC 42001:2023*: information technology — artificial intelligence — management system. Geneva: ISO, 2023. Disponível em: https://www.iso.org/standard/42001.html. Acesso em: 18 out. 2026.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO); INTERNATIONAL ELECTROTECHNICAL COMMISSION (IEC). *ISO/IEC 27001:2022*: information security management systems — requirements. Geneva: ISO, 2022. Disponível em: https://www.iso.org/standard/27001.html. Acesso em: 18 out. 2026.

INTERNATIONAL FINANCIAL REPORTING STANDARDS FOUNDATION (IFRS Foundation). *IFRS Practice Statement 2*: making materiality judgements. Londres: IFRS Foundation, 2017. Disponível em: https://www.ifrs.org/content/dam/ifrs/publications/html-standards/english/2025/issued/ps2.html. Acesso em: 18 out. 2026.

INTERNATIONAL FINANCIAL REPORTING STANDARDS FOUNDATION (IFRS Foundation). Making the transition from TCFD to ISSB. *IFRS Foundation*, Londres, [2024?]. Disponível em: https://www.ifrs.org/sustainability/knowledge-hub/making-the-transition-from-tcfd-to-issb/. Acesso em: 18 out. 2026.

INTERNATIONAL FINANCIAL REPORTING STANDARDS FOUNDATION (IFRS Foundation). International Sustainability Standards Board (ISSB). *ISSB issues inaugural global sustainability disclosure standards* (IFRS S1 e IFRS S2). *IFRS Foundation*, Londres, 26 jun. 2023. 26 jun. 2023. Disponível em: https://www.ifrs.org/news-and-events/news/2023/06/issb-issues-ifrs-s1-ifrs-s2/. Acesso em: 18 out. 2026.

INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION (ISACA). *COBIT 2019 framework*: governance and management objectives. Schaumburg, IL: ISACA, 2018. Disponível em: https://www.isaca.org/resources/cobit. Acesso em: 18 out. 2026.

LENCIONI, João. *Inteligência artificial nos conselhos*: o próximo passo da governança corporativa? IBCG, São Paulo, 15 set. 2020. Disponível em: https://www.ibgc.org.br/blog/inteligencia-artificial-nos-conselhos. Acesso em: 18 out. 2026.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). *Artificial intelligence risk management framework* (AI RMF 1.0). Gaithersburg, MD: NIST, jan. 2023. DOI: https://doi.org/10.6028/NIST.AI.100-1.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). *Contingency planning guide for federal information systems*. Gaithersburg, MD: NIST, 2010. (NIST Special Publication 800-34). DOI: https://doi.org/10.6028/NIST.SP.800-34r1.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). *The NIST cybersecurity framework (CSF) 2.0*. Gaithersburg, MD: NIST, 26 fev. 2024. DOI: https://doi.org/10.6028/NIST.CSWP.29.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD). *G20/OECD principles of corporate governance 2023*. Paris: OECD Publishing, 2023. DOI: https://doi.org/10.1787/ed750b30-en.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD). *OECD due diligence guidance for responsible business conduct*. Paris: OECD Publishing, 2018. Disponível em: https://www.oecd.org/en/publications/oecd-due-diligence-guidance-for-responsible-business-conduct_15f5f4b3-en.html. Acesso em: 18 out. 2026.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD). *Protecting and empowering consumers in the green transition*. Paris: OECD Publishing, 2026. Disponível em: https://www.oecd.org/en/publications/protecting-and-empowering-consumers-in-the-green-transition_12f28e4f-en.html. Acesso em: 18 out. 2026.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD). *Recommendation of the Council on Artificial Intelligence*. Paris: OECD, 2019. OECD/LEGAL/0449. Disponível em: https://legalinstruments.oecd.org/api/print?ids=648&lang=en. Acesso em: 18 out. 2026.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD). *Tax compliance by design*: achieving improved SME tax compliance by adopting a system perspective. Paris: OECD Publishing, 2014. DOI: https://doi.org/10.1787/9789264223219-en.

ORGANIZAÇÃO INTERNACIONAL DO TRABALHO (OIT). *Declaração da OIT relativa aos princípios e direitos fundamentais no trabalho*. Genebra: OIT, 1998. Disponível em: https://www.ilo.org/declaration/lang--pt/index.htm. Acesso em: 18 out. 2026.

SCHWAB, Klaus. Davos manifesto 2020: the universal purpose of a company in the Fourth Industrial Revolution. *World Economic Forum*, Cologny, 2 dez. 2019. Disponível em: https://www.weforum.org/stories/2019/12/davos-manifesto-2020-the-universal-purpose-of-a-company-in-the-fourth-industrial-revolution/. Acesso em: 18 out. 2026.

UNITED NATIONS (UN). *Guiding principles on business and human rights*: implementing the United Nations "Protect, Respect and Remedy" framework. New York; Geneva: United Nations, 2011. Disponível em: https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf. Acesso em: 18 out. 2026.

UNIÃO EUROPEIA. Comissão Europeia (CE). Corporate sustainability due diligence *European Comission*, Bruxelas, 2024. Disponível em: https://commission.europa.eu/topics/business-and-industry/doing-business-eu/sustainability-due-diligence-responsible-business/corporate-sustainability-due-diligence_en. Acesso em: 18 out. 2026.

WORLD ECONOMIC FORUM (WEF). Measuring stakeholder capitalism: towards common metrics and consistent reporting of sustainable value creation. *World Economic Forum,* Cologny, set. 2020. Disponível em: https://www.weforum.org/publications/measuring-stakeholder-capitalism-towards-common-metrics-and-consistent-reporting-of-sustainable-value-creation/. Acesso em: 18 out. 2026.[32] OIT — Organização Internacional do Trabalho. *Declaração da OIT relativa aos Princípios e Direitos Fundamentais no Trabalho* (1998; emenda 2022). Disponível em: https://www.ilo.org/declaration/lang--pt/index.htm

Governança corporativa e integridade:

o papel estratégico da *due diligence* na construção e consolidação da reputação empresarial

Ana Cecília Martyn Milagres

Ana Cecília Martyn Milagres é executiva de GRC, atualmente, responsável pelas áreas de Integridade e Ética e Auditoria Interna da Ocyan. Ministra aulas de *Compliance* e participa, também, do grupo de treinadores da *Alliance For Integrity, sendo* eleita a Treinadora do Ano em 2024. Bacharel em Economia pela UFRJ, com mestrado em Administração pela PUC-RJ. Tem três livros publicados em coautoria sobre as temáticas de GRC.

Introdução

O presente artigo tem como objetivo demonstrar como o processo de *due diligence,* uma importante ferramenta de um Programa de Compliance efetivo, pode atuar na redução de riscos de exposição perante terceiros, parceiros e fornecedores.

Para comprovar essa hipótese, explico como os Programas de Integridade em conjunto com a ferramenta de *due diligence* auxiliam na escolha de parceiros e fornecedores que tenham os mesmos valores e princípios da empresa, ajudando na construção de um mercado íntegro, em que as empresas devem atuar em prol da ética e da integridade. Não faz sentido dizer que sou ético apenas da porta para dentro e, hoje em dia, não aceitamos mais a desculpa de que uma empresa contratou outra empresa com práticas questionáveis e não sabia o que estava acontecendo. Precisamos ter ao nosso lado empresas que compactuem com nossos valores e atuem de forma ética, assim deixaremos um legado positivo no mercado, e os nossos clientes confiarão na nossa empresa.

Esse ponto está intimamente ligado à governança nas organizações, promovendo a construção de uma cultura ética que não esteja apenas presente no seu site institucional, mas que seja vivenciada no dia a dia da organização e dos seus *stakeholders*.

1. Programas de Integridade

Os programas de integridade são os instrumentos utilizados pelas empresas para a implementação de um compliance efetivo. Eles têm a função de prevenção, detecção e remediação de atos corruptos, desvios éticos e de conduta, fraudes, suborno, violação ou desrespeito a direitos que atinjam de alguma forma a reputação institucional.

Tem-se observado um movimento no mercado, aliado ao advento das questões ESG, de os programas de integridade serem, também, importantes instrumentos de valorização de uma cultura empresarial de integridade, longe de atos corruptos, em que fazer o que é certo deve ser ensinado e seguido, tanto pelos funcionários quanto pelas partes interessadas que fazem parte do universo dos diferentes tipos de empresa.

No arcabouço legal brasileiro, observou-se a publicação do Decreto nº 11.129/2022[1], que revogou o Decreto-lei nº 8.420/2015[2] e trouxe mais dois objetivos para o Programa de Integridade, quais sejam: a prevenção e o fomento e a manutenção de uma cultura de integridade no ambiente organizacional.

Observou-se uma preocupação com a mudança cultural dentro da organização, que vai muito além da simples adoção de medidas anticorrupção. Ela preconiza a construção de valores que devem ser compartilhados por todas as partes interessadas da organização.

O Programa de Integridade apoiará a empresa a exercer os seus deveres legais e evitar a prática de irregularidades, mas também deverá auxiliá-la a buscar um propósito que promova uma cultura de integridade e que lhe permita prosperar financeiramente. Essa empresa deverá buscar parceiros, fornecedores e funcionários que tenham os mesmos valores e princípios e, por isso, deve ter muito cuidado em sua seleção.

As razões para a implementação de um Programa de Integridade são muitas, desde as relacionadas à imagem e à reputação, à motivação dos funcionários em trabalhar em uma empresa na qual a liderança tem como mote a cultura da ética e o respeito aos Direitos Humanos e ao meio ambiente, ao aumento de oportunidades comerciais, à redução de custos e de perdas financeiras associados a fraudes e à corrupção.

No novo guia da Controladoria Geral da União (CGU), lançado em outubro de 2024, a proposta foi a criação de um sistema de integridade, composto por 10 passos essenciais, entre eles: (a) a definição dos padrões de conduta esperados de lideranças, funcionários e empresas com as quais mantém relacionamentos, dando ênfase às questões ASG, especificamente, aos direitos humanos, às condições de trabalho e ao meio ambiente; (b) a realização de diligências apropriadas, baseadas em risco,

[1] BRASIL. Decreto Lei 11.129, de 11 de julho de 2022. Regulamenta a Lei 12.846

[2] BRASIL. Decreto Lei 8.420, de 18 de março de 2015. Regulamenta a Lei 12.846

para contratação e supervisão de terceiros, como, fornecedores, prestadores de serviço, agentes intermediários, despachantes, representantes comerciais, associados e consultores, pessoas politicamente expostas e familiares, funcionários, patrocínios e doações, fusões, aquisições e reestruturações, como forma de mitigação de riscos de corrupção e de assegurar que a empresa se relacione comercialmente com entidades que compartilhem seus valores e comportamentos éticos; (c) a detecção de irregularidades, por meio da disponibilização de canais de denúncia, de fácil acesso para os públicos interno e externo, com garantias aos denunciantes de boa-fé, como não retaliação, sigilo e confidencialidade; e (d) o monitoramento, com a definição de procedimentos de verificação da aplicabilidade do Programa de Integridade.

O Programa de Integridade deverá fomentar a criação de uma cultura de integridade, reduzindo não apenas os riscos de corrupção, mas atuando de forma proativa para a construção de uma empresa que quer deixar um legado positivo e compartilha seus valores de ética, de integridade, de respeito aos direitos humanos e de preservação do meio ambiente com todas as partes interessadas, gerando confiança no mercado, devido à certeza de que a empresa faz o que é certo e preza pela sua reputação.

2. ASG e governança

A agenda ASG (Ambiental, Social e Governança) vem ganhando importância nos dias de hoje. Empresas que se destacam no mercado devem apresentar compromissos nas áreas ambiental, social e de governança.

Instituto Brasileiro de Governança Corporativa (IBGC), a governança corporativa pode ser definida como um:

> sistema formado por princípios, regras, estruturas e processos pelo qual as organizações são dirigidas e monitoradas, com vistas à geração de valor sustentável para a organização, para seus sócios e para a sociedade em geral. Esse sistema baliza a atuação dos agentes de governança e demais indivíduos de uma organização na busca pelo equilíbrio entre os interesses de todas as partes, contribuindo positivamente para a sociedade e para o meio ambiente.[3]

A ideia do conceito de ASG é que as empresas tenham como propósito a geração de valor para a sociedade por meio do desenvolvimento de produtos inovadores e que respeitem o meio ambiente, oportunidades de carreira para os seus públicos de interesse e funcionários, negócios rentáveis para fornecedores e parceiros comerciais de sua cadeia produtiva, receitas para o país e rentabilidade para os investidores.

Para isso é importante que seu processo de tomada de decisão leve em consideração aspectos éticos. A governança corporativa é extremamente importante nesse sentido, pois é por meio dela que as organizações se tornam mais transparentes, responsáveis e sustentáveis.

A orientação para a ética e uma cultura forte são importantes para que as pessoas cumpram as normas internas, as leis, tenham um comportamento ético na tomada de decisões, o que terá como consequência o bem-estar comum das partes interessadas da organização a longo prazo.

Essas práticas devem ser vistas e vivenciadas dentro das organizações e não apenas noticiadas como boas. Para isso, é muito importante a construção de princípios sólidos e relacionamentos de longo prazo com partes interessadas que tenham os mesmos princípios e valores.

Como descreve Alexandre Di Miceli:

> Para avançarmos como sociedade, é imprescindível que nossas empresas sejam lideradas por executivos que reflitam sobre as implicações de suas ações sobre terceiros e que possuam elevada empatia. É a partir dessa reflexão que essas lideranças poderão tomar decisões alicerçadas em sólidos princípios éticos. Promover um comportamento ético no ambiente empresarial – indo além do mero cumprimento de normas – é, a meu ver, o principal desafio global de nossa época. Em caso de sucesso, teremos um mundo muito melhor para todos nós e para nossos descendentes (Di Miceli, 2018, p. 8).

[3] IBGC, disponível em https://www.ibgc.org.br/conhecimento/governanca-corporativa, Acesso em: 18 de fevereiro de 2025

Para que isso ocorra, a empresa deverá ter um ambiente em que o comportamento ético seja estimulado e deverá selecionar partes interessadas com um processo bem estruturado de *due diligence*, que inclua questões de ASG, especificamente, direitos humanos, condições de trabalho e meio ambiente e que estejam de acordo com as normas e regras internas e externas voluntariamente.

3. Compliance e ASG na cadeia de fornecimento

A governança corporativa preza pela transparência e atuação ética e sustentável interna e externamente. A geração de valor influenciada por uma boa reputação não vai acontecer se a organização tiver relacionamentos com outras que estejam desalinhadas com seus valores.

A questão aqui é que essas organizações têm outros administradores, com regras e processos próprios. Mas é importante que se conheça aquelas com que nos relacionamos por meio de processos de diligência (*due diligence*), pois a sua adoção demonstra que a empresa tem um compromisso com a ética, a integridade e a transparência na condução dos seus negócios.

Esses processos de diligência podem ser realizados por meio de pesquisas reputacionais das empresas com quem queremos nos relacionar, questionários a respeito das práticas adotadas pelas empresas, verificação de sanções e processos jurídicos nas áreas de integridade, ASG, direitos humanos, declarações e ciência aos documentos da empresa, tais como o Código de Ética e Conduta, e treinamentos para que as partes interessadas tenham ciência dos valores e princípios praticados. O processo de *due diligence* deve ser monitorado e revisado periodicamente. Esse processo também contribui para a tomada de decisão, pois os gestores avaliarão os riscos e oportunidades associados às principais partes interessadas.

O processo de *due diligence* deverá ser implementado junto às áreas que tratam dos relacionamentos das empresas, portanto, é importante que a área de integridade entenda os mecanismos e as ferramentas das áreas que mantêm relacionamentos externos, tais como suprimentos, comercial, contratação de fornecedores, parcerias e vendas por meio de plataformas *sellers*, e construa um processo em que essa análise esteja inserida e seja revisada periodicamente. Para isso, é importante entender os principais mecanismos desses processos correlatos, tais como prazos, formas de contratação e relacionamento, e elaborar um sistema em que a *due diligence* contribua para a celebração de relacionamentos com partes interessadas que tenham boa conduta e reputação.

Essa prática levará os principais parceiros a adotarem medidas para que estejam de acordo com os valores pactuados e gerará valor positivo tanto para os stakeholders[4] quanto para a sociedade em geral. Tanto consumidores quanto investidores têm exigido cada vez mais transparência das organizações quanto às questões ASG. Temos visto movimentos internacionais para impulsionar esse comportamento. O Parlamento Europeu aprovou uma proposta de lei[5] em que as organizações deverão prevenir e remediar questões envolvendo abusos de direitos humanos nas cadeias de abastecimento globais. O Decreto nº 11.129/21[6] também prevê a realização de *due diligence* para mitigação de casos de corrupção. Portanto, além de ser uma questão de posicionamento e cultura voltados para práticas éticas e sustentáveis, também é uma questão legal. As empresas não podem se eximir da responsabilidade de se relacionar com parceiros que tenham práticas indevidas relacionadas a questões de sustentabilidade, direitos humanos e corrupção. Na lei europeia[7], as vítimas podem procurar a justiça, caso estejam sofrendo qualquer tipo de abuso corporativo.

[4] são todas as partes interessadas que podem afetar ou ser afetadas pelas ações, decisões, operações e resultados de uma empresa ou projeto.

[5] COMISSÃO EUROPÉIA, Diretiva 2024/1760, de 25 de julho de 2024. Dispõe sobre Due Diligence de Sustentabilidade Corporativa

[6] BRASIL. Decreto Lei 11.129/2022, de 11 de julho de 2022, regulamenta a Lei 12.846/2013.

A diretiva da União Europeia está pautada em práticas de direitos humanos, proteção ambiental, mudanças climáticas, entre eles trabalho forçado e trabalho infantil, perda da biodiversidade, poluição. A diretriz é aplicável às empresas que operam no âmbito da União Europeia (UE), com faturamento líquido igual ou superior a 450 milhões de euros.

Mesmo não incidindo sobre as empresas que não apresentam os critérios acima, essa diretriz deverá impulsionar nas demais uma evolução das discussões regulatórias sobre uma conduta empresarial responsável, ganhando tração para além da UE, como parâmetros de devida diligência em sustentabilidade e direitos humanos.

4. Reputação empresarial

A reputação pode ser entendida como uma vantagem competitiva para as corporações, contribuindo de uma forma positiva ou negativa para o seu desempenho. Uma empresa com boa reputação normalmente gera uma maior identidade corporativa, o que impacta positivamente a continuidade da organização. As pessoas buscam trabalhar em empresas que tenham um propósito alinhado às suas expectativas e que tenham uma imagem positiva de mercado, o que está sendo bastante impulsionado pelo movimento ASG.

A reputação de uma organização tem a ver com o seu desempenho ao longo do tempo e com as experiências acumuladas no relacionamento com ela. Quando as partes interessadas associam imagens positivas continuamente, isso é um reflexo de como uma organização está impactando positivamente a sociedade.

Podemos simplificar o conceito de reputação como o conceito de confiança; sem confiança, não teremos um relacionamento possível com nossos clientes, fornecedores, partes interessadas em geral. A confiança gera segurança nos relacionamentos e garante estabilidade nos negócios. A reputação estará ligada à imagem da organização perante os seus públicos a partir de experiências concretas e relações de confiança.

A confiança existe quando temos um comportamento harmonioso com princípios e valores aceitos universalmente. Confiamos em organizações que compactuam com a Declaração Universal dos Direitos Humanos, defendem a sustentabilidade, atuam fazendo o que é certo, ou seja, de forma ética, e são transparentes em suas ações.

A reputação está consolidada na cultura organizacional da empresa, na sua história e no seu propósito. Quando falamos de história, é muito importante que haja transparência quanto aos fatos positivos e negativos. Tentar esconder a parte negativa não vai ajudar, pois é muito fácil, no mundo conectado de hoje, ter acesso a qualquer informação. Portanto, é importante ter uma postura positiva, de compromisso com a solução de problemas perante os fatos negativos. O propósito significa o porquê da existência dessa empresa e quais planos são importantes para a sua continuidade, e a cultura organizacional está relacionada a comportamentos, posicionamento no mercado, clima interno e campanhas de marketing. Uma empresa que tem por princípio e possui exemplos de atuação ética tem maior probabilidade de gerar confiança do que uma empresa que tenha exemplos de atuações antiéticas, tais como não cumprir com o que prometeu, produtos de baixa qualidade, pouco cuidado na seleção de fornecedores, cadeias de fornecimento com trabalho análogo ao escravo, ocultação de fatos negativos do passado, entre outros.

A conduta ética deve estar definida nos seus compromissos e documentos, mas, mais do que isso, deve estar presente em ações de comunicação, treinamentos, não somente como uma regra a ser seguida, mas como uma estratégia para a perenidade da organização, para que ela crie valor a longo prazo. A organização deve ser aquela em que as pessoas confiam e que seja vista como exemplo de boa atuação e conduta perante todas as suas partes interessadas.

[7] COMISSÃO EUROPÉIA, Diretiva 2024/1760, de 25 de julho de 2024. Dispõe sobre Due Diligence de Sustentabilidade Corporativa

Conclusão

O objetivo desse artigo é mostrar que a avaliação prévia dos parceiros, fornecedores e intermediários atua como uma importante ferramenta para identificação de riscos e proteção da imagem e da reputação da empresa. Investidores, parceiros e clientes tendem a valorizar organizações que demonstram ter cuidado nas parcerias, terceirizações e seleção de fornecedores e funcionários.

Para isso, falo sobre os programas de integridade, da importância da adoção de uma cultura ética para a mudança organizacional e da sociedade, da importância da disseminação dessa cultura para a cadeia de fornecimento e de como empresas com boa reputação geram confiança e valor para a sociedade e os acionistas, o principal objetivo da governança corporativa.

As práticas empresariais e as políticas públicas devem ser traçadas com objetivos que respeitem os direitos humanos, juntamente com a promoção da integridade e o respeito ao meio ambiente. Para isso, as empresas devem adotar uma cultura de integridade e ética, com valores, funcionários e liderança engajados e comprometidos em fazer o que é o certo. Ao fazer o que é certo, a confiança será alcançada. Marcas em que as pessoas confiam são marcas que as pessoas consomem, o que gerará valor tanto para a sociedade quanto para a empresa.

A governança pautada na ética, integridade e transparência é fundamental para que possamos atingir esses objetivos e gerar valor para as empresas. Os processos de *due diligence* fortalecem a credibilidade da empresa perante o mercado, pois auxiliam na escolha de parceiros, fornecedores e funcionários que compactuem com esses valores, o que tem como consequência uma geração de valor para toda a cadeia e para a sociedade.

Referências

ALMEIDA, Ana Luisa Castro. Pressupostos teórico-metodológicos para o estudo da identidade e da reputação organizacional. *In*: KUNSCH, Margarida M. Krohling (org.). *Relações públicas: história, teorias e estratégias nas organizações contemporâneas*. São Paulo: Saraiva, 2009. p. 263-289.

ALMEIDA, Ana Luisa Castro. Reputação organizacional: a importância de parâmetros para o seu gerenciamento. *Revista Brasileira de Comunicação Organizacional e de Relações Públicas*, São Paulo, n. 2, p. 116-133, jan./jul. 22005. DOI: https://doi.org/10.11606/issn.2238-2593.organicom.2005.138884.

BALMER, John M. T. Corporate identity: what of it, why the confusion, and what's next? *Corporate Reputation Review*, [*S. l.*], v. 1, n. 1/2, p. 183-188, 1997. DOI: https://doi.org/10.1057/bm.2013.15.

BALMER, John M. T.; GREYSER, Stephen A. *Revealing the corporation*. London: Routledge, 2003.

BARNEY, Jay B. Firm resources and sustained competitive advantage. *Journal of Management*, [*S. l.*], v. 17, n. 1, p. 99-120, 1991. DOI: https://doi.org/10.1177/014920639101700108.

BERENS, Guido; VAN RIEL, Cees B. M. Corporate associations in the academic literature. *Corporate Reputation Review*, v. 7, n. 2, p. 161-176, 2004.

BRASIL. Controladoria-Geral da União. *Programa de integridade: diretrizes para empresas privadas*. v. 2. Brasília, DF: CGU, ago. 2024. Disponível em: https://www.gov.br/cgu/pt-br/assuntos/noticias/2024/10/cgu-publica-novo-guia-de-diretrizes-para-empresas-privadas/GuiaDiretrizes_v14out1.pdf. Acesso em: 9 jul. 2026.

BRASIL. Decreto nº 11.129, de 11 de julho de 2022. Regulamenta a Lei nº 12.846, de 1º de agosto de 2013, que dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira. *Diário Oficial da União*: seção 1, Brasília, DF, 12 jul. 2022.

BRASIL. Lei nº 12.846, de 1º de agosto de 2013. Dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou eestrangeira, e dá outras providências. *Diário Oficial da União*: seção 1, Brasília, DF, 2 ago. 2013.

CIMADON, A. Ética nas organizações e proteção dos direitos humanos e fundamentais. *Espaço Jurídico*, Joaçaba, v. 6, n. 1, p. 33-44, 22005. Disponível em: https://periodicos.unoesc.edu.br/espacojuridico/article/view/8800. Acesso em: 20 out. 2026.

COELHO, Nuno M. M. S.; HERINGER, Helimara Moreira Lamounier. Foreign Corrupt Practices Act: uma breve análise da lei que deu origem ao combate internacional da corrupção. *A&C – Revista Jurídica*, Curitiba, v. 1, n. 46, p. 164-187, 2017. DOI: https://doi.org/10.26668/revistajur.2316-753X.v1i46.2004

COMISSÃO EUROPEIA. Diretiva (UE) 2024/1760 do Parlamento Europeu e do Conselho, de 13 de junho de 2024, relativa ao dever de diligência das empresas em matéria de sustentabilidade e que altera a Diretiva (UE) 2019/1937 e o Regulamento (UE) 2023/2859. *Jornal Oficial da União Europeia*, Luxemburgo, 5 jul. 2024. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32024L1760. Acesso em: 20 out. 2026.

CONVENÇÃO DAS NAÇÕES UNIDAS CONTRA A CORRUPÇÃO. *Escritório das Nações Unidas sobre Drogas e Crime* (UNODC), Brasília, [2003?]. Disponível em: https://www.unodc.org/lpo-brazil/pt/corrupcao/convencao.html. Acesso em: 15 fev. 2025.

FERRELL, O. C.; FRAEDRICH, John; FERRELL, Linda. *Ética empresarial: dilemas, tomadas de decisões e casos*. Tradução de Cecília Arruda. Rio de Janeiro: Reichmann & Affonso, 2001.

GIN, Camila de Moura. Uma breve análise sobre a legislação anticorrupção no mundo. In: SEMINÁRIO NACIONAL DEMANDAS SOCIAIS E POLÍTICAS PÚBLICAS NA SOCIEDADE CONTEMPORÂNEA, 12., 2016, Santa Cruz do Sul. *Anais* [...]. Santa Cruz do Sul: UNISC, 2016. p. 1-15. Disponível em: https://online.unisc.br/acadnet/anais/index.php/snpp/article/view/14677/3102. Acesso em: 20 out. 2026.

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA (IBGC). Governança corporativa. *IBGC*, São Paulo, [2025?]. Disponível em: https://www.ibgc.org.br/conhecimento/governanca-corporativa. Acesso em: 18 fev. 2025.

INSTITUTO ETHOS. Manifesto para uma governança corporativa em direitos humanos: um chamado para ação. *Instituto Ethos*, São Paulo, 4 dez. 2024. Disponível em: https://www.ethos.org.br/publicacao/manifesto-para-uma-governanca-corporativa-em-direitos-humanos-um-chamado-para-acao/. Acesso em: 20 out. 2026.

MAURO, Carlos; CABRAL, Gabriel; CAPANEMA, Renato; RAMOS, Tânia. *Muitos*: como as ciências comportamentais podem tornar os programas de compliance. São Paulo: Editora Brasileira, 2021.

OCDE. Convenção sobre o Combate da Corrupção de Funcionários Públicos Estrangeiros em Transações Comerciais Internacionais. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto/d3678.htm. Acesso em: 20 jun. 2026.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS (ONU). Declaração Universal dos Direitos Humanos. *Nações Unidas Brasil*, [2025?]. Disponível em: https://brasil.un.org/sites/default/files/2025-03/ONU_DireitosHumanos_DUDH_UNICRio_20250310.pdf. Acesso em: 22 jun. 2026.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS (ONU). Objetivos de Desenvolvimento Sustentável. *Nações Unidas no Brasil*, [202-]. Disponível em: https://brasil.un.org/pt-br/sdgs. Acesso em: 23 jun. 2026.

SILVEIRA, Alexandre Di Miceli da. *Ética empresarial na prática: soluções para gestão e governança no século XXI*. Rio de Janeiro: Alta Books, 2018.

TRANSPARÊNCIA INTERNACIONAL – BRASIL. Índice de Percepção da Corrupção 2024. *Transparência Internacional – Brasil*, 2025. Disponível em: https://transparenciainternacional.org.br/ipc/2024. Acesso em: 22 jun. 2026.

UNITED STATES OF AMERICA. Foreign Corrupt Practices Act of 1977. *Public Law 95-213, 19 dez. 1977*. Washington, DC: U.S. Government Publishing Office, 1977.

Capítulo 3

Privacidade e proteção de dados como valor organizacional na prática

Incidentes de segurança na era da IA:

quando o problema vai além do vazamento de dados

Caio César Carvalho Lima

Caio César Carvalho Lima é mestre em Direito Processual Civil pela Pontifícia Universidade Católica de São Paulo (PUC-SP); professor em cursos de pós-graduação, ministrando disciplinas de Direito Digital, Proteção de Dados e Inteligência Artificial; autor de artigos e capítulos de livro envolvendo esses temas; sócio do escritório Vainzof, Lima e Karassawa Sociedade de Advogados.

Introdução

Durante anos, a gestão de incidentes de segurança foi estruturada em torno de uma pergunta relativamente conhecida: houve comprometimento da confidencialidade, da integridade, da disponibilidade ou da autenticidade de informações? A expansão da inteligência artificial exige uma pergunta adicional e mais difícil: o sistema produziu, recomendou ou executou algo capaz de causar dano, ainda que nenhum dado tenha sido propriamente vazado?

A mudança não é apenas tecnológica. Ela altera o objeto da investigação, as evidências que precisam ser preservadas, a composição da sala de crise e o próprio raciocínio jurídico sobre comunicação, responsabilidade e reparação. Um agente de Inteligência Artificial (IA) conectado a e-mails, bases internas e ferramentas de pagamento pode expor dados pessoais, revelar segredos de negócio, discriminar candidatos, autorizar uma operação indevida ou interromper um processo crítico a partir de uma única instrução maliciosa. Em situações assim, tratar o evento apenas como incidente de segurança da informação produz uma resposta incompleta.

O conceito de incidente de IA é mais amplo. A Organização para Cooperação e Desenvolvimento Econômico (OCDE) considera incidente o evento em que o desenvolvimento, o uso ou o mau funcionamento de um sistema de IA provoca dano; e trata como perigo de IA a situação que poderia plausivelmente provocá-lo, mesmo antes da materialização. Essa distinção é importante porque uma governança madura não deve esperar o dano para agir. O *near miss*, a perda momentânea de controle, a resposta discriminatória identificada em teste ou a execução bloqueada por uma barreira de segurança também precisam ser registrados, investigados e convertidos em aprendizado.

1. A IA é, ao mesmo tempo, vetor, alvo e instrumento de resposta

A relação entre IA e incidentes tem pelo menos três dimensões. Na primeira, a tecnologia amplia ataques já conhecidos. Modelos generativos reduzem o custo de produzir *phishing* convincente, código malicioso, engenharia social personalizada e conteúdos sintéticos usados em fraude. A automação aumenta escala e velocidade; a qualidade linguística elimina sinais que antes ajudavam a vítima a reconhecer o golpe.

Na segunda, a própria IA se torna alvo. *Prompt injection*, envenenamento de dados, manipulação de modelos, extração de informações, comprometimento da cadeia de fornecedores e abuso de permissões não se encaixam perfeitamente nos *playbooks* tradicionais. A Open Worldwide Application Security Project (OWASP) mantém a injeção de *prompts* entre os riscos centrais de aplicações baseadas em grandes modelos de linguagem. O problema é especialmente grave nos agentes: uma resposta inadequada deixa de ser apenas texto e pode transformar-se em ação sobre sistemas externos.

Na terceira dimensão, a IA integra a defesa. Ela auxilia correlação de eventos, detecção de anomalias, priorização de alertas e análise de grandes volumes de *logs*. Esse uso, porém, não elimina o dever de supervisão. Uma ferramenta defensiva também pode alucinar, omitir sinais, reproduzir vieses ou ser manipulada. A organização não deve transferir à IA a decisão final sobre gravidade, comunicação ou atribuição de responsabilidade sem validação humana e registro das premissas adotadas.

Por isso, nem todo incidente de IA é um incidente de dados pessoais, e nem todo incidente envolvendo IA decorre de um ataque. Pode haver falha de desempenho, deriva do modelo, recomendação clinicamente inadequada, decisão automatizada discriminatória ou conteúdo falso com impacto reputacional. Em sentido inverso, quando dados pessoais são afetados, o regime da Lei Geral de Proteção de Dados Pessoais (LGPD) incide integralmente, ainda que a causa técnica tenha sido específica de IA.

2. Taxonomia própria para incidentes de IA

A primeira dificuldade prática é definir quando um comportamento indesejado deixa de ser erro operacional e passa a constituir incidente. Em software convencional, a fronteira entre *bug* e incidente costuma depender da exploração, da indisponibilidade ou do comprometimento de informação. Em IA, um sistema pode funcionar exatamente como foi tecnicamente projetado e, ainda assim, gerar resultado juridicamente inaceitável. Um modelo de crédito pode aplicar corretamente uma correlação estatística que reproduza discriminação indireta; um agente pode executar fielmente uma instrução maliciosa escondida em documento legítimo; um *chatbot* pode revelar informação que recuperou de fonte para a qual possuía acesso formal, mas que não deveria ter utilizado naquele contexto.

Por isso, a classificação deve considerar pelo menos quatro famílias de eventos. A primeira reúne ataques contra o sistema: *prompt injection*, extração de modelo, envenenamento, evasão, *backdoors*, exploração de dependências e comprometimento de credenciais. A segunda abrange falhas do sistema: alucinações materialmente relevantes, deriva, desempenho abaixo do limite aprovado, comportamento emergente, indisponibilidade e perda de controle sobre agentes. A terceira envolve falhas de uso e governança: *shadow AI*, finalidade incompatível, base de conhecimento inadequada, supervisão ineficaz e implementação fora do contexto validado. A quarta cobre impactos produzidos com o auxílio de IA: fraude sintética, violação de imagem, discriminação, manipulação informacional e decisões que afetem saúde, emprego, crédito ou acesso a serviços.

As categorias podem coexistir. Imagine um agente corporativo que lê documentos recebidos de terceiros. Uma instrução oculta induz o agente a consultar a folha de pagamento e enviar o resultado para endereço externo. Há ataque por *prompt injection*, falha de segregação entre dados e instruções, permissões excessivas, exposição de dados pessoais e segredos de negócio e, possivelmente, descumprimento contratual. Se a organização enxergar apenas o vazamento, poderá corrigir o canal de saída, mas manter intacta a arquitetura que permitiu ao conteúdo não confiável comandar uma ferramenta privilegiada.

Também é necessário separar incidente, perigo e não conformidade. O incidente pressupõe dano efetivo ou potencial diretamente associado ao comportamento da IA. O perigo é a condição capaz de produzir esse dano, como a descoberta de que um agente pode contornar aprovação humana. A não conformidade é o descumprimento de requisito, ainda que nenhum dano plausível tenha sido identificado, como ausência de documento obrigatório. A distinção evita dois extremos: registrar todo erro banal como crise ou ignorar sinais precursores porque o dano ainda não se concretizou.

A OCDE propõe um vocabulário comum justamente para permitir interoperabilidade entre setores e países. Seu *framework* recomenda registrar contexto, sistema, atores, danos, pessoas afetadas, severidade, causas e medidas adotadas. O valor dessa padronização não é apenas estatístico. Uma taxonomia consistente permite comparar eventos, identificar reincidência, calibrar controles e reconhecer quando incidentes aparentemente distintos compartilham o mesmo modo de falha.

3. Severidade não pode ser medida apenas pelo volume de dados

Matrizes tradicionais de incidentes frequentemente combinam número de registros, sensibilidade dos dados e extensão da indisponibilidade. Esses fatores continuam relevantes, mas são insuficientes para IA. Um único resultado pode ser gravíssimo: a recomendação clínica errada para uma pessoa, a recusa discriminatória de uma contratação ou a ordem autônoma que movimenta valor elevado. Em sentido oposto, milhares de respostas de baixa relevância podem representar risco menor. A análise deve medir natureza do direito afetado, reversibilidade, escala real e potencial, duração, autonomia, possibilidade de propagação e vulnerabilidade das pessoas expostas.

Autonomia merece peso próprio. Quanto maior a capacidade do sistema de executar ações sem confirmação, mais curto deve ser o intervalo entre detecção e contenção. Também importa o alcance das permissões: acesso de leitura a uma base pública não equivale a autorização para escrever em sistemas de produção, enviar mensagens, contratar serviços ou movimentar recursos. Para agentes, o *blast radius* deve ser calculado não apenas pelos dados efetivamente acessados, mas pela cadeia de ferramentas, identidades e sistemas que poderiam ser acionados nas condições observadas.

Outro elemento é a replicabilidade. Resposta errada isolada pode resultar de combinação improvável; uma falha reproduzível por qualquer usuário tende a exigir contenção ampla. A ausência de reprodução, porém, não encerra a investigação. Modelos probabilísticos podem não repetir o mesmo resultado, e atualizações silenciosas de fornecedor podem alterar o comportamento antes da coleta de evidências. Devem ser preservados contexto, versão, temperatura, parâmetros, instruções e fontes recuperadas, sempre que tecnicamente possível.

A severidade também muda ao longo do tempo. Um evento inicialmente classificado como baixo pode revelar efeito sistêmico após novas evidências, enquanto uma suspeita grave pode ser reduzida por confirmação de que barreiras impediram qualquer ação. O processo precisa admitir reclassificação, com registro de quem decidiu, quando, com base em quais elementos e quais consequências operacionais e regulatórias decorreram da mudança.

4. No Brasil, não existe vácuo regulatório

A ausência, até o momento, de uma lei geral de IA em vigor não significa ausência de deveres. Constituição Federal, Código Civil, Código de Defesa do Consumidor, legislação trabalhista, regras setoriais, deveres de sigilo, propriedade intelectual e LGPD já alcançam parte relevante dos danos produzidos ou ampliados por sistemas de IA. O PL nº 2.338/2023, aprovado pelo Senado e ainda em tramitação na Câmara dos Deputados em 31 de julho de 2026, adiciona uma arquitetura específica baseada em risco, mas não inaugura a responsabilidade jurídica pelo uso da tecnologia.

Quando o evento comprometer dados pessoais, a Resolução CD/ANPD nº 15/2024 oferece o ponto de partida. O controlador deve comunicar à Agência Nacional de Proteção de Dados e aos titulares, em três dias úteis, o incidente que possa acarretar risco ou dano relevante. O prazo começa com o conhecimento de que o evento afetou dados pessoais; a comunicação preliminar pode ser complementada, de forma fundamentada, em vinte dias úteis. Mesmo quando a comunicação não for necessária, o incidente deve ser registrado e o registro mantido por pelo menos cinco anos.

A presença de IA não altera automaticamente o critério legal de comunicação, mas modifica a análise concreta. Um *prompt* pode conter dado pessoal; uma base vetorial pode reproduzir informação sensível; uma inferência pode revelar condição de saúde ou perfil financeiro; um agente pode combinar fontes que, isoladamente, pareciam pouco críticas. Também se deve avaliar não apenas o que foi exibido, mas o que o sistema podia acessar, quais ações podia executar e se houve persistência em memórias, *logs*, caches ou bases de *feedback*.

A experiência regulatória brasileira reforça outro ponto: a decisão de não comunicar precisa ser tão bem do-

cumentada quanto a decisão de comunicar. A Agência pode exigir o registro das operações de tratamento, o relatório de impacto e o relatório de tratamento do incidente, além de realizar auditorias ou inspeções. A falta de *logs*, de plano de resposta e de documentação tempestiva compromete a capacidade de demonstrar diligência e pode converter uma falha técnica em problema de responsabilização e fiscalização.

No plano internacional, a tendência é semelhante, mas com um conceito autônomo de incidente grave de IA. O artigo 73 do AI Act europeu estabelece reporte de incidentes graves envolvendo sistemas de alto risco, e a Comissão Europeia publicou orientação e modelo preliminares para operacionalizar o dever a partir de agosto de 2026. O foco ultrapassa dados: alcança morte ou dano grave à saúde, perturbação séria de infraestrutura crítica, violação de direitos fundamentais e danos graves à propriedade ou ao meio ambiente. Grupos multinacionais precisarão coordenar esse regime com GDPR, NIS2, DORA e obrigações setoriais, evitando comunicações contraditórias sobre o mesmo fato.

4.1 O mosaico regulatório exige uma única análise, não várias investigações

Um mesmo evento pode ativar deveres paralelos com conceitos, destinatários e prazos diferentes. No Brasil, além da Agência, podem ser relevantes Banco Central, Comissão de Valores Mobiliários, Superintendência de Seguros Privados, Agência Nacional de Saúde Suplementar, autoridades de defesa do consumidor e órgãos setoriais. Contratos podem impor comunicação a clientes em prazo ainda mais curto. Companhias abertas precisam avaliar impacto sobre divulgação ao mercado. Relações de trabalho, segredo profissional e infraestruturas críticas acrescentam camadas próprias.

O ponto central é evitar que cada área produza uma versão autônoma do fato. A organização deve manter uma fonte única de verdade: cronologia validada, sistemas envolvidos, fatos confirmados, hipóteses em investigação, população afetada, medidas de contenção e decisões. A partir dessa base, cada comunicação pode ser adaptada ao requisito aplicável. Sem esse núcleo comum, é frequente que o regulador receba uma causa, o cliente receba outra e a imprensa uma terceira, enfraquecendo credibilidade e defesa.

Na LGPD, a análise não termina em confidencialidade. A Resolução nº 15/2024 inclui violações de integridade, disponibilidade e autenticidade. Em IA, isso alcança alteração indevida de dados usados pelo modelo, indisponibilidade de serviço baseado em IA e produção ou uso de informação cuja origem não pode ser validada. Se uma decisão automatizada é tomada a partir de dado adulterado, o risco ao titular pode decorrer da integridade comprometida, mesmo sem divulgação a terceiro.

Há ainda uma diferença entre comunicar o incidente de dados e explicar a lógica ou o comportamento do sistema. A comunicação aos titulares deve ser simples, direta e útil para mitigação, mas não precisa revelar detalhes técnicos que aumentem risco ou exponham segredo de negócio. Ao regulador, em contrapartida, pode ser necessário apresentar informação técnica mais densa, inclusive medidas de segurança, causa-raiz e relatório de tratamento. O pedido de sigilo deve ser específico e fundamentado; não se deve pressupor que todo anexo técnico será automaticamente restrito.

Na União Europeia, o AI Act incorpora a cibersegurança como elemento de segurança do produto. Para sistemas de alto risco, gestão de riscos, *logging*, supervisão humana, precisão, robustez e cibersegurança formam requisitos integrados. O artigo 73 adota, como regra, reporte imediatamente após estabelecida a relação causal ou razoável probabilidade de relação entre o sistema e o incidente grave, observado o limite de quinze dias, com prazos mais curtos em situações especialmente graves. Isso reforça uma lógica já presente em proteção de dados: não se espera a conclusão pericial para iniciar o fluxo regulatório.

O desafio de grupos globais será coordenar AI Act, GDPR, NIS2, DORA, Cyber Resilience Act e normas nacionais. O evento pode ser grave para uma lei e não comunicável para outra. A resposta correta não é escolher um único regime, mas construir uma matriz por jurisdição contendo gatilho, responsável, destinatário, prazo, conteúdo, sigilo e regra de complementação.

5. A investigação precisa preservar a cadeia decisória da máquina

Em um incidente convencional, *logs* de rede, registros de acesso, imagens forenses e cronologia de eventos são evidências essenciais. Em IA, isso continua válido, mas não basta. A investigação pode depender de *prompts* e respostas, instruções de sistema, versão do modelo, parâmetros, políticas de moderação, chamadas de ferramentas, documentos recuperados por RAG, *embeddings* consultados, memória do agente, identidades não humanas, alterações de configuração, dados de treinamento ou ajuste, métricas de deriva e trilhas da supervisão humana.

Essas evidências precisam existir antes do incidente. Se a organização não definiu telemetria e retenção no desenho do sistema, parte da cadeia causal pode ser irrecuperável. O National Institute of Standards and Technology (NIST) tem enfatizado a necessidade de inventariar identidades não humanas, preparar telemetria específica e definir previamente opções de contenção. Desligar um agente, revogar uma credencial ou reverter um modelo pode interromper operações e corromper estados a jusante. A melhor decisão técnica depende, portanto, de uma avaliação prévia do impacto empresarial de cada medida.

A preservação integral, contudo, não autoriza coleta indiscriminada. *Logs* de *prompts* podem conter dados pessoais, segredos de negócio e comunicações protegidas. A arquitetura deve conciliar rastreabilidade com minimização, controle de acesso, criptografia, prazos de retenção e segregação. Em investigações sensíveis, também é necessário preservar integridade e cadeia de custódia, restringir circulação interna e avaliar sigilo profissional ou legal.

A análise de causa-raiz deve evitar uma explicação confortável, mas insuficiente: "a IA errou". É preciso identificar se houve vulnerabilidade do modelo, integração não autorizada, permissões excessivas, dado inadequado, falha de validação, supervisão humana meramente formal, mudança não controlada, fornecedor comprometido ou decisão de negócio que aceitou risco sem evidência suficiente. O modelo pode ser o ponto visível de uma falha essencialmente organizacional.

5.1 O que deve ser preservado e por quê?

A investigação deve reconstruir a cadeia entre entrada, processamento, decisão e ação. Para isso, convém organizar evidências em camadas. Na camada de interação estão *prompt*, resposta, anexos, identidade do usuário, data, canal e contexto da sessão. Na camada de orquestração estão instrução de sistema, políticas, travas de segurança, memória, chamadas de função, sequência de raciocínio disponibilizada pelo sistema e decisões do agente. Na camada de conhecimento estão consultas, documentos recuperados, permissões da fonte, versão do índice e filtros aplicados. Na camada do modelo estão fornecedor, identificador e versão, parâmetros e alterações. Na infraestrutura estão credenciais, *tokens*, APIs, rede, eventos de nuvem e sistemas de destino.

Nem toda organização terá acesso a todas essas camadas. Modelos contratados como serviço podem não disponibilizar pesos, dados de treinamento ou *logs* internos. Essa limitação não deve ser descoberta durante a crise. *Due diligence* e contratos precisam indicar antecipadamente quais evidências o fornecedor produz, por quanto tempo as retém, em que formato as fornece, em qual prazo coopera e se atualizações de modelo são identificáveis. Quando não houver visibilidade suficiente, o risco residual deve influenciar o caso de uso permitido.

A cadeia de custódia é igualmente importante. Capturas de tela isoladas são frágeis; o ideal é preservar exportações originais, metadados, *hashes*, controles de acesso e histórico de manipulação. Quando houver investigação trabalhista, criminal ou litígio provável, Jurídico e perícia devem alinhar a coleta para evitar perda de valor probatório. Ao mesmo tempo, deve-se impedir que a própria investigação replique dados sensíveis para ambientes menos protegidos.

A reprodução do incidente exige ambiente controlado. Reexecutar *prompt* malicioso em produção pode renovar a exposição ou acionar ferramentas externas. Testes devem usar cópia isolada, credenciais revogadas, dados sintéticos ou anonimizados e bloqueio de tráfego de

saída, sempre que viável. O objetivo é confirmar modo de falha sem ampliar o dano. Também se deve registrar quando a reprodução não foi tentada e por qual risco.

A causa-raiz deve resultar em hipóteses verificáveis. Erro humano, falha do fornecedor e comportamento inesperado do modelo não são conclusões suficientes. A investigação deve alcançar o controle que faltou ou falhou: segregação, autorização, validação de saída, monitoramento, gestão de mudança, qualidade de dados, treinamento, limite de autonomia ou resposta do fornecedor. Só então é possível desenhar remediação mensurável.

5.2 A sala de crise precisa ser redesenhada

Incidentes de IA raramente pertencem a uma única área. Segurança da informação pode conter o ambiente, mas talvez não consiga avaliar discriminação, propriedade intelectual, impacto clínico, dever de transparência ou segurança do produto. Ciência de dados pode explicar o modelo, mas não decidir sozinha sobre comunicação a titulares, mercado ou reguladores. Jurídico, privacidade, compliance, negócio, comunicação, engenharia de IA, segurança, gestão de riscos e, conforme o caso, especialistas setoriais devem atuar com responsabilidades e alçadas previamente definidas.

A classificação inicial deve responder a cinco questões: qual sistema e qual versão participaram do evento; quais pessoas, direitos, dados, ativos e processos foram afetados; que autonomia e permissões o sistema possuía; se o dano já ocorreu ou havia possibilidade plausível; e quais regimes jurídicos e contratos podem impor comunicação. A resposta não deve esperar certeza. É possível conter, preservar evidências e fazer comunicação preliminar enquanto a investigação continua, desde que incertezas e hipóteses sejam claramente registradas.

Também é indispensável olhar para terceiros. Boa parte da cadeia de IA combina modelos, nuvem, conectores, bases externas, ferramentas open source e prestadores de monitoramento. Contratos devem disciplinar notificação rápida, acesso a *logs*, cooperação forense, mudanças de modelo, subcontratação, retenção de evidências, correção de vulnerabilidades e distribuição de custos. A expressão genérica "medidas adequadas de segurança" é pouco útil quando ninguém sabe quem consegue reconstruir uma chamada de ferramenta ou suspender uma integração.

Por fim, comunicar não é confessar culpa. A comunicação bem construída protege pessoas, permite mitigação e demonstra transparência. Deve informar o que ocorreu, quais riscos são concretamente relevantes, quais providências foram tomadas e o que o destinatário pode fazer, sem especulação, linguagem alarmista ou exposição de detalhes que ampliem a vulnerabilidade. Mensagens a titulares, reguladores, clientes, colaboradores e imprensa precisam partir de uma cronologia comum, mas considerar finalidades e deveres distintos.

5.3 *Playbook* específico para as primeiras horas

Nas primeiras horas, a organização precisa atuar em trilhas simultâneas. A detecção deve ser confirmada sem destruir estado volátil; o sistema e suas integrações devem ser identificados; evidências mínimas precisam ser preservadas; e deve haver decisão sobre contenção. Em paralelo, o time jurídico mapeia dados, pessoas, direitos, contratos, países e reguladores potencialmente envolvidos. Comunicação e atendimento preparam respostas sem antecipar fatos não confirmados.

A contenção de IA comporta alternativas graduais. Pode-se suspender todo o sistema, retirar apenas determinada ferramenta, reduzir permissões, desabilitar memória, bloquear tipos de entrada, retornar a versão anterior, impor confirmação humana, limitar usuários ou migrar para fluxo manual. A escolha deve equilibrar risco de continuidade e impacto da interrupção. Um plano de contenção de curto prazo, preparado antes da implantação, evita que a única opção disponível seja desligar tudo ou continuar exposto.

A retomada não deve decorrer apenas da correção aparente. É necessário definir critérios de saída: vulnerabilidade corrigida ou mitigada; testes adversariais concluídos; permissões revistas; evidências preservadas; monitoramento intensificado; usuários e áreas afetadas orientados; riscos residuais aceitos por autoridade competente; e comunicações realizadas ou formalmente des-

cartadas. Para sistemas críticos, pode ser adequado um retorno progressivo, com amostragem humana e limites temporários de autonomia.

Depois da estabilização, a organização deve produzir relatório que diferencie fatos, inferências e pontos ainda inconclusivos. O documento deve incluir cronologia, arquitetura, causa imediata e sistêmica, dados e direitos afetados, extensão real e potencial, decisões de contenção, comunicações, recuperação, risco residual, responsáveis e plano de melhoria. Esse relatório não é mera memória técnica: sustenta prestação de contas, defesa regulatória, acionamento de seguro, execução contratual e aprendizado.

A revisão pós-incidente deve alcançar casos semelhantes. Se a causa foi permissão excessiva em um agente, não basta corrigir aquele agente; é preciso localizar outros sistemas com o mesmo padrão. Se o fornecedor alterou silenciosamente o modelo, devem ser revistos contratos e controles de mudança em toda a cadeia. A resposta termina quando o risco sistêmico foi tratado, não quando o serviço voltou ao ar.

6. Governança é a preparação para o incidente

A melhor resposta começa antes da crise. Inventário de sistemas e agentes, classificação de risco, avaliação de impacto, testes adversariais, *red teaming*, gestão de acessos, validação antes da produção, monitoramento de deriva, controle de mudanças e plano de descontinuação não são controles paralelos: formam a infraestrutura de resposta. O NIST AI RMF e seu perfil para IA generativa, o framework de cibersegurança para IA da ENISA e o monitor de incidentes da OCDE convergem na necessidade de governança contínua, documentação e aprendizado.

Simulações devem incluir cenários propriamente algorítmicos. Não basta testar *ransomware* e indisponibilidade. É preciso simular *prompt injection* em agente conectado a bases internas, vazamento por RAG, fraude com identidade sintética, alteração silenciosa de modelo pelo fornecedor, decisão discriminatória em escala, perda de controle sobre ferramentas e falha do mecanismo de supervisão. O exercício deve testar tanto a contenção quanto a capacidade de localizar evidências, decidir sob incerteza e cumprir vários prazos regulatórios.

Governança madura não é a promessa de que a IA nunca falhará. É a capacidade de perceber cedo, limitar o alcance, proteger pessoas, reconstruir a cadeia causal, reparar consequências e transformar o evento em controle melhor. Na era dos agentes autônomos, a pergunta mais relevante já não é apenas se a organização sofreu um incidente. É se ela consegue explicar, com evidências, o que sua IA viu, decidiu, fez e por quê.

Considerações finais

Um programa consistente de governança começa por inventário que não se limite ao nome da ferramenta. Para cada sistema, devem constar finalidade, proprietário, desenvolvedor e fornecedor, versão, usuários, pessoas afetadas, bases de dados, integrações, identidades não humanas, grau de autonomia, decisões suportadas, criticidade, jurisdições, logs disponíveis, plano de contenção e responsável pela descontinuação. Sem esse mapa, a sala de crise perde tempo para descobrir o que deveria ser conhecido.

O monitoramento também deve ser orientado a risco. Indicadores podem incluir taxa de respostas bloqueadas, tentativas de *prompt injection*, uso de ferramentas privilegiadas, exceções à supervisão humana, variação de desempenho por grupo, deriva, acesso atípico a bases, mudança de versão e incidentes. Métrica sem limite e responsável, porém, não gera controle. Cada indicador precisa de gatilhos, rotina de revisão e ação de escalonamento.

Red teaming não substitui monitoramento, e conformidade não substitui segurança. Testes prévios capturam comportamentos conhecidos em condições delimitadas; produção introduz usuários, dados, integrações e ataques novos. O ciclo adequado combina avaliação de impacto, testes antes da liberação, observabilidade contínua, canais de relato, auditoria periódica e revisão após

mudanças relevantes. O código de prática britânico para cibersegurança de IA, o NIST e a European Union Agency for Cybersecurity (ENISA) convergem em *secure-by-design*, gestão de cadeia de suprimentos, *logging*, controle de acesso, atualização e resposta a incidentes.

A supervisão humana deve ser desenhada como controle real. É preciso definir qual informação chega ao revisor, quanto tempo ele possui, que autoridade tem para discordar, como sua decisão é registrada e se há risco de discriminação. Aprovação humana automática, sem contexto ou possibilidade efetiva de intervenção, apenas desloca formalmente a responsabilidade sem reduzir risco.

Por fim, o conselho e a alta administração precisam receber informação que permita decisão. Não é necessário discutir cada *prompt*, mas conhecer sistemas críticos, concentração em fornecedores, incidentes relevantes, tendências, riscos aceitos, limitações de evidência e eficácia dos planos de ação. Incidentes de IA são tema de tecnologia, mas também de governança corporativa: revelam como a organização distribui autoridade sobre sistemas capazes de influenciar pessoas e executar ações em seu nome.

Referências

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). *Resolução CD/ANPD nº 15, de 24 de abril de 2024*. Aprova o Regulamento de Comunicação de Incidente de Segurança. Diário Oficial da União: Brasília, DF, 26 abr. 2024. Disponível em: https://www.gov.br/anpd/pt-br/acesso-a-informacao/institucional/atos-normativos/regulamentacoes_anpd. Acesso em: 20 out. 2026.

BRASIL. Senado Federal. *Projeto de Lei nº 2.338, de 2023*. Dispõe sobre o uso da Inteligência Artificial. Brasília, DF: Senado Federal, 2023. Texto aprovado pelo Senado Federal em 2024 e remetido à Câmara dos Deputados em 2025. Disponível em: https://www25.senado.leg.br/web/atividade/materias. Acesso em: 20 out. 2026.

EUROPEAN COMMISSION. *Draft guidance and reporting template on serious AI incidents under Article 73 of the AI Act*. Shaping Europe's Digital Future, 26 set. 2025. Disponível em: https://digital-strategy.ec.europa.eu/en/consultations/ai-act-commission-issues-draft-guidance-and-reporting-template-serious-ai-incidents-and-seeks. Acesso em: 20 out. 2026.

EUROPEAN UNION. *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence* (Artificial Intelligence Act). Official Journal of the European Union, 12 jul. 2024. Disponível em: https://eur-lex.europa.eu/eli/reg/2024/1689/oj. Acesso em: 20 out. 2026.

EUROPEAN UNION AGENCY FOR CYBERSECURITY (ENISA). *Multilayer framework for good cybersecurity practices for AI*. [*S. l.*]: ENISA, 2023. Disponível em: https://www.enisa.europa.eu/publications/multilayer-framework-for-good-cybersecurity-practices-for-ai. Acesso em: 20 out. 2026.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). *Artificial Intelligence Risk Management Framework*: Generative Artificial Intelligence Profile. Gaithersburg, MD: NIST, 2024. (NIST AI 600-1). DOI: https://doi.org/10.6028/NIST.AI.600-1.

NISTNATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). *Cybersecurity Framework Profile for Artificial Intelligence (Cyber AI Profile)*: NIST Community Profile. Gaithersburg, MD: NIST, 2025. (NIST IR 8596, Initial Preliminary Draft). DOI: https://doi.org/10.6028/NIST.IR.8596.iprd. Disponível em: https://csrc.nist.gov/pubs/ir/8596/iprd. Acesso em: 20 out. 2026.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD). AI Incidents and Hazards Monitor: overview and methodology. *OECD.AI*, [2024?]. Disponível em: https://oecd.ai/en/incidents-methodology. Acesso em: 20 out. 2026.

OECD AIOPEN WORLDWIDE APPLICATION SECURITY PROJECT (OWASP). *Top 10 for LLM Applications 2025*. [S. l.]: OWASP, 2024. Disponível em: https://genai.owasp.org/resource/owasp-top-10-for-llm-applications-2025/. Acesso em: 20 out. 2026.

OWASP Gen AI Security ProjectUNITED KINGDOM. Department for Science, Innovation and Technology. *Code of Practice for the Cyber Security of AI*. London: UK Government, 2025. Disponível em: https://www.gov.uk/government/publications/ai-cyber-security-code-of-practice. Acesso em: 20 out. 2026. GOV.UK+1

IN-Q-TEL. *AI Incident Response Guidebook: Recommendations for Practitioners*. 2024.

VLK ADVOGADOS. *Comunicação de Incidentes de Segurança*. 2. ed. atualizada, jun. 2026; Inteligência Artificial: riscos, incidentes e governança, jul. 2026.

LGPD além da conformidade:

maturidade, risco e valor para o negócio

Da obrigação legal à estratégia de governança, confiança e competitividade corporativa

Lucas Lessa Ferreira Costa

Lucas Lessa Ferreira Costa é especialista de Controles Internos na Copapa. Graduado em Computação e Gestão de Pessoas, pós-graduando em Data Analytics e Inteligência Artificial Aplicada a Negócios e em Governança, Riscos, Controle e Compliance. Atua no fortalecimento da governança, controles internos, certificações e gestão de riscos, promovendo a ética, a integridade e a melhoria contínua.

Vanessa Natalie Baniski dos Santos

Vanessa Natalie Baniski dos Santos é gerente executiva de Auditoria na Copapa. Graduada em Ciências Contábeis e Análise e Desenvolvimento de Sistemas, possui mais de 12 anos de experiência em Auditoria Interna e GRC. É pós-graduada em Auditoria Interna e Liderança e Dinâmica de Negócios, com MBAs em GRC e Liderança, Inovação e Comunicação Executiva. Sua trajetória inclui os setores de tecnologia, educação, agronegócio e indústria.

Introdução

A transformação digital intensificou a coleta, o compartilhamento e a análise de dados pessoais no ambiente empresarial. Nesse cenário, os dados passaram a representar ativos estratégicos para as organizações, ao mesmo tempo em que ampliaram riscos legais, operacionais, reputacionais e éticos relacionados ao seu tratamento inadequado. Desse modo, a proteção de dados pessoais deixou de ser apenas uma exigência legal para se tornar um elemento estratégico de governança, gestão de riscos e geração de valor para as organizações.

No Brasil, a Lei nº 13.709/2018, denominada Lei Geral de Proteção de Dados Pessoais (LGPD), estabelece normas sobre o tratamento de dados pessoais, por pessoas naturais ou jurídicas, de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural (Brasil, 2018). Assim, a própria legislação demonstra que a proteção de dados não se limita ao cumprimento formal de obrigações, pois exige a observância de princípios como finalidade, adequação, necessidade, transparência, segurança, prevenção, responsabilização e prestação de contas.

Para Pinheiro (2024), a adequação à LGPD ultrapassa a conformidade documental, pois demanda revisão dos modelos de governança corporativa, implementação de mecanismos de compliance digital, investimentos em segurança da informação, aprimoramento dos fluxos de tratamento de dados pessoais, fortalecimento dos controles internos e desenvolvimento de uma cultura organizacional voltada à privacidade e à proteção de dados.

Diante desse contexto, a proteção de dados pessoais assume papel estratégico para as organizações, contribuindo para a mitigação de riscos, o fortalecimento da reputação institucional, a melhoria dos processos internos e a ampliação da confiança nas relações de negócio. Empresas que tratam a LGPD apenas como obrigação regulatória tendem a atuar de forma reativa, enquanto organizações que incorporam a privacidade à cultura, aos processos e às decisões estratégicas podem alcançar níveis mais elevados de maturidade organizacional e competitividade.

Nesse contexto, maturidade em privacidade pode ser compreendida como o grau de integração da proteção de dados aos processos, à governança, à gestão de riscos e à cultura organizacional. Organizações mais maduras não apenas atendem aos requisitos legais, mas incorporam a privacidade como elemento estratégico de suas decisões e operações.

Assim, o presente artigo parte do seguinte problema de pesquisa: como as organizações podem transformar a adequação à LGPD em um modelo de maturidade, gestão de riscos e geração de valor para o negócio?

O objetivo geral consiste em analisar a LGPD além da conformidade legal, demonstrando como a proteção de dados pode contribuir para a maturidade organizacional, a redução de riscos e o fortalecimento da confiança no ambiente empresarial.

Para alcançar esse objetivo, foram definidos os seguintes objetivos específicos: a) compreender a LGPD como instrumento de governança corporativa; b) relacionar proteção de dados, gestão de riscos e segurança da informação; c) demonstrar como programas de privacidade podem gerar valor para o negócio; e d) apresentar práticas aplicáveis ao cotidiano das empresas.

Quanto aos procedimentos metodológicos, o presente estudo caracteriza-se como uma pesquisa bibliográfica e documental, desenvolvida a partir da análise da legislação aplicável, normas técnicas, publicações especializadas e referenciais relacionados à governança corporativa, gestão de riscos, segurança da informação e proteção de dados pessoais.

Justifica-se o estudo pela relevância social, jurídica e econômica da proteção de dados pessoais na sociedade digital. A LGPD representa não apenas um marco regulatório, mas também um instrumento de fortalecimento da cidadania, da transparência e da confiança no uso de informações pessoais. Portanto, analisar a LGPD além da conformidade formal permite compreender seu papel como instrumento de governança, gestão de riscos e geração de valor, contribuindo para a construção de organizações mais maduras, responsáveis e preparadas para enfrentar os desafios e aproveitar as oportunidades da economia baseada em dados.

1. Desenvolvimento

1.1 LGPD como instrumento de governança corporativa

A governança corporativa tem assumido papel cada vez mais relevante no contexto organizacional, especialmente diante da crescente complexidade regulatória, da transformação digital e da necessidade de fortalecimento das relações entre as organizações e suas partes interessadas. Nesse cenário, a proteção de dados pessoais deixou de ser uma questão exclusivamente tecnológica ou jurídica e passou a integrar a agenda estratégica das empresas, constituindo um importante elemento da governança corporativa.

Conforme o Instituto Brasileiro de Governança Corporativa (IBGC, 2023), a governança corporativa consiste no sistema pelo qual as organizações são dirigidas, monitoradas e incentivadas, envolvendo os relacionamentos entre sócios, conselho de administração, diretoria, órgãos de fiscalização e demais partes interessadas. Esse sistema é fundamentado nos princípios da integridade, transparência, equidade, responsabilização (*accountability*) e sustentabilidade.

A LGPD apresenta forte convergência com os princípios da governança corporativa ao estabelecer diretrizes para o tratamento de dados pessoais e exigir que as organizações adotem mecanismos capazes de assegurar a conformidade, a segurança e a responsabilização em suas atividades.

De acordo com o artigo 6° da Lei n° 13.709/2018, o tratamento de dados pessoais deve observar princípios como finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas (Brasil, 2018).

A presença dos princípios de transparência, da responsabilização e da prestação de contas evidencia que a LGPD não se limita ao cumprimento de obrigações legais, mas busca promover uma gestão ética, responsável e sustentável dos dados pessoais. Nesse contexto, a legislação aproxima-se dos fundamentos da governança corporativa ao exigir que as organizações demonstrem capacidade de prevenir riscos, monitorar seus processos e prestar contas sobre as atividades de tratamento de dados realizadas.

A adequação à LGPD requer uma abordagem integrada de governança, envolvendo gestão de riscos, compliance, segurança da informação, controles internos e conscientização dos colaboradores. Ao incorporar a proteção de dados aos seus processos e à tomada de decisão, as organizações fortalecem seus mecanismos de controle, aprimoram sua capacidade de resposta a incidentes e reduzem sua exposição a riscos regulatórios, operacionais e reputacionais.

Essa perspectiva é reforçada pelo artigo 50 da LGPD, que incentiva agentes de tratamento a adotarem regras de boas práticas e programas de governança em privacidade voltados à organização do tratamento de dados pessoais, ao estabelecimento de procedimentos, normas de segurança, mecanismos de supervisão e medidas de mitigação de riscos (Brasil, 2018). A previsão legal evidencia que a conformidade com a LGPD não se restringe à elaboração de documentos e políticas formais, mas requer a implementação de processos estruturados, mecanismos de controle e ações contínuas de monitoramento, avaliação e aprimoramento das práticas de proteção de dados.

Sob a perspectiva da governança corporativa, a proteção de dados também deve ser considerada uma responsabilidade da alta administração. O IBGC (2023) destaca que compete aos órgãos de governança assegurar que os riscos relevantes para a organização sejam adequadamente identificados, avaliados, monitorados e tratados. Considerando que incidentes de privacidade podem gerar impactos financeiros, regulatórios, operacionais e reputacionais significativos, a supervisão dos riscos relacionados à proteção de dados torna-se parte integrante das atribuições da administração e dos conselhos.

Da mesma forma, a LGPD fortalece o princípio da *accountability* ao exigir que as organizações sejam capazes de demonstrar evidências da conformidade de suas atividades com os requisitos legais e regulatórios aplicáveis à proteção de dados. Esse conceito está alinhado às práticas modernas de governança corporativa, nas quais não basta apenas cumprir obrigações, mas também comprovar a efetividade dos controles implementados e a diligência na gestão dos riscos corporativos.

Nesse sentido, a proteção de dados pessoais passa a re-

presentar não apenas um requisito regulatório, mas também um instrumento de fortalecimento da governança corporativa. Organizações que incorporam a privacidade aos seus processos decisórios, suas estruturas de controle e seus mecanismos de supervisão tendem a alcançar maior maturidade organizacional, maior capacidade de gestão de riscos e maior transparência e confiança perante clientes, investidores, parceiros, órgãos reguladores e demais partes interessadas.

Assim, a LGPD consolida-se como importante vetor de aprimoramento da governança corporativa, contribuindo para a sustentabilidade, a resiliência e a competitividade das organizações na economia digital. Mais do que um instrumento regulatório, a proteção de dados passa a integrar os mecanismos de governança, gestão de riscos e compliance, fortalecendo a capacidade das organizações de gerar valor e preservar a confiança de suas partes interessadas.

1.2 Proteção de dados, gestão de riscos e segurança da informação

A proteção de dados pessoais está diretamente relacionada à gestão de riscos corporativos, uma vez que o tratamento inadequado de dados pode gerar impactos financeiros, regulatórios, operacionais, reputacionais e estratégicos nas organizações. Na economia digital, os dados pessoais passaram a representar ativos significativos para a execução das atividades, tornando sua proteção uma necessidade não apenas jurídica, mas também gerencial.

Nesse cenário, a LGPD adota uma abordagem fundamentada em prevenção e responsabilização, exigindo que as organizações sejam capazes de identificar, avaliar, tratar e monitorar os riscos relacionados ao tratamento de dados pessoais. Tal direcionamento possui embasamento nos princípios da prevenção, da segurança, da responsabilização e da prestação de contas previstos no artigo 6º da Lei nº 13.709/2018 (Brasil, 2018).

Conforme definido pela ABNT NBR ISO/IEC 27701:2026, a gestão de riscos consiste em "atividades coordenadas para dirigir e controlar uma organização no que se refere a riscos". Nesse sentido, os riscos relacionados à privacidade devem integrar a estrutura corporativa de gestão de riscos, permitindo que as organizações tomem decisões mais assertivas e proporcionais ao nível de exposição identificado. Logo, a proteção de dados passa a ser identificada como elemento integrante da governança corporativa e da sustentabilidade organizacional.

A segurança da informação é um dos principais instrumentos para garantir a proteção dos dados pessoais e a conformidade com a LGPD. Apesar de estarmos falando de conceitos distintos, eles são complementares e interdependentes. Enquanto a proteção de dados está relacionada aos direitos dos titulares e à legitimidade do tratamento de dados pessoais, a segurança da informação fornece mecanismos necessários para a proteção desses dados contra acessos indevidos, perdas, alterações ou divulgações não autorizadas.

A relação entre privacidade e segurança da informação é amplamente reconhecida na literatura especializada. D'Avila e outros (2020) destacam que não é possível dissociar a proteção da privacidade dos mecanismos de segurança da informação, uma vez que a efetividade dos direitos assegurados pela legislação depende da adoção de medidas técnicas e administrativas capazes de proteger os dados pessoais durante todo o seu ciclo de vida. Dessa maneira, a segurança da informação constitui elemento essencial para a concretização dos princípios da prevenção, da segurança e da responsabilização previstos na LGPD.

Conforme a ABNT NBR ISO/IEC 27001:2022, a gestão da segurança da informação busca assegurar a confidencialidade, a integridade e a disponibilidade das informações, por meio da implementação de controles destinados à proteção dos ativos informacionais. Esses três princípios constituem a base da segurança da informação para a implementação de controles capazes de reduzir vulnerabilidades e mitigar ameaças que possam comprometer os dados pessoais tratados pelas organizações.

Conforme observam D'Avila e outros (2020), os princípios da confidencialidade, integridade e disponibilidade constituem os fundamentos da segurança da informação e orientam a implementação dos controles destinados à proteção dos ativos informacionais. A preservação

desses atributos contribui diretamente para a mitigação dos riscos relacionados ao tratamento de dados pessoais e para a conformidade com os requisitos da LGPD.

A importância da segurança da informação também é evidenciada pelo artigo 46 da LGPD (Brasil, 2018), que assim determina:

> os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito (Brasil, 2018).

Em razão disso, a segurança da informação representa um requisito essencial para a efetividade dos programas de privacidade e para a mitigação dos riscos associados ao tratamento de dados pessoais.

A efetividade da proteção de dados depende da capacidade das organizações de identificar riscos, avaliar seus impactos e implementar controles adequados para sua mitigação. Diante disso, a LGPD incorpora uma lógica de gestão baseada em riscos ao incentivar a adoção de mecanismos preventivos e medidas proporcionais à natureza e à sensibilidade dos dados tratados.

Sob a perspectiva da gestão de riscos, D'Avila e outros (2020) destacam que os incidentes envolvendo dados pessoais normalmente decorrem da exploração de vulnerabilidades por ameaças internas ou externas. Dessa forma, a realização de análises periódicas de riscos e vulnerabilidades permite identificar fragilidades existentes nos processos e sistemas organizacionais, subsidiando a implementação de controles preventivos e mitigatórios mais eficazes.

Complementando essa abordagem, Silva e outros (2020) destacam que a mitigação dos riscos relacionados ao tratamento de dados pessoais pode ser analisada a partir de três dimensões complementares: o potencial das ameaças, o grau de vulnerabilidade da organização e sua capacidade de resiliência diante de incidentes. Segundo os autores, a compreensão integrada desses elementos contribui para a definição de controles mais eficazes e para o fortalecimento da governança da privacidade.

Um dos principais instrumentos previstos na legislação é o Relatório de Impacto à Proteção de Dados Pessoais (RIPD), previsto no artigo 38 da LGPD (Brasil, 2018). O documento descreve as operações de tratamento realizadas, os dados coletados, as medidas de segurança adotadas e os mecanismos implementados para reduzir riscos aos direitos e liberdades dos titulares, contribuindo para a conformidade legal e a demonstração da responsabilidade organizacional (*accountability*).

D'Avila e outros (2020) ressaltam que o RIPDs deve ser utilizado como instrumento preventivo de identificação e mitigação de riscos relacionados à privacidade e à segurança da informação. Segundo os autores, a realização prévia dessa avaliação permite identificar vulnerabilidades, mensurar impactos potenciais e definir medidas de tratamento adequadas antes da execução das operações de tratamento de dados.

Essa abordagem está alinhada às boas práticas internacionais de gestão de riscos e privacidade, especialmente às diretrizes da ABNT NBR ISO/IEC 27701:2019, que orienta a implementação de controles específicos para gestão da privacidade da informação. Entre os principais controles aplicáveis destacam-se a classificação das informações, a gestão de acessos, a criptografia, o monitoramento de atividades, a gestão de terceiros, a realização de treinamentos e a implementação de planos de resposta a incidentes. A adoção desses mecanismos contribui para reduzir vulnerabilidades e aumentar a resiliência organizacional diante de ameaças relacionadas à privacidade e à proteção de dados.

A proteção de dados não depende exclusivamente de tecnologias ou controles formais. Sua efetividade está diretamente relacionada à existência de uma cultura organizacional orientada à ética, à segurança da informação e à proteção da privacidade. Nesse contexto, treinamentos, ações de conscientização, definição de responsabilidades, comunicação interna e comprometimento da alta administração tornam-se fatores essenciais para a consolidação de uma cultura de proteção de dados.

O artigo 50 da LGPD (Brasil, 2018) incentiva a implementação de programas de governança em privacidade que contemplem mecanismos de supervisão, políticas internas, gestão de riscos e melhoria contínua. Essa abordagem reforça a necessidade de integrar a proteção de dados à rotina organizacional e aos processos de tomada de decisão.

Nessa mesma linha, Silva e outros (2020) ressaltam que programas de conformidade em proteção de dados devem contemplar mecanismos voltados à redução das vulnerabilidades organizacionais, à proteção das infor-

mações tratadas e ao fortalecimento da capacidade de resposta da organização frente a incidentes de privacidade, contribuindo para o aumento da resiliência corporativa.

Assim, a integração entre proteção de dados, gestão de riscos, segurança da informação e governança corporativa fortalece a capacidade das organizações de prevenir incidentes, responder a eventos adversos e adaptar-se às constantes mudanças regulatórias e tecnológicas. Além disso, a adoção de práticas consistentes de privacidade contribui para o fortalecimento da confiança de clientes, investidores, parceiros comerciais e órgãos reguladores, transformando a proteção de dados em um diferencial competitivo e em um importante gerador de valor para o negócio.

1.3 Programas de privacidade como geradores de valor para o negócio

A LGPD estabelece, em seu artigo 1º, a proteção dos direitos fundamentais de liberdade, privacidade e livre desenvolvimento da personalidade da pessoa natural (Brasil, 2018). Desde a entrada em vigor da legislação, muitas organizações têm conduzido seus processos de adequação sob uma perspectiva predominantemente jurídica ou tecnológica, concentrando esforços no atendimento de requisitos legais, regulatórios e de segurança da informação.

Entretanto, essa abordagem, embora necessária, mostra-se insuficiente diante do potencial estratégico da proteção de dados. Programas de privacidade estruturados vão além da conformidade legal, contribuindo para a consolidação da reputação institucional, para a mitigação de riscos e para a construção de relações de confiança sustentáveis com clientes, colaboradores, fornecedores e demais partes interessadas.

O artigo 2º da LGPD estabelece, entre os fundamentos da proteção de dados pessoais, o desenvolvimento econômico e tecnológico, a inovação, a livre iniciativa e a defesa do consumidor (Brasil, 2018). Dessa forma, a própria legislação reconhece que a proteção da privacidade não constitui obstáculo ao crescimento econômico, mas elemento capaz de promover relações mais seguras, transparentes e sustentáveis no ambiente de negócios.

Organizações que incorporam a privacidade à sua estratégia corporativa tendem a obter benefícios relevantes. Entre eles, destaca-se o fortalecimento da confiança como diferencial competitivo, uma vez que consumidores e parceiros comerciais valorizam empresas que adotam práticas transparentes e responsáveis no tratamento de dados pessoais. Nesse contexto, o princípio da transparência, previsto no artigo 6º da LGPD, contribui para a ampliação da credibilidade institucional e para a consolidação da confiança dos titulares.

Outro benefício relevante refere-se à mitigação de riscos financeiros e reputacionais. Incidentes envolvendo dados pessoais podem resultar em sanções administrativas, ações judiciais, perda de credibilidade e impactos negativos à imagem institucional. Programas de privacidade adequadamente estruturados contribuem para reduzir essa exposição e fortalecer a capacidade de prevenção e resposta da organização.

A privacidade também pode favorecer o acesso a novos mercados e oportunidades comerciais. Cada vez mais, clientes corporativos, parceiros estratégicos e órgãos públicos exigem evidências de conformidade com requisitos de proteção de dados como condição para o estabelecimento de relações comerciais e contratuais.

Além dos benefícios relacionados à conformidade regulatória, programas de privacidade maduros podem contribuir para a redução da assimetria informacional entre organizações e partes interessadas. A demonstração de práticas transparentes, responsáveis e alinhadas aos princípios da proteção de dados fortalece a confiança institucional, favorece processos de *due diligence*, avaliação de fornecedores e parceiros comerciais, bem como amplia a credibilidade da organização perante investidores, clientes e órgãos reguladores. Nesse contexto, a privacidade passa a atuar como elemento de governança e integridade capaz de gerar vantagens competitivas sustentáveis.

Além disso, a aplicação dos princípios da LGPD pode promover ganhos de eficiência operacional. O princípio da necessidade, por exemplo, estimula a coleta e o tratamento apenas dos dados estritamente necessários para

determinada finalidade, contribuindo para a simplificação de processos, redução de custos de armazenamento e melhoria da gestão das informações.

Assim, a proteção de dados deve ser compreendida não apenas como um requisito regulatório, mas como um ativo estratégico capaz de gerar valor para o negócio, fortalecer a confiança das partes interessadas, apoiar a gestão de riscos, ampliar a maturidade organizacional e contribuir para a sustentabilidade e competitividade das organizações no longo prazo.

1.4 Boas práticas para implementação da privacidade no cotidiano das organizações

A consolidação de uma cultura de proteção de dados exige a adoção de práticas que integrem a privacidade às atividades rotineiras da organização. Independentemente do porte ou segmento de atuação, determinadas iniciativas podem contribuir significativamente para a construção de programas de privacidade efetivos e sustentáveis.

Uma das etapas fundamentais consiste na realização do mapeamento de dados e do inventário das operações de tratamento. Conhecer quais dados pessoais são tratados, as respectivas finalidades e bases legais, os períodos de retenção e os responsáveis pelo acesso constitui requisito essencial para a implementação de controles adequados. Esse processo está diretamente relacionado ao princípio da responsabilização e prestação de contas previsto no artigo 6° da LGPD e representa o alicerce de qualquer programa de privacidade.

De forma complementar, Silva e outros (2020) destacam que a redução dos riscos relacionados ao tratamento de dados passa pelo conhecimento dos fluxos de dados pessoais, pela minimização da coleta de informações, pela adoção de controles de segurança da informação, pela transparência no tratamento realizado e pela adequada gestão dos terceiros envolvidos nas operações de tratamento.

Outro elemento relevante é a designação do Encarregado pelo Tratamento de Dados Pessoais (DPO). Conforme previsto no artigo 5°, inciso VIII, da LGPD (Brasil, 2018), esse profissional atua como canal de comunicação entre a organização, os titulares dos dados e a Agência Nacional de Proteção de Dados. Além do atendimento às exigências legais e regulatórias, o encarregado desempenha papel estratégico na orientação das áreas internas, na disseminação da cultura de privacidade e no acompanhamento dos riscos relacionados ao tratamento de dados pessoais.

A capacitação contínua dos colaboradores também representa fator crítico para a efetividade das iniciativas de proteção de dados. Grande parte dos incidentes de segurança decorre de falhas humanas, tornando indispensáveis ações permanentes de treinamento e conscientização. Nesse sentido, o princípio da prevenção reforça a necessidade de adoção de medidas destinadas a evitar a ocorrência de danos antes que eles se materializem.

Adicionalmente, a área de Tecnologia da Informação desempenha papel fundamental na implementação e sustentação dos controles de privacidade. A incorporação dos conceitos de Privacy by Design e Privacy by Default permite que requisitos de proteção de dados sejam considerados desde a concepção de produtos, serviços e processos, reduzindo riscos, custos de adequação e retrabalho.

Da mesma forma, a existência de procedimentos estruturados para resposta a incidentes fortalece a capacidade organizacional de atuar diante de eventos que possam comprometer dados pessoais. Conforme previsto no artigo 48 da LGPD (Brasil, 2018), incidentes que possam acarretar risco ou dano relevante aos titulares devem ser comunicados à Autoridade Nacional de Proteção de Dados e, quando aplicável, aos próprios titulares afetados. Organizações que possuem planos de resposta previamente definidos tendem a responder com maior agilidade e efetividade, reduzindo impactos e fortalecendo sua governança.

A maturidade em privacidade pode ser compreendida como o grau de institucionalização das práticas de proteção de dados na organização. Em níveis iniciais, predominam ações voltadas ao atendimento de requisitos legais, à correção de não conformidades e à implementação de controles básicos de proteção de dados. À medida que a organização evolui, a privacidade passa a

integrar processos, controles internos, gestão de riscos e mecanismos de governança. Nos níveis mais avançados, a proteção de dados torna-se parte da cultura organizacional e da estratégia corporativa, orientando decisões de negócio e promovendo melhoria contínua.

Dessa forma, programas de privacidade sustentáveis não devem ser compreendidos como projetos pontuais, mas como processos contínuos de aprimoramento. Organizações que alcançam esse estágio transformam a conformidade regulatória em maturidade organizacional, fortalecem sua governança, reduzem sua exposição a riscos, ampliam a confiança das partes interessadas e potencializam sua capacidade de geração de valor no longo prazo.

Conclusão

A transformação digital ampliou significativamente a relevância dos dados pessoais para as organizações, tornando sua proteção um elemento indispensável para a sustentabilidade dos negócios e para a manutenção da confiança das partes interessadas. Nesse contexto, o presente artigo buscou responder ao seguinte problema de pesquisa: como as organizações podem transformar a adequação à LGPD em um modelo de maturidade, gestão de riscos e geração de valor para o negócio?

A análise realizada demonstrou que a LGPD ultrapassa a condição de mero instrumento regulatório, consolidando-se como importante mecanismo de governança corporativa. Ao estabelecer princípios, responsabilidades e diretrizes para o tratamento de dados pessoais, a legislação incentiva a adoção de práticas estruturadas de gestão, controle, supervisão e prestação de contas, fortalecendo a transparência, a integridade e a responsabilização organizacional.

Também foi possível verificar que a proteção de dados está diretamente relacionada à gestão de riscos e à segurança da informação. A identificação de ameaças e vulnerabilidades, a implementação de controles preventivos, a adoção de medidas de segurança e o monitoramento contínuo dos processos contribuem para a mitigação de riscos regulatórios, operacionais, financeiros e reputacionais. Dessa forma, a privacidade deixa de ser uma preocupação restrita às áreas jurídica e tecnológica e passa a integrar a estratégia corporativa e os mecanismos de gestão organizacional.

Além disso, constatou-se que programas de privacidade estruturados podem gerar valor para o negócio ao fortalecer a confiança de clientes, colaboradores, parceiros, investidores e demais partes interessadas, melhorar a eficiência operacional, ampliar oportunidades comerciais e contribuir para a construção de uma reputação institucional sólida. Da mesma forma, a adoção de práticas como o mapeamento de dados, a capacitação contínua dos colaboradores, a atuação do Encarregado pelo Tratamento de Dados Pessoais, a incorporação dos princípios de Privacy by Design e a gestão estruturada de incidentes demonstram que a proteção de dados pode ser incorporada de forma efetiva à rotina das organizações.

Nesse processo, a maturidade organizacional em privacidade surge como elemento central. Organizações em estágios iniciais tendem a concentrar seus esforços no atendimento aos requisitos legais mínimos e na implementação de controles básicos. À medida que evoluem, passam a integrar a proteção de dados à gestão de riscos, à governança corporativa, aos programas de compliance e aos processos decisórios. Nos níveis mais avançados de maturidade, a privacidade torna-se parte da cultura organizacional e da estratégia empresarial, contribuindo para a geração sustentável de valor, para o fortalecimento da confiança das partes interessadas e para o aumento da resiliência organizacional.

Conclui-se, portanto, que a LGPD representa uma oportunidade para que as organizações desenvolvam modelos de gestão mais responsáveis, resilientes e alinhados às exigências da economia digital. Mais do que atender a uma obrigação legal, investir em governança, gestão de riscos, segurança da informação e cultura de privacidade constitui um caminho para o fortalecimento da competitividade, da reputação e da sustentabilidade dos negócios no longo prazo.

Sob essa perspectiva, a proteção de dados deixa de representar exclusivamente um mecanismo de conformidade regulatória e passa a constituir um ativo estratégico capaz de fortalecer a governança corporativa, aumentar a confiança das partes interessadas, apoiar a tomada de decisões e gerar vantagens competitivas

sustentáveis em ambientes de negócios cada vez mais orientados por dados.

Como limitação deste estudo, destaca-se o fato de ter sido desenvolvido com base em pesquisa bibliográfica e documental, não contemplando estudos de caso ou análises empíricas sobre a maturidade em privacidade nas organizações. Nesse sentido, pesquisas futuras poderão aprofundar a avaliação prática dos impactos da LGPD na governança corporativa, na gestão de riscos, nos programas de compliance e na geração de valor em diferentes setores econômicos.

Referências

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). ABNT NBR ISO 31000:2018. *Gestão de riscos — Diretrizes*. Rio de Janeiro: ABNT, 2018.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). ABNT NBR ISO/IEC 27001:2022. *Segurança da informação, cibersegurança e proteção da privacidade — Sistemas de gestão da segurança da informação — Requisitos*. Rio de Janeiro: ABNT, 2022.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). ABNT NBR ISO/IEC 27701:2026. *Segurança da informação, segurança cibernética e proteção da privacidade — Sistemas de gestão da privacidade da informação — Requisitos e orientações*. Rio de Janeiro: ABNT, 2026.

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: 20 out. 2026.

D'AVILA, Ana Vitória Germani; SILVA, Bruna Fabiane da; ARAÚJO, Thiago Volpi de; DESERV TECNOLOGIA E SERVIÇOS. *LGPD:* muito além da lei: uma análise do direito em conjunto com a segurança da informação. Curitiba: DeServ Tecnologia e Serviços, 2020.

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA (IBGC). *Código das melhores práticas de governança corporativa*. 6. ed. São Paulo: IBGC, 2023.

PINHEIRO, Patrícia Peck. *Proteção de dados pessoais:* comentários à Lei n. 13.709/2018 (LGPD). 4. ed. São Paulo: Saraiva Jur, 2024.

SILVA, Marcelo; RASINI, Carlos A.; COELHO, Frederico A.; MORAES, Ricardo C. *Guia para o Programa de Conformidade LGPD*. São Paulo: GL BA Brasil, 2020.

O Encarregado de Dados (Data Protection Officer – DPO) como vetor de efetividade na LGPD

Dos fundamentos constitucionais às diretrizes da resolução ANPD nº 18/2024: a atuação multidisciplinar do DPO e o cenário real de maturidade no mercado brasileiro

Giovana Cunha Queiroz Araújo

Giovana Cunha Queiroz Araújo é formada em Direito pela Universidade Federal Fluminense (UFF), com atuação nas áreas de Direito do Trabalho e Proteção de Dados Pessoais. Atualmente exerce a função de Encarregada pelo Tratamento de Dados Pessoais (Data Protection Officer – DPO), atuando em temas relacionados à privacidade, governança de dados e conformidade regulatória, incluindo a adequação à Lei Geral de Proteção de Dados (LGPD). Possui experiência na interface entre as áreas jurídica, de recursos humanos e compliance, com foco na implementação de soluções práticas para gestão de riscos, comunicação estratégica e promoção da cultura de proteção de dados. Também participa de iniciativas institucionais, integrando o Comitê Jovem do Instituto Brasileiro de Petróleo e Gás (IBP) e a Câmara de Governança da Firjan.

Introdução

A ascensão da sociedade da informação transformou os dados pessoais em ativos de valor central para a economia global, mas também evidenciou a fragilidade da privacidade individual diante do processamento massivo de informações. No Brasil, esse cenário impulsionou a promulgação da Lei Geral de Proteção de Dados (Lei nº 13.709/2018 – LGPD), marco regulatório que não apenas estabeleceu regras para o tratamento, mas consolidou uma nova estrutura de governança no país. A relevância do tema alcançou elevado grau de relevância jurídica com a Emenda Constitucional nº 115/2022, que elevou a proteção de dados pessoais à categoria de direito fundamental.

No cerne dessa estrutura, a LGPD introduziu a figura do Encarregado pelo Tratamento de Dados Pessoais. No Brasil, utiliza-se a nomenclatura "encarregado" de forma semelhante àquela utilizada na tradução oficial do texto do General Data Protection Regulation (GDPR) para o português, cuja denominação no original, em inglês, é Data Protection Officer (DPO). O termo DPO tem sido utilizado, frequentemente, para se referir ao Encarregado pelo Tratamento de Dados Pessoais previsto na LGPD (ANPD, 2024). Designado pelo artigo 41 da referida lei, o Encarregado atua como o elo estratégico entre os três polos do sistema: o agente de tratamento (Controlador), o titular dos dados e a Agência Nacional de Proteção de Dados (ANPD).

Todavia, a implementação prática dessa função no Brasil revela um distanciamento entre a simplicidade do texto legal e a complexidade das exigências técnicas. Enquanto a lei original se manteve sucinta quanto aos requisitos para o exercício do cargo, a recente Resolução CD/ANPD nº 18/2024 e o Guia Orientativo da ANPD de 2024 trouxeram novos contornos para essa figura. A presente pesquisa busca analisar esse enquadramento regulatório, focando na transição de uma designação meramente formal para uma exigência de eficácia material baseada em campos específicos de conhecimento.

Em segundo lugar, verifica-se que o Brasil se encontra em um estágio fundamental de transição e amadurecimento cultural. Em contraste com a União Europeia, onde a proteção de dados já é intrínseca à estratégia de negócios e ao cotidiano institucional, o cenário nacional ainda enfrenta o desafio de transcender uma postura puramente reativa e formalista. Nesse contexto, o profissional que atua na área assume o papel de catalisador dessa mudança, empenhando-se em consolidar a proteção de dados como um pilar de governança estratégica, superando a percepção limitada de que a conformidade se restringe a um mero rito burocrático.

A pesquisa justifica-se pela necessidade de diagnosticar como o mercado tem suprido a ausência de balizas legais quanto ao perfil do Encarregado. Com esse propósito, o trabalho utiliza o método dedutivo e exploratório, fundamentado em técnica de pesquisa bibliográfica e documental, incluindo a comparação pontual entre as disposições sobre o DPO na LGPD e na Resolução nº 18/2024 da ANPD com o modelo estabelecido pelo Regulamento Europeu (General Data Protection Regulation – GDPR) e as diretrizes do European Data Protection Board (EDPB)[1].

[1] European Data Protection Board (EDPB), ou Comitê Europeu para a Proteção de Dados, é um órgão europeu independente, com personalidade jurídica, instituído pelo Regulamento Geral sobre a Proteção de Dados (GDPR). É composto pelos chefes das autoridades de controle de cada Estado-membro da União Europeia e pelo Supervisor Europeu para a Proteção de Dados (EDPS). Sua função primordial é garantir a aplicação coerente do GDPR em toda a União Europeia por meio da emissão de diretrizes (guidelines), recomendações, pareceres e a resolução de conflitos entre autoridades nacionais, servindo como a principal referência interpretativa para a governança de dados em nível global. (em tradução livre) Disponível em: https://www.edpb.europa.eu/about-edpb/who-we-are/european-data-protection-board_en. Consulta em: 27 mai. 2026.

O método exploratório ganha contornos por meio da análise de dados recentes do relatório "Perfil DPO Brasil 2025"[2], que investiga as particularidades da atuação desse profissional, explorando os obstáculos enfrentados, as melhores práticas adotadas e o impacto de sua atuação. Estruturalmente, este artigo divide-se em três seções principais, além desta introdução e das considerações finais. Inicialmente, apresenta-se a fundamentação teórica e histórica, abordando a transição do conceito clássico de privacidade para o direito à proteção de dados, sua elevação a garantia fundamental pela EC nº 115/2022 e a arquitetura da LGPD. A seção seguinte constitui o núcleo crítico e analítico do estudo, no qual se confronta a matriz europeia do GDPR com o modelo regulatório brasileiro, delimitando as balizas normativas e operacionais introduzidas pela Resolução CD/ANPD nº 18/2024. Por fim, explora-se a dimensão empírica e pragmática do ecossistema nacional, investigando os desafios reais de implementação da função no mercado a partir de dados consolidados de maturidade corporativa.

1. Os fundamentos da proteção de dados: da evolução histórica à garantia constitucional

Historicamente, a privacidade foi concebida no final do século XIX com a formulação do *right to be let alone* (o direito de ser deixado só) por Samuel Warren e Louis Brandeis. Em artigo pioneiro publicado em 1890, os juristas norte-americanos fundamentaram o direito à privacidade como uma resposta à intrusão da imprensa e às inovações tecnológicas da época (Warren; Brandeis, 1890, p. 195-196). No entanto, com o advento da "Sociedade da Informação"[3] e a onipresença da coleta de dados, essa visão de "isolamento" tornou-se insuficiente.

Nesse contexto, Stefano Rodotà, jurista italiano e um dos maiores teóricos mundiais sobre o tema, propõe a superação da ideia de privacidade como isolamento, defendendo sua vinculação à dignidade e à construção da identidade da pessoa humana em um mundo dataficado (Rodotá, 2008).

No Brasil, Danilo Doneda, jurista e pesquisador brasileiro, se tornou a principal referência no país ao conectar o pensamento de Rodotà à evolução do Direito Civil nacional. Doneda consolida essa perspectiva ao destacar que, enquanto a privacidade clássica buscava "esconder" o dado, a proteção de dados busca conferir ao titular o poder de controle sobre o seu fluxo (Doneda, 2019). Dessa forma, a proteção de dados emerge como um direito de natureza ativa e participativa, essencial para o exercício da cidadania plena e para a garantia da liberdade individual em todas as esferas da vida social.

Nesse cenário, o DPO (Encarregado) assume papel estratégico ao viabilizar, na prática, o exercício desse controle. Mais que uma função administrativa, o DPO viabiliza os princípios de governança e prestação de contas *(accountability)*, os quais serão apresentados mais adiante, traduzindo a proteção de dados em conformidade efetiva e contribuindo para o amadurecimento do direito no Brasil

[2] Dados extraídos da pesquisa empírica inédita intitulada 'Perfil DPO Brasil 2025', elaborada conjuntamente pelo escritório Opice Blum e pela Rede Líderes. O estudo quantitativo foi conduzido entre os meses de junho e agosto de 2025 e contou com uma amostra qualificada de 203 profissionais que atuam como Encarregados pelo Tratamento de Dados Pessoais (DPOs) em organizações de diversos setores e portes no cenário brasileiro. Disponível em: https://www.opiceblum.com.br/relatorio-perfil-dpo-brasil/. Consulta em: 30 mai. 2026.

[3] O conceito de sociedade da informação refere-se à configuração social surgida a partir da Terceira Revolução Industrial, na qual a informação e as tecnologias da informação e comunicação (TICs) assumem papel central nas relações econômicas, sociais e culturais. Segundo Santos e Carvalho (2009), a sociedade da informação caracteriza-se pela crescente relevância da informação como recurso estratégico e elemento fundamental para o desenvolvimento e exercício da cidadania.

1.1 A proteção de dados como direito fundamental

A promulgação da Emenda Constitucional nº 115, em 10 de fevereiro de 2022, representa o ápice do processo de amadurecimento jurídico do tema no Brasil. Ao alterar a Constituição Federal para incluir a proteção de dados pessoais no rol dos direitos e garantias fundamentais (artigo 5º, inciso LXXIX), o constituinte derivado não apenas conferiu maior robustez à LGPD, mas consolidou a proteção de dados como uma cláusula pétrea e central ao Estado Democrático de Direito.

A Emenda também definiu a competência privativa da União para legislar sobre o tema, promovendo uniformidade normativa e segurança jurídica. A Emenda atribuiu à União a competência para organizar e fiscalizar a proteção de dados (artigo 21, inciso XXVI) e promoveu o fortalecimento institucional da ANPD (Lei nº 14.460/2022), a qual passou a atuar como autarquia de natureza especial, dotada de autonomia técnica e administrativa. Tal centralização contribui para a uniformização de diretrizes no âmbito nacional, conferindo maior previsibilidade e segurança jurídica à governança de dados, bem como orientando a atuação do DPO.

Para o DPO, a elevação constitucional redefine a natureza de sua função, que deixa de se limitar à gestão de conformidade para assumir a posição de garantidor prático de um direito fundamental. Tal responsabilidade exige atuação técnica e eticamente independente, conferindo-lhe o papel de assegurar a conformidade constitucional no âmbito organizacional. Sua atuação, portanto, transcende a dimensão operacional, orientando-se pela proteção da dignidade do titular como eixo central das atividades de tratamento de dados.

1.2 A arquitetura da Lei Geral de Proteção de Dados (LGPD)

A Lei Geral de Proteção de Dados (Lei nº 13.709/2018) estabelece um modelo normativo baseado em deveres de diligência e transparência, exigindo conformidade contínua e demonstrável. Sua estrutura organiza-se a partir da definição dos agentes de tratamento e de um conjunto normativo integrado de princípios e governança, que orientam e operacionalizam as atividades de tratamento de dados.

1.2.1 Os agentes de tratamento

A LGPD define uma cadeia de responsabilidades ao estabelecer os agentes de tratamento (artigo 5º, IX). A compreensão precisa desses papéis revela-se essencial, na medida em que a LGPD atribui obrigações específicas e regimes próprios de responsabilidade civil a cada agente envolvido.

O Controlador, responsável pelas decisões sobre o tratamento (artigo 5º, VI), assume papel central, cabendo-lhe definir finalidades, adotar medidas de segurança e implementar instrumentos de conformidade, como o Registro de Operações (RoPA) e, quando aplicável, o Relatório de Impacto (RIPD). No que tange ao regime de responsabilidade, a LGPD estabelece, em seu artigo 42[4], que o Controlador responde pelos danos causados pelo exercício da atividade de tratamento de dados pessoais. No entanto, o legislador previu hipóteses taxativas de exclusão de responsabilidade no artigo 43[5], visando assegurar que o dever de reparar não se torne um ônus

[4] BRASIL. Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais). Art. 42. "O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo."

[5] BRASIL. Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais). Art. 43. "Os agentes de tratamento só não serão responsabilizados quando provarem: I - que não realizaram o tratamento de dados pessoais que lhes é atribuído; II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro."

desarrazoado para o agente que atua com diligência.

O Operador, por sua vez, surge como o agente de execução técnica e atua sob as instruções do Controlador (artigo 5º, VII), sem autonomia decisória. Ainda assim, deve adotar práticas de governança e pode responder solidariamente caso descumpra a legislação ou as instruções recebidas.

Cumpre destacar a figura do DPO, que, embora não integre a categoria dos agentes de tratamento, desempenha função estratégica ao atuar como instância de interlocução entre a organização, os titulares de dados e a ANPD. O exercício de suas atribuições não implica a transferência de responsabilidade pela conformidade das operações de tratamento, a qual permanece vinculada ao controlador. Todavia, admite-se a responsabilização pessoal do DPO, com fundamento no direito civil, caso sua atuação configure conduta ilícita apta a ensejar danos, nos termos dos artigos 186[6], 187[7] e 927[8] do Código Civil. Considerando a centralidade dessa figura no sistema de proteção de dados, sua atuação será objeto de análise mais aprofundada em seção própria.

1.2.2 Princípios e governança de dados

Os princípios previstos no artigo 6º da LGPD constituem requisitos obrigatórios para a validade do tratamento de dados pessoais, orientando toda a atividade por parâmetros como finalidade, adequação e necessidade, que limitam o uso das informações ao estritamente necessário. Soma-se a esses princípios a transparência, o livre acesso e a qualidade dos dados, que asseguram ao titular o controle sobre suas informações, bem como a segurança, a prevenção e a vedação a práticas discriminatórias. Nesse contexto, destaca-se o princípio da responsabilização e prestação de contas (*accountability*), que impõe aos agentes o dever não apenas de cumprir a legislação, mas de demonstrar, de forma efetiva, a conformidade de suas atividades.

A operacionalização desses princípios ocorre por meio da governança de dados. No cenário corporativo, é comum a confusão entre os termos "governança" e "compliance", mas, embora correlacionados, eles possuem naturezas distintas. Em termos simples, a **governança** refere-se ao sistema de direção e controle das organizações - o "*autover*" estratégico. Já o **compliance** (do inglês, *to comply*) é o dever de estar em conformidade com leis e regulamentos - o "obedecer" operacional.

No contexto desta pesquisa, a Governança de Dados não deve ser reduzida ao cumprimento burocrático de uma lista de verificação (*checklist),* ela representa a espinha dorsal sobre a qual se sustenta a proteção de dados. Como ensina Carlos Barbieri:

> De forma bem simplificada, a governança de dados é um conjunto de práticas, dispostas em um *framework*, com o objetivo de organizar o uso e o controle adequado dos dados como um ativo organizacional. Seria, por assim dizer, uma forma de pôr ordem na casa com relação aos aspectos de dados, visando disponibilidade, integridade, consistência, usabilidade, segurança, controle, etc. (Barbieri, 2019, p. 62).

Assim, princípios e governança se articulam de forma indissociável: enquanto os primeiros estabelecem o norte normativo, a segunda assegura sua efetividade na prática. Nesse cenário, o DPO desempenha papel central ao viabilizar essa articulação e promover a conformidade contínua.

Dessa forma, provida a arquitetura geral da LGPD – contemplando a definição dos agentes, a aplicação dos princípios e, primordialmente, a estruturação da governança como motor de conformidade –, o capítulo seguinte se dedicará à investigação da atuação do DPO no cenário brasileiro.

[6] BRASIL. Lei nº 10.406, de 10 de janeiro de 2002 (Código Civil) . Art. 186. "Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito."

[7] BRASIL. Lei nº 10.406, de 10 de janeiro de 2002 (Código Civil) . Art. 187. "Também comete ato ilícito o titular de um direito que, ao exercê-lo, excede manifestamente os limites impostos pelo seu fim econômico ou social, pela boa-fé ou pelos bons costumes."

[8] BRASIL. Lei nº 10.406, de 10 de janeiro de 2002 (Código Civil). Art. 927. "Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo."

2. O DPO na estrutura de governança: da matriz europeia às exigências da ANPD

A compreensão da figura do DPO no Brasil exige um olhar sobre sua gênese no Direito Europeu. O DPO não constitui uma criação autônoma da LGPD, mas a transposição de um modelo oriundo da GDPR. A partir dessa matriz, torna-se possível examinar sua configuração no ordenamento brasileiro, bem como as tensões entre previsão normativa, prática de mercado e desafios de efetividade que marcam sua atuação no país.

2.1 A matriz europeia (GDPR) e o paradigma do mapa de competências funcionais

No ordenamento europeu, o DPO é concebido como uma figura central na estrutura de governança em proteção de dados. O General Data Protection Regulation (GDPR) dedica artigos específicos[9] para delinear as hipóteses de nomeação, as garantias institucionais e as tarefas fundamentais deste agente. Desde o seu surgimento, o legislador europeu adotou uma postura pragmática: o Regulamento Europeu optou por não condicionar o exercício da função a um título acadêmico específico, graduação ou inscrição em conselho profissional. Conferiu-se, com isso, total discricionariedade para que o Controlador escolhesse o perfil profissional mais alinhado à sua realidade operacional e ao seu modelo de negócio.

Entretanto, essa liberdade de escolha nunca significou amadorismo ou falta de critérios. O artigo 37(5)[10] do GDPR estabelece que o DPO deve ser designado com base em suas qualidades profissionais e, de forma especial, em seus conhecimentos especializados no domínio do direito e das práticas de proteção de dados. Complementarmente, o Recital 97[11] do Regulamento dispõe que o nível necessário de conhecimento especializado deve ser determinado de acordo com a sensibilidade, a complexidade e o volume das operações de tratamento de dados realizadas pela organização. Conforme as orientações históricas do Working Party Article 29 (2017)[12], esse nível de *expertise* é guiado por três dimensões norteadoras:

- **Conhecimento Proporcional ao Risco:** O subsídio europeu determina que o nível de conhecimento deve ser aferido de acordo com as operações de tratamento realizadas. Conforme as orientações do órgão europeu:

  > O nível de especialização exigido não é estritamente definido, mas deve ser proporcional à sensibilidade, complexidade e quantidade de dados que uma organização processa. Por exemplo, quando uma atividade de tratamento de dados é particularmente complexa, ou quando envolve uma grande quantidade de dados sensíveis, o DPO pode necessitar de um nível mais elevado de conhecimento especializado e apoio (WP29, 2017, em tradução livre).

- **Multidisciplinaridade:** Embora não exija um diploma, o Regulamento exige que o DPO tenha capacidade para cumprir as tarefas do artigo 39. Isso inclui entender de sistemas de informação, segurança de dados

[9] Art. 37 - *Designation of the data protection officer; Art 38 - Position of the data protection officer.; Art. 39 - Tasks of the data protection office.*

[10] Art. 37 - *Designation of the data protection officer. […] 5. The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39;"*

[11] Os Recitais são textos introdutórios que acompanham os regulamentos da União Europeia. Eles servem para explicar as razões de cada dispositivo e fornecer orientações interpretativas valiosas sobre o espírito e a intenção do legislador.

[12] O Working Party Article 29 (Grupo de Trabalho do Artigo 29) foi um órgão consultivo europeu independente, composto por representantes das autoridades de proteção de dados de todos os Estados-Membros da União Europeia e instituído pela Diretiva 95/46/CE. Com a entrada em vigor do GDPR em 2018, o WP29 foi sucedido pelo European Data Protection Board (EDPB). Suas diretrizes (*guidelines*) e pareceres permanecem como a principal fonte de interpretação técnica e doutrinária para os institutos da proteção de dados, tendo sido oficialmente endossados pelo EDPB para garantir a continuidade da segurança jurídica no bloco europeu.

e ter uma compreensão profunda da organização do controlador. O WP29 esclarece que é elemento relevante que o profissional possua conhecimento das leis e práticas nacionais e europeias de proteção de dados e uma compreensão aprofundada do GDPR.

- **Habilidade de cumprir tarefas:** A capacidade de cumprir as tarefas incumbidas ao DPO deve ser interpretada tanto em referência às suas qualidades pessoais e aos seus conhecimentos, quanto à sua posição dentro da organização. As qualidades pessoais devem incluir, por exemplo, integridade e elevada ética profissional, sendo a preocupação primária do DPO permitir a conformidade com o Regulamento. O DPO desempenha um papel fundamental na promoção de uma cultura de proteção de dados e auxilia na implementação de elementos essenciais, como os princípios de tratamento, direitos dos titulares, a proteção de dados desde a conceção (*privacy by design*) e por padrão (*by default*)[13], registros de operações de tratamento (RoPA) e segurança do tratamento.

Essa abordagem baseada em competências demonstra que a ausência de um diploma específico não significa ausência de rigor. Pelo contrário, ela transfere para a organização a responsabilidade de mapear e selecionar uma bagagem técnica híbrida capaz de garantir a eficácia do programa de privacidade. No contexto brasileiro, contudo, a assimilação desse modelo percorreu trajetórias distintas até alcançar certo grau de estabilização, refletindo os movimentos legislativos que acompanharam sua evolução na prática de mercado atual.

2.2 A trajetória brasileira: do veto à resolução CD/ANPD nº 18/2024

Diferente da matriz europeia, que fornece subsídios mais robustos para a escolha do DPO, a Lei Geral de Proteção de Dados (LGPD) apresenta um cenário de maior abertura normativa, o que pode ser interpretado como uma lacuna regulatória. A legislação brasileira dedica uma seção específica para tratar do Encarregado pelo Tratamento de Dados Pessoais, concentrada primordialmente no artigo 41. No entanto, o perfil técnico desse agente foi alvo de um debate legislativo que culminou em uma omissão deliberada. A redação original, alterada pela Medida Provisória nº 869/2018, buscava estabelecer requisitos mínimos de qualificação para garantir a eficácia da norma. Contudo, ao sancionar a conversão na Lei nº 13.853/2019, a Presidência da República vetou o § 4º do artigo 41, que estabelecia tais diretrizes. A justificativa oficial para o veto sustentou que tal exigência constituiria um rigor excessivo, configurando uma interferência desnecessária do Estado na seleção de quadros do setor produtivo e uma violação ao livre exercício profissional garantido pela Constituição. Sob a ótica da Análise Econômica do Direito[14], o argumento possuía lógica: visava reduzir custos de transação para as empresas e evitar reservas de mercado.

Nesse contexto, considerando que a LGPD foi introduzida em um ambiente ainda marcado por baixa maturidade em proteção de dados, a supressão de critérios mínimos de qualificação para o DPO produziu efeitos que transcendem a mera flexibilidade regulatória. A ausência de parâmetros técnicos pode ter contribuído para uma variação significativa na forma de estruturação e exercício

[13] Os conceitos de *Privacy by Design* (proteção de dados desde a concepção) e *Privacy by Default* (proteção de dados por padrão) correspondem à obrigação de incorporar medidas técnicas e organizacionais de proteção de dados desde as fases iniciais de desenvolvimento de sistemas, produtos e processos, bem como de assegurar que as configurações padrão adotem o mais elevado nível de proteção à privacidade, limitando o tratamento de dados ao estritamente necessário para cada finalidade específica (*European Data Protection Board*, 2026, em tradução livre).

[14] A Análise Econômica do Direito (AED) consiste na aplicação de ferramentas da teoria econômica à interpretação e avaliação das leis, instituições legais e políticas públicas, buscando compreender seus impactos sobre o comportamento dos agentes e sobre o bem-estar social. Fundamentada nas contribuições de autores como Coase (1960), Posner (2007) e Cooter e Ulen (2010), essa abordagem parte da premissa de que os indivíduos tomam decisões com base na análise de custos e benefícios, permitindo avaliar a eficiência das normas, especialmente por meio de critérios como a maximização do bem-estar e a análise de custo-benefício.

da função, dificultando não apenas a orientação das organizações quanto à escolha de perfis adequados, mas também a construção de práticas internas consistentes. Como resultado, a temática pode ser apreendida pelos colaboradores de forma superficial, dissociada de sua dimensão estruturante, o que retarda a assimilação de padrões mais qualificados de governança informacional. Esse cenário permaneceu como um desafio até publicação da Resolução CD/ANPD nº 18/2024, que representa uma tentativa de preencher esse vácuo e equilibrar a liberdade de seleção.

Nesse sentido, a norma procurou conferir maior densidade jurídica à função, detalhando regras explícitas sobre o rito de indicação, a obrigatoriedade de atos formais e as garantias de autonomia técnica. Complementando o arcabouço, em 19 de dezembro de 2024, a ANPD publicou o seu "Guia Orientativo sobre a Atuação do Encarregado" consolidando o entendimento de que a eficácia da lei depende de uma confluência multidisciplinar de saberes:

> Em relação à capacidade técnica necessária para o desempenho das atribuições de encarregado, além do conhecimento sobre a legislação de proteção de dados pessoais, e sobre as normas e demais publicações da ANPD, conhecimentos multidisciplinares sobre gestão de riscos, gestão de dados e governança, compliance e auditoria, e segurança da informação podem ser de grande valia para o exercício de suas atividades (ANPD, 2024).

Sob essa ótica, o ponto central da questão deixa de ser a exigência de um diploma de graduação específico – até porque a própria norma requer conhecimentos que, na estrutura acadêmica tradicional, estariam fragmentados em diferentes cursos superiores. O que se impõe, na realidade, é a necessidade de uma bagagem técnica que melhor atenda à complexidade do setor de atuação do controlador.

Diante da necessidade de alinhar a bagagem técnica do DPO à complexidade de cada modelo de negócio, a governança de privacidade exige a tradução de comandos normativos em parâmetros corporativos concretos. A transição dessa multidisciplinaridade para o cotidiano das organizações demanda a estruturação de salvaguardas institucionais explícitas, capazes de garantir a eficácia do programa de dados e mitigar riscos de conformidade. Para orientar essa transposição prática, a subseção a seguir aborda, de forma detalhada e integrada, dimensões regulatórias essenciais fixadas pela ANPD, delineando os critérios de elegibilidade, as exigências formais de nomeação, as dinâmicas de transparência e a gestão de conflitos de interesse que devem guiar a atuação desse agente estratégico.

2.3 Diretrizes regulatórias e operacionais para a estruturação da função do Encarregado de Dados

A publicação da Resolução CD/ANPD nº 18/2024 e o subsequente Guia Orientativo da ANPD removeram o caráter abstrato que cercava a função do Encarregado de Dados (DPO) no Brasil. Para as organizações do mercado geral, a governança de privacidade passou a exigir o cumprimento de ritos formais e salvaguardas institucionais explícitas. A seguir, analisa-se detalhadamente o ecossistema de obrigações e parâmetros práticos que devem nortear os agentes de tratamento em eixos estratégicos fundamentais.

2.3.1 Nomeação e divulgação das informações do Encarregado

No ordenamento jurídico estabelecido pela LGPD, a indicação do Encarregado está prevista no artigo 41 como uma obrigação atribuída, em regra, ao controlador. A função pode ser exercida tanto por pessoa natural, vinculada ou não ao quadro de empregados da organização, quanto por pessoa jurídica especializada na prestação de serviços de proteção de dados, modelo amplamente conhecido como "*DPO as a Service*".

A única exceção à obrigatoriedade de indicação pelo controlador decorre de critérios de proporcionalidade previstos na Resolução CD/ANPD nº 2/2022, que flexibilizou a exigência para os chamados Agentes de Tratamento de Pequeno Porte. Contudo, conforme a ANPD, não é todo e qualquer agente de tratamento de pequeno porte que está desobrigado de indicar Encarregado, permanecendo tal dever àqueles que (i)

realizem tratamento de alto risco; (ii) aufiram, em cada ano-calendário, receita bruta superior a R$ 360.000,00 (trezentos e sessenta mil reais) e igual ou inferior a R$ 4.800.000,00 (quatro milhões e oitocentos mil reais) ou, no caso de *startups*, com receita bruta de até R$ 16.000.000,00 (dezesseis milhões de reais) no ano-calendário anterior ou de R$ 1.333.334,00 (um milhão, trezentos e trinta e três mil trezentos e trinta e quatro reais) multiplicado pelo número de meses de atividade no ano-calendário anterior, quando inferior a 12 (doze) meses, independentemente da forma societária adotada; ou (iii) pertençam a grupo econômico de fato ou de direito, cuja receita global ultrapasse tais limites (ANPD, 2024).

Para os controladores de médio e grande porte do mercado geral, contudo, a nomeação a indicação do Encarregado constitui, como regra, requisito obrigatório de conformidade, cuja ausência constitui infração administrativa direta sujeita a sanções.

Em relação ao operador, a legislação não impõe, de forma geral, a obrigatoriedade de indicação de Encarregado. Nesses casos, sua nomeação possui caráter facultativo, embora seja recomendada como boa prática de governança e mecanismo de fortalecimento dos processos de conformidade em proteção de dados (ANPD, 2024).

Quanto à divulgação da identidade do Encarregado, a Resolução CD/ANPD nº 18/2024 estabelece que devem ser informadas, no mínimo, as seguintes identificações: o nome completo, quando se tratar de pessoa natural; ou, no caso de pessoa jurídica, o nome empresarial ou o título do estabelecimento. Nessa última hipótese, é igualmente necessário indicar o nome completo da pessoa natural responsável (ANPD, 2024).

2.3.2 Designação do Encarregado substituto

Uma das principais inovações introduzidas pela Resolução CD/ANPD nº 18/2024 foi a exigência de governança voltada à perenidade e à continuidade operacional: a obrigatoriedade de previsão e designação de um Encarregado substituto. As organizações não podem mais permitir que seus canais de atendimento fiquem paralisados devido a contingências humanas da liderança da área.

O Encarregado substituto deve ser formalmente indicado para atuar nas ausências, nos impedimentos temporários, nas licenças ou nas situações de vacância do titular do cargo. Essa diretriz visa mitigar o risco de interrupção no fluxo de conformidade. Sob a ótica prática, a indicação do substituto deve seguir os mesmos procedimentos e requisitos aplicáveis à designação do titular, incluindo a divulgação de sua identidade e de seus canais de contato. Além disso, quando o Encarregado designado for pessoa jurídica, torna-se obrigatório indicar também um substituto para a pessoa natural responsável. A ausência de uma figura suplente devidamente formalizada expõe a organização a sanções por descontinuidade nos canais de atendimento.

2.3.3 Atividades e atribuições do Encarregado

O escopo de atuação do Encarregado é vasto, dividindo-se entre papéis de intermediação externa e gestão estratégica interna. Suas atribuições essenciais, consolidadas no artigo 41 da LGPD e detalhadas pela Resolução 18/2024, incluem:

- **Canal de Intermediação com os Titulares:** receber reclamações, comunicações e, criticamente, processar e responder às requisições de direitos dos titulares (acesso, correção, eliminação, portabilidade) dentro dos prazos legais.
- **Ponto de Contato com a ANPD:** receber as comunicações, notificações e requisições de esclarecimento da autoridade reguladora, adotando as providências necessárias em nome do controlador.
- **Orientação Interna:** orientar, treinar e conscientizar os colaboradores, terceirizados e contratados da organização a respeito das melhores práticas de privacidade e do cumprimento das normas protetivas.
- **Apoio na Gestão de Riscos e Incidentes:** prestar assistência técnica na elaboração de Relatórios de Impacto à Proteção de Dados (RIPD) e atuar de forma central na mitigação de incidentes de segurança que envolvam dados pessoais.

Diante desse conjunto de atribuições, observa-se que o Encarregado não atua apenas como um ponto operacional, mas como uma função estratégica essencial à governança de dados pessoais. Seu papel é determinante para assegurar a conformidade com a LGPD, promover uma cultura organizacional voltada à privacidade e fortalecer a confiança entre a organização, os titulares de dados e a autoridade reguladora.

2.3.4 Conflitos de interesse no cargo de Encarregado

A correta gestão do conflito de interesses passou a ocupar posição central nas discussões de governança. De acordo com o artigo 2°, II, do Regulamento sobre a atuação do Encarregado, o conflito de interesse é a situação que possa comprometer, influenciar ou afetar, de maneira imprópria, a objetividade e o julgamento técnico no desempenho das atribuições do encarregado (ANPD, 2024). O conflito de interesses pode surgir tanto no acúmulo de funções desempenhadas no âmbito de um mesmo agente de tratamento quanto no exercício da atividade de DPO junto a diferentes agentes de tratamento.

De modo geral, a ANPD presume a ocorrência de conflito caso o profissional seja designado para fiscalizar e auditar operações de tratamento das quais ele próprio definiu as finalidades ou quando ocupa posições executivas estratégicas com alto poder decisório na alta administração, como cargos de chefia, gerência ou direção, responsáveis pela determinação de meios e objetivos do tratamento de dados pessoais (ANPD, 2024). Por isso, recomenda-se a análise do caso concreto e, sempre que possível, a segregação de funções para garantir maior independência no exercício do cargo.

Compete ao DPO comunicar formalmente à alta administração a existência de situações de conflito de interesses, reais ou potenciais, relacionadas ao exercício de suas funções. Para mitigar esse risco, a ANPD recomenda a instituição de uma unidade organizacional própria e segregada, assegurando independência funcional e reporte direto ao mais alto nível executivo.

Por fim, compreendidos os contornos regulatórios que balizam a estruturação jurídica e institucional do Encarregado, torna-se indispensável confrontar esse arcabouço normativo idealizado pela ANPD com a realidade fática do ecossistema corporativo nacional. A transição de um compliance meramente formal "de fachada" para uma governança de privacidade viva e material depende da capacidade real das empresas de absorverem essas regras em suas estruturas de custos e operações diárias. No próximo capítulo, analisaremos a dimensão prática dessa implementação sob uma perspectiva eminentemente empírica, investigando como o mercado brasileiro tem se portado diante dessas exigências regulatórias e quais são os reais desafios orçamentários e de infraestrutura humana enfrentados pelos DPOs no cenário nacional.

3. O DPO no cenário real: diagnóstico e desafios de implementação prática

Conforme demonstrado na seção anterior, a ANPD estabeleceu parâmetros normativos relevantes para a estruturação da atuação do Encarregado pelo Tratamento de Dados Pessoais (DPO). Todavia, a efetividade desse modelo não se esgota na regulação formal, dependendo, de forma decisiva, da capacidade das organizações de internalizarem essas diretrizes em suas práticas de governança.

Nesse contexto, a análise empírica da realidade empresarial brasileira revela-se essencial para aferir o grau de aderência entre o modelo regulatório proposto e sua aplicação concreta. Para esse fim, utiliza-se como principal base o relatório "Perfil DPO Brasil 2025", elaborado pelo Opice Blum Advogados, em parceria com a Rede Líderes. A pesquisa, conduzida com 203 profissionais atuantes como DPO em organizações públicas e privadas de diversos portes e setores, fornece elementos relevantes para a compreensão do estágio atual de maturidade da função no país.

Os resultados apontam avanços significativos desde a entrada em vigor da LGPD, evidenciando a progressiva inserção do Encarregado em posições mais estratégicas dentro das estruturas organizacionais. Não obstante, também demonstram que tal processo de amadurecimento ocorre de forma heterogênea, persistindo desafios estruturais relacionados à alocação de recursos, à autonomia funcional e à consolidação de uma cultura organizacional orientada à proteção de dados pessoais.

3.1 Estrutura organizacional e alocação da função do Encarregado

Os dados do relatório permitem identificar que parcela significativa das organizações já avançou na formalização da função do Encarregado, especialmente em empresas de médio e grande porte, com destaque para setores como tecnologia, saúde, sistema financeiro, energia e indústria, segmentos caracterizados pelo elevado volume de tratamento de dados e maior exposição a riscos regulatórios.

Outro aspecto relevante diz respeito à localização institucional do Encarregado dentro da estrutura organizacional. Verifica-se a predominância de sua vinculação a áreas de natureza normativa e de controle, como Jurídico, Compliance, Governança e Gestão de Riscos, que concentram aproximadamente 72% dos casos. Em contrapartida, apenas uma parcela minoritária (cerca de 15%) atua diretamente em departamentos técnicos, como Tecnologia da Informação ou Segurança da Informação. Esse dado sugere que a função vem sendo interpretada, no contexto brasileiro, predominantemente sob uma perspectiva jurídica-regulatória, em detrimento de uma abordagem vinculada com as dimensões tecnológicas da proteção de dados.

Esse cenário é complementado pela análise do tempo efetivamente dedicado às atividades de Encarregado. Observa-se que 49% dos profissionais despendem ao menos 16 horas semanais na função, sendo que apenas 25% atuam de forma exclusiva. A maioria, portanto, acumula outras atribuições, frequentemente em áreas correlatas como Jurídico e Compliance.

A estrutura organizacional disponível para o exercício da função constitui outro indicador relevante do nível de maturidade da governança em privacidade. A pesquisa evidencia que a maioria dos Encarregados (69%) atua em equipes reduzidas, com até cinco profissionais, enquanto apenas uma fração limitada das organizações dispõe de estruturas mais robustas, com mais de dez integrantes. Ademais, chama atenção o fato de que aproximadamente 22% dos respondentes exercem suas atividades sem qualquer equipe de apoio, o que reforça o caráter ainda incipiente da institucionalização da função em parte das organizações.

Nesse sentido, observa-se que o caminho ideal para a eficácia da função parece não residir apenas na figura individual do Encarregado, mas sim na estruturação de

equipes multidisciplinares que o auxiliem, visto que não se apresenta como uma expectativa razoável que um único profissional domine com profundidade absoluta os campos jurídico, tecnológico e de gestão de riscos simultaneamente. Tal entendimento encontra respaldo no Guia Orientativo sobre a atuação do encarregado (ANPD, 2024), que reconhece que, a depender das atividades desempenhadas, do porte da organização e do volume de operações de tratamento, o encarregado poderá necessitar de uma equipe de apoio ou comitê que lhe forneça suporte no desempenho de suas funções. Essa simbiose garante que a proteção de dados seja integrada de forma sistêmica à estratégia da empresa, consolidando o Encarregado como um agente estratégico de resiliência corporativa.

3.2 Autonomia funcional, reporte e desafios à efetividade da atuação

Além da estrutura organizacional, a efetividade da atuação do Encarregado depende diretamente do grau de autonomia funcional que lhe é conferido. A independência na condução de suas atividades, aliada ao acesso à alta administração, constitui elemento central para o cumprimento adequado de suas atribuições, especialmente diante de potenciais conflitos de interesse.

Os dados da pesquisa indicam que 66% dos Encarregados percebem possuir autonomia funcional. Contudo, parcela relevante dos profissionais relata que essa independência é apenas parcial (24%) ou inexistente (10%). Tal constatação evidencia que, embora o modelo normativo preveja a autonomia como um requisito essencial, sua efetiva concretização ainda enfrenta dificuldades práticas no ambiente organizacional brasileiro.

Outro desafio relevante diz respeito ao apoio institucional conferido ao Encarregado. A governança em proteção de dados pressupõe comprometimento da alta administração, uma vez que decisões relacionadas à alocação de recursos, definição de prioridades e implementação de controles internos dependem diretamente dos níveis estratégicos da organização. Embora a pesquisa demonstre avanço na participação do DPO em reuniões e processos decisórios, parte dos profissionais ainda relata dificuldades de acesso à alta gestão ou limitação de sua influência nas decisões corporativas. Isso demonstra que a consolidação da função exige não apenas reconhecimento formal, mas efetivo apoio institucional, capaz de conferir ao Encarregado legitimidade para influenciar a formulação das políticas internas e a gestão dos riscos relacionados ao tratamento de dados pessoais.

Todavia, os desafios enfrentados pelas organizações brasileiras não decorrem apenas da limitação de recursos humanos. A pesquisa revela que um dos principais obstáculos identificados pelos próprios Encarregados está relacionado à consolidação de uma cultura organizacional voltada à proteção de dados. Entre as dificuldades mais frequentemente apontadas destacam-se a baixa conscientização dos colaboradores, o desconhecimento da legislação por fornecedores e parceiros comerciais, bem como a dificuldade de manutenção contínua dos processos internos de conformidade.

Esse cenário demonstra que a efetividade da LGPD depende de transformação cultural que ultrapassa a simples adoção de medidas documentais. A elaboração de políticas internas, a revisão contratual e a nomeação formal do Encarregado representam etapas importantes do processo de adequação, mas não são suficientes para assegurar a proteção de dados como prática cotidiana.

A governança em privacidade pressupõe a incorporação dos princípios da responsabilização (*accountability),* da prevenção e da transparência aos processos decisórios, exigindo o envolvimento permanente das diferentes áreas da organização.

Nesse contexto, a atuação do DPO assume papel que transcende a fiscalização do cumprimento da legislação. O Encarregado passa a exercer função pedagógica e estratégica, promovendo treinamentos, orientando colaboradores, difundindo boas práticas e contribuindo para a construção de uma cultura institucional orientada pela proteção de dados pessoais. Essa perspectiva reforça a compreensão de que a conformidade não constitui resultado de ações isoladas, mas de um processo contínuo de gestão de riscos e aprimoramento organizacional.

A percepção dos próprios profissionais acerca do nível de maturidade das organizações reforça essa conclusão. Embora parcela significativa dos respondentes considere elevado o grau de maturidade em proteção de dados,

muitos atuam em organizações que realizam operações classificadas como de alto risco ou reconhecem limitações estruturais capazes de comprometer a efetividade dos programas de privacidade. Isso indica que a maturidade organizacional não pode ser aferida apenas pela existência de documentos formais ou pela designação de um Encarregado, mas pela capacidade da instituição de integrar a proteção de dados ao seu modelo de governança e à sua cultura corporativa.

Nesse sentido, a consolidação da função do Encarregado demanda não apenas o cumprimento formal das exigências legais, mas a internalização de uma cultura organizacional orientada à proteção de dados, aliada à estruturação de modelos de governança que garantam efetiva independência e capacidade de atuação. Apenas a partir dessa convergência será possível assegurar que o Encarregado atue, de fato, como agente central na promoção da conformidade e na mitigação de riscos no contexto da LGPD.

Conclusão

A presente análise buscou examinar o enquadramento regulatório do Encarregado pelo Tratamento de Dados Pessoais (DPO) no Brasil, investigando a relação entre as exigências formais de conformidade e a necessidade premente de uma eficácia material no ecossistema corporativo nacional. Frente à abertura normativa deixada pelo texto original da LGPD e pelo subsequente veto presidencial aos requisitos mínimos de qualificação do cargo, o advento da Resolução CD/ANPD nº 18/2024 e do Guia Orientativo da ANPD demarcou um ponto de inflexão essencial, impondo parâmetros explícitos de governança, continuidade e autonomia técnica para a atuação desse profissional.

O diagnóstico fático do mercado nacional trouxe à superfície os desafios práticos enfrentados no cotidiano corporativo, sobretudo no que diz respeito à consolidação de uma autêntica cultura de privacidade. Nesse contexto, o Encarregado assume, muitas vezes, um papel de agente de aculturação, responsável por promover a conscientização interna e fomentar a incorporação da privacidade como valor organizacional. Verificou-se, ainda, que a atuação do Encarregado, nesse setor, tende a se estruturar de forma coletiva, por meio de arranjos organizacionais que extrapolam a figura individual do DPO. Nesse sentido, destacam-se os comitês de proteção de dados e as estruturas de governança baseadas em equipes multidisciplinares, que reúnem profissionais das áreas de Direito, Tecnologia da Informação, Segurança da Informação (*cybersecurity*) e Engenharia. Longe de representar mera soma de especializações, tais arranjos viabilizam a construção de uma governança verdadeiramente multidisciplinar, capaz de integrar diferentes saberes na análise dos riscos, na definição de controles e na implementação de medidas de conformidade.

A principal contribuição deste escrito repousa na contextualização desse descompasso entre a teoria dogmática e o pragmatismo empresarial, oferecendo às organizações e ao setor produtivo um referencial crítico para reestruturar suas linhas de defesa e governança informacional. Por outro lado, reconhecem-se como limitações do estudo o recorte amostral e temporal intrínseco aos dados analisados, bem como o caráter recente da própria Resolução nº 18/2024, cujos efeitos práticos sobre a fiscalização e a aplicação de sanções administrativas pela ANPD ainda demandarão acompanhamento de longo prazo.

Sob a ótica das tendências futuras, delineia-se um movimento gradual de amadurecimento no ecossistema de proteção de dados no Brasil, impulsionado pela adoção de modelos de governança baseados em estruturas colaborativas. A emergência de comitês e instâncias multidisciplinares dentro das organizações – arranjos já chancelados de forma incipiente pela própria ANPD – reflete uma resposta institucional pragmática à complexidade da matéria, permitindo a integração de diferentes saberes. Dessa forma, supera-se a lógica de atuação isolada, conferindo maior robustez e efetividade aos programas de privacidade. Assim, entre a teoria normativa e os desafios da prática, a figura do Encarregado se revela não apenas como elemento de conformidade, mas como protagonista na construção de uma nova racionalidade organizacional, na qual a proteção de dados precisa deixar de ser apenas uma obrigação formal para se afirmar como expressão concreta da dignidade humana na sociedade da informação.

Referências

AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD). *Centrais de Conteúdo*. Brasília: ANPD, [20--]. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo. Acesso em: 13 jun. 2026.

AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD). *Guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado*. Brasília: ANPD, 2022. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes. Acesso em: 25 maio 2026.

AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD). *Guia orientativo sobre a atuação do encarregado*. Brasília, 2024. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes. Consulta em: 25 mai. 2026.

AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD). *Resolução CD/ANPD nº 18, de 16 de julho de 2024*. Aprova o Regulamento sobre a atuação do encarregado pelo tratamento de dados pessoais. Brasília: ANPD, 2024. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-18-de-16-de-julho-de-2024-572632074. Acesso em: 25 maio 2026.

BRASIL. *Emenda Constitucional nº 115, de 10 de fevereiro de 2022*. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Brasília: Presidência da República, 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/emendas/emc/emc115.htm. Acesso em: 25 maio 2026.

BRASIL. *Lei nº 10.406, de 10 de janeiro de 2002*. Institui o Código Civil. Brasília: Presidência da República, 2002. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm. Acesso em: 27 jun. 2026.

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

BRASIL. *Mensagem nº 288, de 8 de julho de 2019*. Brasília: Presidência da República, 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/msg/vep/VEP-288.htm. Acesso em: 30 maio 2026.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. 2. ed. Rio de Janeiro: Forense, 2019.

EUROPEAN DATA PROTECTION BOARD (EDPB). *Data protection by design & by default*: when to act and what to do. Bruxelas: EDPB, fev. 2026. Disponível em: https://www.edpb.europa.eu/system/files/2026-02/edpb-summary-gdpr-data-protection-design-default_en.pdf. Acesso em: 2 jul. 2026.

EUROPEAN DATA PROTECTION BOARD (EDPB). *Guidelines on Data Protection Officers* ('DPOs'). Bruxelas: EDPB, 2017. Disponível em: https://ec.europa.eu/newsroom/article29/items/612048. Acesso em: 30 maio 2026.

EUROPEAN DATA PROTECTION BOARD (EDPB). *Who we are*. Bruxelas: EDPB, [2018?]. Disponível em: https://www.edpb.europa.eu/about-edpb/who-we-are/european-data-protection-board_en. Acesso em: 27 maio 2026.

FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (coord.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro*. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

OPICE BLUM; REDE LÍDERES. *Perfil DPO Brasil 2025*. São Paulo: Opice Blum, 2025. Disponível em: https://www.opiceblum.com.br/publicacoes/relatorio-perfil-dpo-brasil/. Acesso em: 30 maio 2026.

RODOTÀ, Stefano. *A vida na sociedade da vigilância:* a privacidade hoje. Rio de Janeiro: Renovar, 2008.

SANTOS, Plácida Leopoldina Ventura Amorim da Costa; CARVALHO, Angela Maria Grossi de. Sociedade da informação: avanços e retrocessos no acesso e no uso da informação. *Informação & Sociedade*: Estudos, João Pessoa, v. 19, n. 1, p. 45-55, jan./abr. 2009. Disponível em: https://periodicos.ufpb.br/index.php/ies/article/view/1782. Acesso em: 26 out. 2026.

TABAK, Benjamin Miranda. A análise econômica do direito: proposições legislativas e políticas públicas. *Revista de Informação Legislativa*, Brasília, ano 52, n. 205, p. 321-345, jan./mar. 2015. Disponível em: https://www2.senado.leg.br/bdsf/handle/id/509955. Acesso em: 26 out. 2026.

UNIÃO EUROPEIA. *Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016*, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Jornal Oficial da União Europeia: Luxemburgo, L 119, p. 1-88, 4 maio 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016R0679. Acesso em: 10 jun. 2026.

WARREN, Samuel; BRANDEIS, Louis. The right to privacy. *Harvard Law Review*, [S. l.], v. 4, n. 5, p. 193-220, 15 dez. 1890. Disponível em: https://doi.org/10.2307/1321160.

Oportunidades nas adversidades:

o que tirar de aprendizado em processos de fiscalização

Januária
Sá Barreto Lopes

Januária Sá Barreto Lopes é gerente de Integridade Corporativa e DPO do Sistema Firjan. Membra do Compliance Women Committee.
Formada em Ciências Contábeis, com MBA Executivo em Governança Corporativa e Compliance pelo Mackenzie, certificada em Compliance Healthcare pelo CBEXS.
Formada em curso de extensão em Proteção de Dados e de Governança em IA no Dara Privacy Brasil.

Introdução

Parte da rotina de quem trabalha ou estuda proteção de dados pessoais inclui a observação e o aprendizado sobre casos emblemáticos no mercado, seja no que diz respeito a notícias na mídia, processos de investigação, sanções aplicadas pela Agência Nacional de Proteção de Dados (ANPD) ou outras instituições fiscalizadoras.

Casos de terceiros que resultaram em sanções e/ou recomendações oriundas de processos de fiscalização, em especial da ANPD, oportunizam às empresas a antecipação de adequações e melhorias nos seus programas de privacidade e proteção de dados, a partir de entendimentos que por vezes não estão regulamentados ou muito claros no arcabouço legal, o que pode evitar, em última instância, penalidades futuras.

Neste artigo, será abordado um caso amplamente divulgado em veículos de comunicação, com o objetivo de fazer um paralelo com as práticas que, à luz da Lei Geral de Proteção de Dados (LGPD) (nº 13.709/18), poderiam ter evitado ou minimizado os danos causados aos titulares dos dados e às empresas.

Destaca-se que não é o objetivo do artigo fazer juízo de valor quanto às empresas envolvidas ou ao processo em si.

1. O caso: compartilhamento de dados pessoais entre Claro e Serasa

Para ilustrar as questões que serão discutidas neste artigo, tomamos como pano de fundo um caso concreto analisado pela ANPD. O processo teve origem em um questionamento encaminhado pelo Ministério Público Federal (MPF) em conjunto com o Conselho Administrativo de Defesa Econômica (Cade) para a ANPD, em 2021, e teve como objeto a apuração do compartilhamento de dados pessoais de clientes da Claro S.A. à Serasa Experian S.A., segundo os autos, com a finalidade de monetizar informações pessoais restritas de clientes.

Conforme Nota Técnica nº 3/2023/FIS/CGF/ANPD, parte integrante do processo administrativo conduzido pela ANPD, havia um contrato firmado entre as empresas, cujo escopo era o fornecimento pela contratada (Claro) para a contratante (Serasa), de forma remunerada, de um *Book* em *Ranges*[1] com o cálculo das pontuações, resultantes de dados não identificados ou que não permitiriam a identificação dos serviços prestados pela contratada, com a finalidade exclusiva de utilização pela Serasa em um projeto piloto. Este, se bem-sucedido, seria aproveitado como insumo de suas soluções com a finalidade de proteção ao ciclo de crédito e/ou de prevenção a fraudes.

Por esse motivo, em 2022, foi determinada pela ANPD a abertura de Procedimento Preparatório para início das diligências com o objetivo de averiguar os fatos relatados pelo MPF junto ao Cade.

A partir da análise das respostas das empresas Claro e Serasa, em 2023, foi emitida a Nota Técnica nº 3, a qual concluiu que a continuidade do compartilhamento de dados pessoais entre as empresas Claro e Serasa deveria ser condicionada à implementação de medidas que foram então determinadas pela ANPD.

Em 2026, por meio da conclusão da Nota Técnica nº 2/2026/CPDP/CGF/SFI/ANPD, houve a recomendação de instauração de Processo Administrativo Sancionador em face da Claro e iniciado um procedimento de fiscalização para apurar as medidas de transparência e exercício de direito dos titulares adotadas pela Serasa.

Em junho de 2026, a Claro recebeu um auto de infração, indicando os dispositivos legais e regulamentares infringidos, além da possibilidade de aplicação de uma ou mais sanções listadas no artigo 52 da LGPD, que seria definida ao fim da análise do processo administrativo sancionador, de acordo com o Regulamento de Dosimetria e Aplicação de Sanções Administrativas.

[1] O *Book de Ranges* consiste em um documento de referência que consolida as faixas, limites e critérios usados para classificar o risco de crédito de clientes.

1.1. Da instauração do processo fiscalizatório

Com base no artigo 6° da LGPD, ou seja, observados os princípios previstos na lei, inicialmente foram considerados alguns pontos que ensejaram a necessidade de abertura de procedimento de desenvolvimento preparatório para diligências pela ANPD, para fins de averiguação, descritos na seguinte ordem:

I. Quanto ao inciso I, se a **finalidade** do compartilhamento de dados pessoais de clientes da Claro com a Serasa teria legitimidade. Ainda no mesmo inciso, se a finalidade do compartilhamento desses mesmos dados pela Serasa aos seus clientes também seria legítima;
II. Partindo para o inciso II, se a(s) hipótese(s) legal(is) (também conhecidas como bases legais) para esses tratamentos obedecia(m) ao critério de **adequação**;
III. Considerando o instrumento contratual entre Claro e Serasa, se este estaria em conformidade com o inciso VI, qual seja, o da **transparência**;
IV. Depois há um retorno ao inciso III, com questionamento sobre a observância da **necessidade** ou minimização dos dados;
V. Por fim, sobre o inciso IV, se o compartilhamento obedeceu ao princípio da **não discriminação**.

Observando o ordenamento dos itens, verifica-se que foram inicialmente considerados cinco princípios para averiguação de possíveis desconformidades. Sendo o primeiro o mais relevante, pois não havendo finalidade legítima para o tratamento, os demais princípios somente agravariam o possível descumprimento legal.

As bases legais utilizadas nas duas hipóteses de tratamento não foram entendidas como legítimas pela ANPD, na conclusão do processo (o que será mencionado adiante).

Com relação ao princípio da transparência, considerando haver a boa-fé do agente de tratamento, ao publicizar de forma clara a finalidade do compartilhamento nos principais instrumentos utilizados, como no aviso de privacidade, o titular poderia ter oportunizados os seus direitos previstos, como de acesso, de apagamento, de revisão de decisão ou de oposição. Porém, há de se considerar a assimetria de conhecimento para a maioria dos titulares de dados quanto à LGPD e que o os dados compartilhados em questão são provenientes do serviço de telefonia móvel, internet e outros serviços utilizados de forma massiva e por diversos níveis sociais.

Assim, ainda que houvesse o melhor uso do princípio da transparência, este não constitui o ponto prioritário de análise quanto à desconformidade do processo — ou não deveria constituí-lo —, mas ser objeto de uma avaliação secundária.

Já em relação ao risco de discriminação decorrente do compartilhamento dos dados com a Serasa para as finalidades informadas, faz-se importante ressaltar que este princípio não se observa apenas no tratamento de dados sensíveis. Assim, dados, como os de residência ou geolocalização, por exemplo, podem ensejar um resultado que atribua ao titular um *score,* não necessariamente correto, de capacidade de pagamento.

1.2 Da análise do processo instaurado pela ANPD

A análise descrita na Nota Técnica n° 3 do processo administrativo conduzido pela ANPD é iniciada com menção de referências a artigos doutrinários e posicionamentos jurisprudenciais.

Considerando os dispositivos da própria LGPD somados aos entendimentos utilizados como referência, a ANPD apontou indícios de falhas da Claro como controladora originária no processo de compartilhamento de dados para a Serasa, especialmente em relação aos itens a seguir.

i. A inadequação da hipótese legal utilizada

Considerada como questão central do caso, a ANPD analisou as duas hipóteses legais informadas como utilizadas pela Claro, proteção ao crédito e/ou prevenção a fraudes.

Quanto à utilização da base legal de proteção ao crédito, a ANPD entendeu que ela não seria aplicável ao tratamento realizado, pois o compartilhamento de dados não visou à avaliação do risco de crédito da Claro, mas à avaliação do risco de inadimplência de seus clientes para terceiros, por meio dos *scores* calculados pela empresa Serasa.

Por outro lado, apesar da ANPD entender que a Serasa poderia se utilizar dessa base legal, em razão de sua própria atividade fim, seria necessário que sua coleta desses dados por meio do compartilhamento da controladora originária (Claro) fosse considerado como legítimo.

Quanto ao tratamento de dados para fins de prevenção a fraudes, fundamentado no legítimo interesse, a ANPD entendeu que também não havia amparo legal. Ainda que não estivessem em jogo dados sensíveis, o que afastaria uma vedação mais evidente, a finalidade invocada não correspondia a um interesse legítimo da própria controladora, no caso, a Claro, mas sim ao interesse da Serasa, destinatária dos dados. Segundo a ANPD, essa dissociação entre a finalidade do tratamento e o interesse do controlador inviabiliza o recurso ao artigo 7°, IX (ou artigo 11, II, "g"), da LGPD como base legal aplicável.

Nesse ponto, a ANPD ressaltou ainda um aspecto relevante: a necessidade de que cada finalidade de tratamento esteja amparada em uma única base legal, não sendo admissível a escolha posterior ou a sobreposição de fundamentos legais para justificar a mesma operação.

ii. Dos direitos dos titulares

A dificuldade apontada pela Agência para o exercício de direitos por parte dos titulares gira em torno das lacunas de informação no aviso de privacidade disponibilizado aos clientes da Claro em seu site, remetendo desta forma também à inadequação ao princípio da transparência.

Quanto ao compartilhamento, a empresa inicialmente informava em seu aviso que os dados dos seus clientes eram compartilhados com empresas de crédito e cobranças. Posteriormente, reforçou que esse compartilhamento também tinha como objetivo fornecer insumos para o desenvolvimento de produtos voltados à análise e concessão de crédito e soluções antifraude. Porém, a ANPD não considerou esta informação suficiente para o entendimento dos seus clientes sobre a real finalidade do tratamento.

A Agência considerou ainda que, na informação sobre o compartilhamento realizado, seria necessário denominar o receptor dos dados e sua classificação enquanto agente de tratamento, nesse caso, a Serasa como controladora.

Também houve questionamento sobre a falta de informações disponibilizadas quanto à forma e duração do tratamento dos dados. Nesse ponto, a ANPD pondera a necessidade de explicitar os prazos de retenção no aviso de privacidade.

Pontua ainda a responsabilidade da Claro quanto ao dever de garantia de que a empresa para a qual os dados são compartilhados, mesmo enquanto controladora, atuará em conformidade com a legislação de proteção de dados, por meio de dispositivos e instrumentos jurídicos que prevejam obrigações, inclusive sobre o dever de transparência quanto ao tratamento e prazo de retenção dos dados pessoais.

A falta de clareza no aviso de privacidade apontada pela ANPD, em sua interpretação, poderia implicar a impossibilidade de exercício dos direitos previstos na LGPD, pelos titulares, uma vez que o desconhecimento não permitiria ao cliente o exercício dos direitos de livre acesso, correção, exclusão, revisão de decisões ou oposição, inclusive perante os terceiros com quem os dados eram compartilhados.

iii. Do princípio da transparência e da boa-fé

Em linha com o que foi mencionado na análise sobre os direitos dos titulares, a ANPD apontou a importância sobre a prestação de informação mais clara e específica aos titulares em políticas de privacidade e contratos, em especial sobre: a) os dados pessoais compartilhados; b) o agente de tratamento destinatário do compartilhamento (ou seja, o nome do ente público ou privado com o qual há o compartilhamento); c) as finalidades específicas do compartilhamento, explicando de maneira acessível o motivo pelo qual os dados estão sendo compartilhados, incluindo se é realizado eventual perfilamento do titular a partir de tal tratamento; d) a hipótese legal que fundamenta o compartilhamento; e e) a duração do compartilhamento. Ademais, eventuais mudanças de regras de compartilhamento após a assinatura do contrato precisariam ser comunicadas aos titulares afetados por essas mudanças, sendo conferido a eles, quando for o caso, o direito de oposição ao novo tratamento, especialmente se realizado com fundamento no artigo 7°, inciso IX, da LGPD.

Como consequência da falta de transparência questionada pela ANPD, é mencionado em item posterior, o princípio da boa-fé, indicando a necessidade de avaliação sobre a conduta das empresas, se estaria de acordo com o que o consumidor/titular de dados poderia legitimamente esperar.

iv. Dos princípios da finalidade, adequação e necessidade

Complementando a análise sobre a inadequação das hipóteses legais indicadas pela Claro, a ANPD também apontou o excesso de dados compartilhados em relação às finalidades pretendidas, ainda que, como visto, essas finalidades sequer estivessem amparadas em uma hipótese legal legítima.

v. Do livre acesso

Ao analisar esse princípio, a ANPD entendeu que a falta de transparência e de informação clara aos clientes quanto à finalidade do compartilhamento entre Claro e Serasa inviabilizava o exercício dos direitos previstos no artigo 18 da LGPD, não se podendo considerar observado o princípio do livre acesso.

vi. Da qualidade dos dados

Nessa análise, a ANPD traz como ponto central o questionamento sobre o prazo de retenção de 10 anos informado pela Serasa, com base no artigo 205 do Código Civil, segundo o qual "a prescrição ocorre em dez anos, quando a lei não lhe haja fixado prazo menor". A Agência pondera, ainda, se a relevância e a qualidade desses dados se mantêm ao longo de um prazo tão extenso, a ponto de justificar sua necessidade para o cumprimento da finalidade do tratamento, no caso, a análise de crédito e a prevenção a fraudes.

vii. Da segurança e da prevenção

Como medida técnica principal para garantia da segurança, a Claro apresentou à Agência o instrumento contratual firmado com a Serasa, que continha cláusula de proteção de dados. Em linhas gerais, foram ressaltados os seguintes pontos da cláusula: responsabilidades das partes, compromisso de conformidade com a LGPD e direito de auditoria.

Com base nessas cláusulas, a ANPD considerou atendido o princípio da segurança, não avaliando como necessárias medidas técnicas e administrativas adicionais. Já quanto ao princípio da prevenção, a Agência entendeu que este não poderia ser considerado atendido, tendo em vista os apontamentos de desconformidade e de violação aos direitos dos titulares constantes na Nota Técnica.

viii. Não discriminação

Em razão do desconhecimento do titular quanto ao tratamento dos dados realizado pela Serasa, relativo ao objeto do contrato, a ANPD considerou que não foi elucidado como o titular poderia exercer seus direitos de pedido de revisão ou de oposição, frente a condutas discriminatórias eventualmente ocorridas.

Dessa forma, a ANPD menciona que "não é suficiente que a Serasa desenvolva método e o disponibilize no mercado; faz-se necessário que permita ao titular fazer face aos resultados por ela diretamente disponibilizados ao concedente de crédito". Assim, a garantia da não discriminação no tratamento dos dados depende da possibilidade de acesso pelos titulares aos resultados auferidos, assim como do direito de revisão dos dados e de oposição.

ix. Da prestação de contas

A Agência pondera em sua análise que a prestação de contas exige a "demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas".

Assim, considerando as desconformidades identificadas, a ANPD menciona que são necessárias medidas para "conduzir o agente de tratamento à plena conformidade ou evitar ou remediar situações que acarretem risco ou dano aos titulares de dados pessoais".

x. Conclusão da Nota Técnica

Na conclusão da Nota Técnica, a ANPD condiciona a continuidade do compartilhamento dos dados pela Claro para a Serasa ao cumprimento dos seguintes itens:

a) Eliminação ou readequação dos tratamentos de dados fundamentados nas hipóteses de prevenção à fraude e proteção do crédito, considerando que as hipóteses legais não teriam legitimidade;

b) Adequação do processo de tratamento de dados aos princípios previstos na LGPD, mencionados na análise da Nota Técnica;

c) Adequação aos requisitos de transparência para a garantia do direito dos titulares; e

d) Abstenção de utilização ou eliminação de dados excessivos (estes seguiram em sigilo no documento) para o tratamento de dados com finalidade de proteção ao crédito.

As três primeiras determinações foram comuns à Claro e à Serasa. Em complemento, para verificação posterior pela Agência, esta solicita para ambas as empresas o Relatório de Impacto referente ao compartilhamento realizado entre as partes e o Registro de Operações de Tratamento (ROPA).

1.3. Auto de infração Claro

A partir das conclusões da Nota Técnica, a ANPD remeteu o caso à Coordenação-Geral de Sanções, dando origem a um Processo Administrativo Sancionador contra a Claro, distinto do processo de fiscalização original. No auto de infração então lavrado, são descritos os fatos e os dispositivos normativos considerados infringidos.

Segundo entendimento da ANPD, a Claro, na qualidade de controladora originária, teria falhado em "delimitar finalidades específicas e demonstrar a necessidade e a proporcionalidade dos dados pessoais compartilhados; atender a princípios diversos da LGPD; e viabilizar o exercício de direitos pelos titulares de dados pessoais afetados pelo compartilhamento".

Após ressaltar o princípio da boa-fé, a ANPD aponta a desconformidade com os princípios da finalidade, pois não haveria propósito legítimo e específico no uso secundário dos dados pessoais dos seus clientes; adequação, devido à incompatibilidade com os dados tratados; e necessidade, pelo uso de dados excessivos no tratamento. A ANPD considerou a prática "desproporcional e potencialmente abusiva, ampliando riscos à privacidade e violando o direito dos titulares".

Com relação ao aviso de privacidade, a ANPD apontou que as informações disponibilizadas sobre o tratamento de dados pessoais no contexto de relações com empresas de soluções de crédito seriam "excessivamente abrangentes e genéricas", não transparecendo ao titular dos dados a finalidade específica do contrato celebrado com a Serasa, não se assegurando ao titular "a compreensão precisa sobre as características essenciais do tratamento realizado, como sua extensão, duração, finalidade concreta e eventuais compartilhamentos específicos envolvidos, o que compromete a transparência e dificulta o exercício informado de seus direitos.

A Agência também pontuou que a Claro não disponibilizaria o contato do Encarregado de forma clara e acessível no Portal de Privacidade, indicando a necessidade de acesso a diversas telas para se obter o acesso, o que estaria em desacordo com o artigo 41, §1º da LGPD, c/c o artigo 9º, caput e inciso IV, e detalhadas na Resolução CD/ANPD nº 18. Ressaltou ainda não haver a identificação do Encarregado na página que daria acesso ao contato do Encarregado/DPO e que esta informação estaria disponível apenas na Política de Privacidade, como último item. Em virtude disso considerou infração a ausência de objetividade e clareza na indicação da identidade do encarregado pelo tratamento de dados pessoais no sítio eletrônico do controlador, em desrespeito ao artigo 41, §1º da LGPD, c/c artigo 9º, caput e inciso IV.

Importante ressaltar que essa etapa do processo ainda assegurava à Claro o direito de defesa. Já a Serasa passou a responder a procedimento de fiscalização próprio, voltado à apuração das medidas de transparência e de exercício de direitos por ela adotadas, desdobramentos que mantêm o caso em aberto para ambas as empresas.

Conclusão

Embora a operação de compartilhamento de dados entre Claro e Serasa tenha sido encerrada, o caso segue relevante, não pela conduta específica das empresas envolvidas, mas como paradigma para observar, na prática, como a ANPD interpreta e aplica os princípios e critérios da LGPD. É esse o propósito deste artigo: extrair, dos pontos avaliados pela Agência, lições aplicáveis a qualquer operação de compartilhamento de dados pessoais, independentemente de qualquer juízo sobre as empresas aqui mencionadas.

O ponto central da análise conduzida pela ANPD foi o enquadramento da base legal. Segundo a Agência, sem finalidade legítima que ampare o tratamento, o compartilhamento não pode ocorrer ou deve ser adequado até que essa legitimidade exista. Os demais princípios avaliados, como adequação, necessidade, transparência, não discriminação pressupõem essa etapa anterior, e por isso dependem dela.

O princípio da minimização também foi objeto de escrutínio. A ANPD reforçou, reiteradamente, que apenas os dados estritamente necessários e adequados à finalidade pretendida podem ser tratados. No caso concreto, dados relativos ao exercício de direitos pelo consumidor, como registros de reclamações, cancelamentos e ocorrências, foram considerados excessivos para as finalidades informadas, o que também esbarra no artigo 21 da LGPD, que veda a utilização de dados pessoais referentes ao exercício regular de direitos pelo titular em seu prejuízo.

Do ponto de vista de governança, dois pontos práticos se destacam. O primeiro é a necessidade de documentar integralmente as decisões e os controles adotados nos processos de compartilhamento, incluindo o Relatório de Impacto à Proteção de Dados Pessoais (RIPD), cuja elaboração pode ser exigida pela ANPD em circunstâncias de alto risco, como no caso em análise. O segundo é a importância de instrumentos contratuais que vão além de cláusulas genéricas de confidencialidade e segurança: cláusulas robustas devem assegurar auditoria e fiscalização do cumprimento das obrigações pelo controlador receptor dos dados, delimitar claramente as responsabilidades entre os agentes de tratamento envolvidos e prever a eliminação dos dados compartilhados ao término da atividade ou do contrato.

Em relação à Serasa, a análise preliminar identificou possíveis falhas estruturantes nos instrumentos de transparência ativa disponibilizados, como Termo de Uso, Política de Privacidade e Portal de Privacidade, com potencial de comprometer a relação de confiança com os titulares e, por consequência, a própria legitimidade dos tratamentos por ela realizados. Diante disso, a ANPD recomendou a instauração de procedimento de fiscalização específico, voltado a apurar as medidas de transparência adotadas pela empresa e os mecanismos oferecidos para o exercício de direitos pelos titulares.

O caso reúne, assim, elementos que podem orientar outras empresas quanto às expectativas da ANPD na análise de operações semelhantes. Nem todas as medidas exigem grande esforço de implementação; algumas são relativamente simples de adotar, mas sua ausência pode acarretar riscos reputacionais, legais e financeiros relevantes, como demonstra o desfecho deste processo.

Por fim, cabe registrar que este artigo se baseou exclusivamente nos fatos e entendimentos tornados públicos até o momento. Por se tratar de processo ainda em curso, resguardado o direito ao contraditório, parte relevante da tramitação permanece sob sigilo, o que limita, mas não invalida, as lições que dele já se pode extrair.

Referências

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: 20 out. 2026.

BRASIL. Autoridade Nacional de Proteção de Dados. Resolução CD/ANPD nº 18, de 16 de julho de 2024. Aprova o Regulamento sobre a atuação do encarregado pelo tratamento de dados pessoais. *Diário Oficial da União*: seção 1, Brasília, DF, n. 136, p. 42, 17 jul. 2024.

BRASIL. Autoridade Nacional de Proteção de Dados (ANPD). *Processo de fiscalização nº 00261.000227/2022-06*. Verificação de conformidade do tratamento de dados pessoais por Claro S.A. e Serasa S.A. Brasília, DF: ANPD, 2022.

BRASIL. Autoridade Nacional de Proteção de Dados (ANPD). *Processo administrativo sancionador nº 00261.003285/2026-15*. Claro S.A.

BRASIL. Autoridade Nacional de Proteção de Dados (ANPD). *Processo de fiscalização nº 00261.003351/2026-49*. Serasa S.A. Brasília, DF: ANPD, 2026.

Gestão de incidentes e vazamentos de dados pessoais:

da prevenção à resposta

Uma abordagem integrada entre governança, tecnologia e conformidade regulatória

Sarah Raquel Nunes Câmara Santos

Sarah Raquel Nunes Câmara Santos é advogada, especialista em Governança de Dados e Cibersegurança pela PUC Minas e graduada em Defesa Cibernética pela FIAP. Analista de Privacidade na Firjan, foi Encarregada de Dados (DPO) da Unimed-Rio, com atuação em governança em privacidade, gestão de incidentes e análise de riscos. Integra a Comissão de Inteligência Artificial da OAB/RJ e é certificada em Privacidade e Proteção de Dados pela Data Privacy Brasil.

Introdução

Os incidentes de segurança envolvendo dados pessoais têm apresentado relevância crescente nas organizações, não apenas pelos impactos técnicos que podem provocar, mas também pelas possíveis consequências jurídicas, regulatórias, operacionais e reputacionais associadas a esses eventos.

Falhas de configuração em ambientes de nuvem, comprometimento de credenciais, *phishing*, concessão excessiva de permissões, indisponibilidade de sistemas, ataques de *ransomware* e incidentes relacionados a fornecedores evidenciam que a gestão de incidentes não se limita à dimensão tecnológica. Quando há comprometimento de dados pessoais, podem surgir obrigações regulatórias, decisões de natureza jurídica, medidas de comunicação com os titulares, necessidade de preservação de evidências e impactos reputacionais, circunstâncias que podem demandar atuação coordenada entre diferentes funções da organização.

Entre as modalidades de incidente, o *ransomware* merece atenção específica pela possível combinação entre indisponibilidade de dados e a possível quebra de confidencialidade, gerando impacto sobre a continuidade do negócio. Em análise publicada em 2026, a Gartner destaca que o *ransomware* continua a provocar interrupções operacionais e perda de receita e que o uso de inteligência artificial amplia a escala, o volume e a sofisticação dessa ameaça (Gartner, 2026).

A dimensão econômica dos incidentes também aparece no "Cost of a Data Breach Report 2025", da International Business Machines Corporation (IBM), que estimou custo médio global de aproximadamente US$ 4,44 milhões por violação de dados. No Brasil, o "Relatório Integrado de Gestão 2025" da Agência Nacional de Proteção de Dados (ANPD) registrou 1.508 comunicações de incidentes entre 2021 e 2025, das quais 362 ocorreram em 2025 (IBM, 2025; ANPD, 2026). Embora esses indicadores não signifiquem que todos os incidentes produzam o mesmo impacto, eles reforçam a necessidade de preparação prévia, capacidade de resposta e resiliência operacional.

No Brasil, esse cenário também é acompanhado por um arcabouço jurídico e regulatório cada vez mais específico. A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018, impõe ao controlador o dever de comunicar à ANPD e aos titulares a ocorrência de incidente que possa acarretar risco ou dano relevante, enquanto a Resolução CD/ANPD nº 15/2024 detalha critérios, conteúdo, prazos e dever de registro. Em paralelo, a Política Nacional de Cibersegurança, instituída pelo Decreto nº 11.856/2023, e a Estratégia Nacional de Cibersegurança (E-Ciber), instituída pelo Decreto nº 12.573/2025, reforçam a centralidade da prevenção, da resiliência e da resposta coordenada a incidentes no ambiente digital brasileiro.

Nesse contexto, a questão central passa a ser como estruturar uma gestão de incidentes que conecte prevenção, detecção, resposta, comunicação e aprendizado sem fragmentar responsabilidades entre segurança da informação, privacidade, jurídico, compliance e negócio. O objetivo deste artigo é apresentar esse ciclo de forma integrada, destacando os controles que precisam existir antes do incidente, as decisões que ganham urgência durante a crise e os registros que permitem demonstrar diligência e sustentar a melhoria contínua após o encerramento do incidente.

Essa abordagem parte da premissa de que prevenção e resposta são dimensões do mesmo sistema de governança. Uma organização pode investir em ferramentas robustas e, ainda assim, responder mal se não souber quem decide, quem comunica, onde estão os registros e quais prazos precisam ser observados. Da mesma forma, um plano de resposta bem escrito perde efetividade quando não está apoiado em inventário, classificação de dados, gestão de acessos, monitoramento, contratos adequados e exercícios periódicos. É justamente a conexão entre essas camadas que sustenta a maturidade da gestão de incidentes.

1. Gestão de incidentes como ciclo de governança

Nesse contexto, a gestão de incidentes deve ser tratada como um processo contínuo e integrado à gestão de riscos da organização. Essa perspectiva é reforçada pelo NIST SP 800-61 Rev. 3, publicado em 2025, que substituiu a versão anterior e passou a alinhar a resposta a incidentes às seis funções do Cybersecurity Framework 2.0: Govern, Identify, Protect, Detect, Respond e Recover. Com isso, a resposta deixa de ser vista como uma atuação isolada, acionada apenas quando o incidente ocorre, e passa a integrar um ciclo mais amplo de governança, prevenção, detecção, resposta e recuperação (NIST, 2025).

Na prática, essa integração significa reconhecer que a capacidade de responder começa muito antes do primeiro alerta de segurança. A governança define papéis e responsabilidades, apetite a risco e critérios de escalonamento; a identificação mapeia ativos, dados, sistemas e terceiros; a proteção implementa controles preventivos; a detecção cria meios de reconhecer as anomalias; a resposta organiza contenção, análise e comunicação; e a recuperação devolve o ambiente à operação com critérios de segurança. Ao final, o aprendizado decorrente do incidente retroalimenta essas funções e permite ajustar controles, processos e responsabilidades.

1.1 Incidente de segurança e incidente envolvendo dados pessoais

Nesse ciclo, uma das primeiras decisões é distinguir o incidente de segurança em sentido amplo daquele que envolve dados pessoais. Nem todo evento de segurança ativa obrigações da LGPD: uma indisponibilidade em sistema que não trate dados pessoais, por exemplo, pode demandar resposta técnica e de continuidade, sem necessariamente exigir comunicação à ANPD. Em sentido inverso, quando dados pessoais são afetados por violação de confidencialidade, integridade, disponibilidade ou autenticidade, o evento precisa ser analisado à luz do regime de proteção de dados.

A orientação operacional atualmente publicada pela ANPD faz uma distinção útil ao esclarecer que a mera existência de uma vulnerabilidade não constitui, por si só, incidente de segurança, embora sua exploração possa resultar em um incidente. Para fins de comunicação, a Agência indica a verificação cumulativa da ocorrência confirmada, do envolvimento de dados pessoais sujeitos à LGPD e da possibilidade de risco ou dano relevante aos titulares.

Sempre que possível, essa avaliação precisa ocorrer logo na triagem, e não apenas depois de concluída a investigação. O fluxo de resposta deve permitir identificar, desde o início, se há dados pessoais envolvidos, direta ou indiretamente. Quando essa informação ainda não puder ser confirmada, a incerteza também deve ser considerada na condução das etapas seguintes da resposta. A demora nessa classificação pode comprometer os prazos aplicáveis, a coleta de informações e a qualidade da comunicação.

Além do regime específico da LGPD, a proteção de dados pessoais possui fundamento constitucional autônomo. A Emenda Constitucional nº 115/2022 incluiu no artigo 5º, LXXIX, o direito à proteção de dados pessoais, inclusive nos meios digitais, e atribuiu à União competência privativa para legislar sobre proteção e tratamento de dados pessoais. Conforme a dinâmica do evento, o mesmo fato também pode atrair a incidência do Marco Civil da Internet e de tipos penais relacionados à invasão de dispositivo informático ou à extorsão.

1.2 Governança preventiva: inventário, classificação, riscos e terceiros

Para que essa resposta ocorra com rapidez, a organização precisa chegar à crise com informações previamente estruturadas. Não deveria ser necessário descobrir, durante o incidente, qual sistema foi afetado, quais dados ele trata, quem é o fornecedor responsável, onde estão os *logs* ou quem possui alçada para interromper uma operação. Por isso, inventário de ativos e dados, registro das operações de tratamento, matriz de criticidade e mapa de dependências, embora usualmente associados à governança, também funcionam como controles de resposta.

Nesse arranjo, o artigo 37 da LGPD exige que controlador e operador mantenham registro das operações de tratamento, enquanto o artigo 38 prevê a possibilidade de elaboração do Relatório de Impacto à Proteção de Dados Pessoais (RIPD). Para que esses instrumentos tenham utilidade prática, precisam orientar decisões concretas. Se o RIPD identifica um tratamento de alto risco, por exemplo, essa conclusão deve se refletir em controles adicionais, limitação de acesso, plano de contingência, retenção definida, testes de segurança ou monitoramento reforçado.

A mesma lógica se aplica à classificação da informação, que permite definir prioridades antes que a crise ocorra. Dados pessoais sensíveis, dados financeiros, credenciais de autenticação, informações protegidas por sigilo e dados de crianças e adolescentes podem elevar o potencial de impacto para os titulares, e a Resolução CD/ANPD nº 15/2024 incorpora parte desses fatores ao juízo de risco ou dano relevante. Quando essa classificação já existe e está atualizada, a análise durante o incidente tende a ser mais rápida e consistente.

Essa estrutura de governança também precisa alcançar terceiros, já que o artigo 39 da LGPD determina que o operador trate os dados segundo as instruções do controlador, a quem cabe verificar a observância dessas instruções e das normas aplicáveis. Na prática, esse dever se traduz em *due diligence*, requisitos mínimos de segurança, definição de responsabilidades, acesso a evidências e obrigação de cooperação. Em incidentes originados em fornecedores, fragilidades contratuais ou de governança costumam aparecer justamente quando o tempo para corrigi-las já é escasso.

1.3 Contratos e o protocolo mínimo de resposta

No plano contratual, essa preparação exige mais do que cláusulas genéricas sobre segurança. Contratos que envolvam tratamento de dados pessoais ou operação de sistemas críticos precisam disciplinar a resposta a incidentes de forma objetiva, especialmente quanto ao prazo de notificação, às informações que devem ser fornecidas, aos canais de emergência e à responsabilidade pela coordenação das comunicações regulatórias.

Para que esse mecanismo funcione mesmo em situações de pressão, um protocolo contratual mínimo deve prever notificação rápida ao controlador, canal de emergência, obrigação de contenção e mitigação, preservação e disponibilização de evidências, cooperação técnica e forense, atualização periódica das informações, repartição de responsabilidades e suporte para comunicações a titulares, reguladores e clientes.

De acordo com a Resolução CD/ANPD nº 15/2024, o controlador dispõe de três dias úteis para comunicar o incidente à ANPD quando estiver configurada a obrigatoriedade de comunicação. Esse prazo é contado a partir do conhecimento, pelo próprio controlador, de que o incidente afetou dados pessoais, de modo que eventual ciência anterior do operador não constitui, por si só, o marco inicial do prazo aplicável ao controlador. Ainda assim, para evitar atrasos na cadeia de comunicação e preservar tempo suficiente para a análise do incidente, a avaliação dos riscos envolvidos e a definição das providências necessárias, é recomendável que o contrato estabeleça prazo interno mais curto para que o operador reporte a ocorrência ao controlador. A ANPD orienta, ainda, que o operador informe o controlador sem demora injustificada e forneça as informações necessárias à comunicação à Agência e aos titulares, recomendando que essas obrigações sejam previstas contratualmente para tornar o procedimento mais ágil e reduzir os riscos aos titulares.

Nas transferências internacionais realizadas com base nas cláusulas-padrão contratuais, a Resolução CD/ANPD nº 19/2024 também estabelece obrigações específicas relacionadas à resposta a incidentes. Nesses casos, cabe à parte designada comunicar à ANPD e aos titulares a ocorrência de incidente que possa acarretar risco ou dano relevante, observando o prazo de três dias úteis previsto na regulamentação. Essa previsão reforça a importância de que as responsabilidades relacionadas à gestão e à comunicação de incidentes estejam claramente definidas nos instrumentos contratuais utilizados na transferência internacional de dados.

1.4 Controles técnicos, cultura e fator humano

A governança precisa estar acompanhada de controles técnicos e organizacionais compatíveis com os riscos envolvidos, de modo que fortaleça a prevenção e dê suporte à resposta a incidentes. A definição desses controles deve considerar as características do ambiente, a criticidade dos ativos, a natureza dos dados tratados, a superfície de ataque, os riscos identificados e os possíveis impactos decorrentes de uma indisponibilidade ou comprometimento.

Nesse contexto, podem ser adotadas, entre outras medidas, autenticação multifator, princípio do menor privilégio, segmentação de rede, gestão de vulnerabilidades, criptografia, manutenção de cópias de segurança íntegras e testadas, registro de eventos e monitoramento contínuo. A escolha e o nível de implementação desses controles não devem decorrer de uma lista padronizada de ferramentas, mas de uma avaliação proporcional ao risco e às necessidades da organização.

Embora direcionado a agentes de tratamento de pequeno porte, o "Guia Orientativo de Segurança da Informação" da ANPD oferece uma referência útil ao recomendar, entre outras medidas, política de segurança da informação, revisão periódica de controles, gestão de acessos, tratamento de vulnerabilidades, cópias de segurança, treinamento e definição de requisitos contratuais. Em organizações de maior porte ou com operações mais complexas, essas medidas devem ser adaptadas e aprofundadas de acordo com a escala, a criticidade e os riscos associados às atividades de tratamento.

Entre esses controles, os *logs* merecem atenção especial porque ajudam tanto a detectar comportamentos anômalos quanto a reconstruir a cronologia do evento durante a investigação. O Marco Civil da Internet disciplina a guarda de registros de acesso a aplicações e admite sua requisição judicial para formação de conjunto probatório, enquanto o Decreto nº 8.771/2016 detalha diretrizes de segurança relacionadas à guarda, ao armazenamento e ao tratamento de registros, dados pessoais e comunicações privadas. A ausência de *logs* também repercute na análise regulatória: em processos administrativos sancionadores, a ANPD já considerou a falta de registros de acesso, ou de outras evidências técnicas equivalentes, deve levar a organização a examinar o incidente sob a hipótese mais desfavorável, uma vez que não há elementos em sentido contrário que a afastem[1].

Ainda assim, controles tecnológicos não substituem o componente humano, que deve ser considerado no próprio desenho da prevenção. Treinamentos anuais isolados têm alcance limitado; programas mais maduros combinam conscientização contínua, simulações, comunicação de ameaças, revisão de acessos, processos de desligamento, canais simples de reporte e um ambiente que incentive o relato precoce de erros. A ANPD, inclusive, recomenda que a organização estimule usuários a informar incidentes e vulnerabilidades detectadas. Quanto mais cedo um colaborador reporta um envio indevido, um clique suspeito ou uma credencial exposta, maior tende a ser a possibilidade de contenção.

Nesse desenho, o encarregado desempenha um papel relevante. A Resolução CD/ANPD nº 18/2024 regulamenta sua atuação e trata do conflito de interesses, enquanto o "Guia Orientativo sobre a Atuação do Encarregado"

[1] BRASIL. Autoridade Nacional de Proteção de Dados (ANPD). Decisões em processos sancionadores. *ANPD*, Brasília, [2026]. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/decisoes-em-processos-sancionadores. Acesso em: 21 set. 2026.

acrescenta uma dimensão prática especialmente importante para incidentes: o Encarregado pode integrar equipes especializadas de resposta e tratamento de incidentes e orientar essas equipes quanto ao registro e à comunicação de ocorrências envolvendo dados pessoais. Ao mesmo tempo, o guia reforça que as decisões sobre o tratamento permanecem sob responsabilidade do controlador. A estrutura organizacional deve, portanto, permitir assessoramento técnico efetivo sem transformar o Encarregado no responsável exclusivo pela decisão ou pela conformidade.

1.5 Detecção, triagem e classificação de severidade

Quando o alerta surge, detecção e triagem exigem que a organização aja mesmo com informação incompleta. Esperar por absoluta certeza para preservar evidências, revogar credenciais ou isolar um ativo pode ampliar o dano; por isso, o fluxo de resposta deve admitir medidas preliminares proporcionais enquanto a investigação avança.

À medida que o incidente é confirmado, a classificação de severidade precisa considerar mais do que o volume de registros afetados. A orientação atual da ANPD destaca, entre outros fatores, o contexto da atividade de tratamento, as categorias e quantidades de titulares afetados, a natureza e a quantidade de dados violados, os potenciais danos materiais, morais e reputacionais, a existência de proteção capaz de impedir a identificação dos titulares e a suficiência das medidas de mitigação adotadas. Esses elementos podem ser combinados com duração da exposição, reversibilidade, facilidade de uso indevido, impacto operacional e presença de grupos vulneráveis, de modo que a avaliação reflita as características concretas do evento, e não apenas uma pontuação automática.

Como a investigação é progressiva, essa classificação também precisa admitir revisão. Um evento inicialmente considerado restrito pode se revelar mais amplo à medida que *logs*, evidências ou informações de terceiros são analisados. Sempre que houver reclassificação, convém registrar a data, o responsável, o fundamento e as consequências da mudança, formando um histórico capaz de demonstrar os motivos que fundamentaram a comunicação ou a sua ausência pela organização, bem como eventuais mudanças na estratégia de resposta.

1.6 Plano de resposta e sala de crise

Para dar suporte a esse fluxo decisório, o plano de resposta a incidentes que envolvem dados pessoais precisa ser suficientemente objetivo para ser usado durante a crise e suficientemente completo para reduzir improvisos. Mais do que o número de páginas, é importante que contenha critérios de acionamento, papéis, alçadas, matriz de escalonamento, contatos alternativos, *checklists* para as primeiras horas, critérios de comunicação, fornecedores de suporte e regras de encerramento.

Para fins de organização da análise, as funções de Segurança da Informação, Privacidade, Jurídico, Compliance, Comunicação e Negócio estão apresentadas neste artigo como áreas distintas. Essa referência, contudo, não pressupõe a existência de estruturas organizacionais autônomas para cada uma dessas atividades. A distribuição de responsabilidades deve ser compreendida de acordo com a realidade de cada organização, considerando seu porte, seu modelo de governança e sua estrutura interna, de modo que diferentes atribuições possam estar concentradas em uma mesma área, função ou profissional.

A execução desse plano de resposta, por sua vez, exige atuação multidisciplinar. Como exemplo de organização, Segurança e Tecnologia da Informação podem conduzir a contenção e a análise técnica; as funções de Privacidade e Jurídico podem avaliar os dados afetados, as obrigações legais e regulatórias e os aspectos contratuais; Comunicação pode estruturar o envio das comunicações aos titulares e às demais partes afetadas; a área de negócio afetada pode indicar a criticidade e os impactos operacionais; Riscos e Compliance podem acompanhar a aderência a políticas e normativos internos da instituição; e a Alta Administração pode ser acionada quando as decisões envolverem continuidade, reputação ou exposição financeira.

Esse arranjo deve ser entendido como uma referência possível, a ser adaptada ao porte, à estrutura e ao modelo de governança de cada organização. As atribuições podem estar distribuídas de forma distinta, inclusive con-

centradas em uma mesma área, função ou profissional, desde que estejam claramente definidas as responsabilidades e as alçadas necessárias para a resposta ao incidente.

A partir dessa definição de responsabilidades, também é importante estabelecer previamente como serão tomadas as decisões durante a resposta ao incidente. Medidas como interromper um sistema crítico, contratar suporte pericial em caráter emergencial, realizar comunicações a reguladores ou clientes ou adotar ações de continuidade podem envolver diferentes funções e níveis de decisão. Quando essas responsabilidades não estão claramente definidas, podem surgir dúvidas, sobreposições de atuação ou divergências quanto à condução das providências necessárias. Por isso, as decisões consideradas relevantes no plano de resposta devem ter responsáveis definidos, substitutos previstos e níveis de aprovação compatíveis com sua criticidade, permitindo uma atuação mais coordenada e célere durante a crise.

A efetividade desse desenho também depende de sua validação prática. Nesse sentido, exercícios de resposta a incidentes podem ser utilizados para testar, em cenários simulados, papéis, fluxos de comunicação, alçadas e recursos previstos no plano. Essas simulações permitem verificar, antes de uma situação real, se os procedimentos definidos são aplicáveis e se as pessoas envolvidas conhecem suas responsabilidades. Cenários envolvendo vazamento de dados, incidentes com *ransomware*, comprometimento de fornecedores ou indisponibilidade de sistemas podem revelar fragilidades que nem sempre são identificadas apenas pela revisão documental.

1.7 Contenção, erradicação, recuperação e particularidades do incidente com *ransomware*

Uma vez confirmado e classificado o incidente, a contenção busca limitar a continuidade do dano e pode envolver isolamento de equipamentos, revogação de credenciais, bloqueio de contas, interrupção de integrações, restrição de tráfego ou suspensão parcial de serviços. A escolha deve ser proporcional ao contexto: algumas situações justificam desligamento imediato, enquanto outras permitem contenção segmentada para evitar impacto desnecessário no negócio.

Depois de contida a ameaça, a erradicação precisa remover a causa do comprometimento, seja ela *malware*, vulnerabilidade explorada, configuração indevida, credencial exposta ou persistência do atacante. A recuperação, por sua vez, deve ocorrer a partir de ambiente confiável, com validação de integridade e monitoramento reforçado, porque restabelecer o serviço não é o mesmo que demonstrar que a ameaça foi efetivamente eliminada.

Dentro desse conjunto, o *ransomware* exige atenção adicional porque pode combinar indisponibilidade, criptografia, exfiltração, extorsão e destruição de evidências. A Gartner observa que essa ameaça continua a interromper operações e comprometer receitas e que o emprego de inteligência artificial amplia sua escala, seu volume e sua sofisticação, reforçando a necessidade de bases preventivas sólidas e capacidade operacional de resposta (Gartner, 2016). Sob a ótica penal, conforme a dinâmica concreta, o evento pode envolver invasão de dispositivo informático e, quando houver exigência de vantagem mediante grave ameaça, hipóteses relacionadas à extorsão, sem prejuízo de outros enquadramentos.

Além das medidas técnicas de contenção e recuperação, a resposta ao incidente também deve considerar a preservação de evidências e, quando necessário, a adoção de medidas extrajudiciais ou judiciais voltadas à identificação dos responsáveis. Nesse contexto, o Marco Civil da Internet permite à parte interessada requerer judicialmente o fornecimento de registros para formação de conjunto probatório e estabelece, para determinados provedores de aplicações, o dever de guarda dos registros de acesso pelo prazo de seis meses.

As limitações na preservação ou obtenção de evidências podem dificultar a confirmação de eventual exfiltração de dados em incidentes de *ransomware*, especialmente quando o ataque compromete ou destrói registros relevantes para a investigação. Nessas situações, a avaliação sobre a necessidade de comunicação aos titulares deve considerar os critérios previstos na LGPD e na Resolução CD/ANPD nº 15/2024, bem como as informações efetivamente disponíveis, as limitações identificadas na apuração e os elementos reunidos ao longo da investigação.

Quando não for possível determinar com segurança a extensão do comprometimento, a organização deve registrar as limitações identificadas, os elementos considerados na avaliação do risco ou dano relevante e os fundamentos que sustentaram a decisão adotada. Essa documentação é especialmente importante para demonstrar a diligência empregada na análise do incidente e permitir a revisão da decisão caso novas evidências sejam posteriormente identificadas.

1.8 LGPD e Resolução CD/ANPD nº 15/2024: quando e como comunicar

Do ponto de vista regulatório, o artigo 48 da LGPD estabelece o dever do controlador de comunicar à ANPD e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante. A Resolução CD/ANPD nº 15/2024 detalha esse procedimento e fixa, como regra, o prazo de três dias úteis para a comunicação, contado do conhecimento de que o incidente afetou dados pessoais e pode acarretar risco ou dano relevante, além de admitir a complementação posterior de informações nas hipóteses e nos prazos previstos no próprio regulamento. Por isso, a comunicação não deve ser tratada como um simples formulário regulatório. Ela precisa refletir o estado real da investigação, separar fatos de hipóteses, descrever dados e titulares afetados, riscos identificados, medidas técnicas e administrativas existentes, providências adotadas e recomendações aos titulares. Quando ainda houver incerteza, o mais adequado é registrá-la como tal, em vez de preencher lacunas com suposições.

Se, após a análise, a organização concluir que o incidente não precisa ser comunicado, ainda assim permanece o dever de documentá-lo. A Resolução CD/ANPD nº 15/2024 exige a manutenção do registro por pelo menos cinco anos, de forma que seja possível reconstruir a ocorrência, a avaliação de risco, a decisão tomada e as medidas adotadas. Em termos de governança, a decisão de não comunicar precisa ser tão bem fundamentada quanto a decisão de comunicar.

Essa documentação ganha relevância adicional porque a atuação da ANPD não depende exclusivamente da iniciativa do controlador. As orientações atuais da Agência esclarecem que pode ser instaurado procedimento de apuração de incidente de segurança (PAI) quando ela tome conhecimento, por outra via, de evento potencialmente comunicável que não tenha sido reportado, com possibilidade de requisição de informações e determinação posterior de comunicação à Agência e aos titulares. A mesma página institucional registra que a comunicação voluntária demonstra transparência, cooperação e boa-fé e pode ser considerada em eventual ação fiscalizatória.

Há, ainda, tratamento diferenciado para agentes de tratamento de pequeno porte. A Resolução CD/ANPD nº 2/2022, considerada a alteração promovida pela Resolução CD/ANPD nº 15/2024, prevê prazo em dobro para a comunicação de incidentes nos termos do regulamento específico. Essa flexibilização, contudo, não elimina o dever de análise nem justifica postergar medidas de contenção e investigação.

A lógica de prestação de contas também aparece na dosimetria. A Resolução CD/ANPD nº 4/2023 prevê, para a multa simples, circunstâncias atenuantes relacionadas à implementação de políticas de boas práticas e governança, à adoção de medidas de mitigação e à cooperação ou boa-fé. Isso reforça uma conexão importante para este artigo: a governança estruturada antes e durante o incidente pode produzir efeitos concretos na avaliação administrativa posterior.

1.9 Comunicação coordenada: titulares, reguladores, clientes e mercado

Quando a comunicação do incidente for necessária, sua realização não implica, por si só, reconhecimento de responsabilidade. Seu objetivo é cumprir as obrigações aplicáveis, contribuir para a mitigação dos riscos e fornecer aos titulares informações relevantes sobre o ocorrido. A mensagem aos titulares deve ser clara, direta e útil, explicando o que ocorreu, quais dados podem ter sido afetados, quais riscos são relevantes, o que a organização já fez e quais providências a pessoa pode adotar. A orientação atual da ANPD privilegia a comunicação individual e direta sempre que possível, preferencialmente pelo canal já utilizado na relação com o titular; a comunicação indireta, por publicação em meios de comunicação, é tratada como medida excepcional e deve ser justificada. Além disso, a Agência também pode solicitar ao controlador cópia da comunicação enviada aos titulares para fins de fiscalização.

Além das obrigações previstas na LGPD, determinados setores estão sujeitos a regras específicas para a comunicação de incidentes. No caso do Pix, por exemplo, a Resolução BCB nº 342/2023 introduziu no Regulamento do Pix a obrigação de comunicar às pessoas naturais titulares de contas transacionais a ocorrência de incidentes de segurança com dados pessoais envolvendo banco de dados relacionado a componente ou à infraestrutura do Pix. Essa comunicação deve ocorrer mesmo quando o participante que mantém a conta não tiver sido o responsável pelo incidente e ainda que o evento não possa acarretar risco ou dano relevante aos titulares, estabelecendo, nesse aspecto, um dever de comunicação mais amplo do que o previsto de forma geral na LGPD.

Para evitar inconsistências sobre o mesmo fato e manter a coerência das informações, especialmente quando o incidente gera diferentes obrigações de comunicação, é importante que a organização trabalhe a partir de uma base comum e previamente validada. Essa base deve reunir, entre outros elementos, a cronologia do incidente, os fatos já confirmados, os pontos ainda em investigação, os sistemas envolvidos, os titulares afetados e as medidas adotadas. A partir dessas informações, cada comunicação pode ser ajustada ao respectivo destinatário, preservando a consistência das informações sobre o evento.

1.10 Investigação, evidências e cadeia de custódia

A coordenação da resposta também depende de uma investigação capaz de atender, simultaneamente, a finalidades técnicas e jurídico-probatórias. É necessário compreender causa-raiz e extensão do incidente, mas também preservar elementos que possam sustentar defesa administrativa ou judicial, acionamento de seguro, execução contratual e eventual responsabilização de terceiros.

Nesse contexto, *logs*, registros de acesso, imagens forenses, alertas, comunicações internas, registros de fornecedores e evidências de alteração de configurações, por exemplo, devem ser preservados com método. Sempre que possível, a coleta precisa registrar quem realizou o procedimento, quando, de qual fonte, onde o material foi armazenado e quais controles preservam sua integridade. A cadeia de custódia, portanto, deve ser considerada desde o momento em que a organização identifica que determinada evidência poderá ser relevante para a investigação ou para eventual apuração administrativa ou judicial, de modo que seja possível demonstrar sua origem, integridade e histórico de tratamento.

Para que a investigação produza melhoria concreta, a análise de causa-raiz também precisa ir além de conclusões genéricas como "erro humano", "falha do fornecedor" ou "ataque sofisticado". O foco deve estar no controle que faltou ou falhou: autenticação multifator, segregação, gestão de mudança, revisão de acesso, monitoramento ou aplicação de correção, por exemplo. É esse nível de especificidade que permite transformar a investigação em um plano de ação mensurável.

1.11 Aprendizado pós-incidente e melhoria contínua

Depois da estabilização do ambiente e do cumprimento das comunicações necessárias, a resposta ainda precisa passar por uma revisão estruturada. É nesse momento que a organização deve avaliar se o incidente poderia ter sido evitado com controles já conhecidos, se a detecção ocorreu no tempo esperado, se o plano foi seguido, quais informações ou recursos fizeram falta, se houve gargalos decisórios e se os fornecedores responderam como previsto contratualmente.

O resultado dessa revisão precisa ser convertido em ações com responsável, prazo e critério de conclusão, alcançando não apenas o ativo diretamente afetado, mas também ambientes semelhantes. Se o incidente decorreu de permissão excessiva em um sistema, por exemplo, a correção não deve se limitar àquele caso; é necessário verificar onde o mesmo padrão pode estar reproduzido na organização.

Para acompanhar se essas medidas produzem efeito, indicadores como tempo de detecção, tempo de contenção, percentual de incidentes identificados internamente, reincidência por causa-raiz, cumprimento de prazos e conclusão de planos de ação ajudam a medir a evolução da maturidade. A alta administração não precisa receber detalhes de cada alerta, mas deve ter visibilidade sobre tendências, riscos aceitos e eficácia das medidas corretivas.

Considerações finais

A gestão de incidentes e vazamentos de dados pessoais deve ser compreendida como um processo contínuo de governança, que articula prevenção, detecção, resposta, comunicação e aprendizado. Ao longo desse ciclo, a capacidade de resposta não depende apenas da existência de um plano formal, mas também da qualidade das informações disponíveis, da definição prévia de responsabilidades e alçadas, da adoção de controles proporcionais aos riscos, da preparação dos fornecedores e da preservação adequada de evidências.

Quando o incidente envolve dados pessoais, essa estrutura precisa ainda estar preparada para incorporar as exigências específicas da LGPD e da Resolução CD/ANPD nº 15/2024. A avaliação do risco ou dano relevante, a observância dos prazos de comunicação, a documentação das decisões e a manutenção dos registros do incidente exigem coordenação entre diferentes funções da organização e capacidade de atuação mesmo quando a investigação ainda não está concluída. Nesse contexto, tanto a decisão de comunicar quanto a de não comunicar devem estar apoiadas em elementos verificáveis e em uma análise devidamente documentada.

A experiência prática demonstra, ainda, que parte relevante da efetividade da resposta é construída antes da ocorrência do incidente. Inventários atualizados, definição de papéis, contratos adequados, mecanismos de monitoramento, canais de comunicação, exercícios de resposta e critérios de escalonamento reduzem a dependência de decisões improvisadas durante a crise. Da mesma forma, a análise posterior do incidente deve permitir identificar falhas de controle, revisar processos e evitar que a organização apenas restabeleça a operação sem tratar as causas que contribuíram para o evento.

A maturidade da gestão de incidentes, portanto, não está na expectativa de eliminar completamente sua ocorrência, mas na capacidade da organização de identificar os incidentes, limitar seus impactos, proteger os titulares, fundamentar as decisões adotadas e reduzir a possibilidade de recorrência. É essa capacidade que transforma a gestão de incidentes em componente efetivo da governança corporativa.

Referências

BRASIL. Agência Nacional de Proteção de Dados. *Comunicação de Incidente de Segurança*. Publicado em 23 dez. 2022; atualizado em 26 ago. 2026. Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis. Acesso em: 18 set. 2026.

BRASIL. Agência Nacional de Proteção de Dados. *Relatório Integrado de Gestão 2025*. Brasília, DF, 2026.

BRASIL. Autoridade Nacional de Proteção de Dados. *Guia Orientativo sobre Segurança da Informação para Agentes de Tratamento de Pequeno Porte. Versão 1.0*. Brasília, DF, 2021. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia_seguranca_da_informacao_para_atpps___defeso_eleitoral.pdf/@@display-file/file. Acesso em: 22 out. 2026.

BRASIL. Autoridade Nacional de Proteção de Dados. *Resolução CD/ANPD nº 2, de 27 de janeiro de 2022*. Regulamento de aplicação da Lei nº 13.709/2018 para agentes de tratamento de pequeno porte. Brasília, DF, 2022. Disponível em: https://www.gov.br/anpd/pt-br/acesso-a-informacao/institucional/atos-normativos/regulamentacoes_anpd/resolucao-cd-anpd-no-2-de-27-de-janeiro-de-2022. Acesso em: 22 out. 2026.

BRASIL. Autoridade Nacional de Proteção de Dados. *Resolução CD/ANPD nº 4, de 24 de fevereiro de 2023*. Regulamento de Dosimetria e Aplicação de Sanções Administrativas. Brasília, DF, 2023. Disponível em: https://www.gov.br/anpd/pt-br/acesso-a-informacao/institucional/atos-normativos/regulamentacoes_anpd/resolucao-cd-anpd-no-4-de-24-de-fevereiro-de-2023. Acesso em: 22 out. 2026.

BRASIL. Autoridade Nacional de Proteção de Dados. *Resolução CD/ANPD nº 15, de 24 de abril de 2024*. Regulamento de Comunicação de Incidente de Segurança. Brasília, DF, 24 abr. 2024. Disponível em: https://www.gov.br/anpd/pt-br/acesso-a-informacao/institucional/atos-normativos/regulamentacoes_anpd/resolucao-cd-anpd-no-15-de-24-de-abril-de-2024. Acesso em: 22 out. 2026.

BRASIL. Autoridade Nacional de Proteção de Dados. *Resolução CD/ANPD nº 18, de 16 de julho de 2024*. Regulamento sobre a atuação do encarregado pelo tratamento de dados pessoais. Brasília, DF, 16 jul. 2024. Disponível em: https://www.gov.br/anpd/pt-br/acesso-a-informacao/institucional/atos-normativos/regulamentacoes_anpd/resolucao-cd-anpd-no-18-de-16-de-julho-de-2024. Acesso em: 22 out. 2026.

BRASIL. Autoridade Nacional de Proteção de Dados. *Resolução CD/ANPD nº 19, de 23 de agosto de 2024*. Regulamento de Transferência Internacional de Dados e cláusulas-padrão contratuais. Brasília, DF, 23 ago. 2024. Disponível em: https://www.gov.br/anpd/pt-br/acesso-a-informacao/institucional/atos-normativos/regulamentacoes_anpd/resolucao-cd-anpd-no-19-de-23-de-agosto-de-2024. Acesso em: 22 out. 2026.

BRASIL. Autoridade Nacional de Proteção de Dados. *Guia Orientativo: Atuação do Encarregado pelo Tratamento de Dados Pessoais*. Brasília, DF, 2024. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-lanca-guia-sobre-atuacao-do-encarregado. Acesso em: 22 out. 2026.

BRASIL. Banco Central do Brasil. *Resolução BCB nº 342, de 26 de setembro de 2023*. Altera o Regulamento do Pix para dispor sobre a comunicação aos titulares da ocorrência de incidente de segurança com dados pessoais, e altera os Anexos I e II à Resolução BCB nº 177, de 22 de dezembro de 2021 (Manual de Penalidades do Pix), para dispor sobre o descumprimento de requisitos técnicos de segurança do Pix e sobre os critérios para aplicação de penalidades. Brasília, DF: Banco Central do Brasil, 2023. Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?numero=342&tipo=resolu%C3%A7%C3%A3o+bcb. Acesso em: 22 out. 2026.

BRASIL. *Decreto-Lei nº 2.848, de 7 de dezembro de 1940*. Código Penal. Brasília, DF: Presidência da República, 1940. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 22 out. 2026.

BRASIL. *Lei nº 12.965, de 23 de abril de 2014*. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 22 out. 2026.

BRASIL. *Decreto nº 8.771, de 11 de maio de 2016*. Regulamenta a Lei nº 12.965, de 23 de abril de 2014, 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações. Brasília, DF: Presidência da República, 2016. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8771.htm. Acesso em: 22 out. 2026.

BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 22 out. 2026.

BRASIL. *Decreto nº 11.856, de 26 de dezembro de 2023*. Institui a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança. Brasília, DF: Presidência da República, 2023. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/d11856.htm. Acesso em: 22 out. 2026.

BRASIL. *Decreto nº 12.573, de 4 de agosto de 2025*. Institui a Estratégia Nacional de Cibersegurança – E-Ciber. Brasília, DF: Presidência da República, 2025. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/decreto/d12573.htm. Acesso em: 22 out. 2026.

GARTNER. Cybersecurity threat: ransomware/extortionware. *Gartner*, [*S. l.*], 28 maio 2026. Disponível em: https://www.gartner.com/en/documents/7814417. Acesso em: 22 out. 2026.

INTERNATIONAL BUSINESS MACHINES CORPORATION (IBM). *Cost of a data breach report 2025*. [S. l.]: IBM, 2025.

NIST. *Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile*. Gaithersburg, MD: NIST, 2025. (NIST SP 800-61, Rev. 3).

Cyber compliance:

a convergência entre segurança da informação, LGPD e integridade

Rodrigo Emídio Coutinho

Rodrigo Emídio Coutinho tem mais de 20 anos de carreira, construiu sua trajetória nas áreas de Compliance, Privacidade de Dados e Enterprise Risk Management, ocupando posições de liderança nos últimos seis anos. Antes de ingressar no Sistema Firjan, dedicou 11 anos à TIM Brasil, onde conduziu programas integrados de Privacidade de Dados, Compliance e de Gestão de Riscos Corporativos. Atualmente, é gestor de Compliance e responsável pelo Núcleo de Privacidade do Sistema Firjan, liderando o Programa de Integridade Corporativa, com atuação que abrange estruturação de políticas, capacitações corporativas, controles, diagnósticos de maturidade e resposta a incidentes. É certificado em Privacidade e Proteção de Dados pela ISACA (CDPSE).

Introdução

A transformação digital trouxe para as organizações um conjunto de riscos que já não cabe dentro das fronteiras tradicionais da tecnologia da informação. Ataques de *ransomware*, vazamentos de dados em larga escala, fraudes digitais e interferências em infraestruturas críticas deixaram de ser eventos excepcionais e passaram a fazer parte do cotidiano corporativo, com impactos financeiros, regulatórios e reputacionais consideráveis. Quem atua na área percebe, no dia a dia, que a aproximação entre Compliance, Segurança da Informação e Proteção de Dados deixou de ser uma escolha estratégica: tornou-se condição de sobrevivência organizacional.

O conceito de "Cyber Compliance" surge para dar nome a esse movimento de integração. Trata-se de um modelo de governança que busca alinhar ética, integridade, proteção de dados, segurança da informação, gestão de riscos e estratégia empresarial em uma abordagem única e estruturada. A diferença em relação às iniciativas isoladas de conformidade regulatória ou de proteção tecnológica está justamente aí: no Cyber Compliance, essas disciplinas não operam em paralelo nem competem entre si; elas se sustentam mutuamente e são igualmente essenciais.

No Brasil, a Lei Geral de Proteção de Dados Pessoais (LGPD) (Lei nº 13.709/2018) e a atuação cada vez mais presente da Agência Nacional de Proteção de Dados (ANPD), sobretudo após a publicação da Resolução CD/ANPD nº 15/2024, que regulamentou os procedimentos de comunicação de incidentes de segurança, deram nova urgência ao tema, reforçada pela Lei nº 15.352/2026, que transformou a ANPD em agência reguladora, ampliando sua autonomia e sua capacidade de fiscalização. No cenário internacional, o movimento é o mesmo: a publicação do "NIST Cybersecurity Framework 2.0" (2024), a entrada em vigor da Diretiva NIS2 e do Digital Operational Resilience Act (DORA) na União Europeia e o Regulamento Europeu de Inteligência Artificial (AI Act, 2024) mostram que a regulação do ambiente cibernético avança em ritmo acelerado em praticamente todas as jurisdições relevantes.

É diante desse cenário que este artigo se propõe a examinar a convergência entre segurança da informação, proteção de dados e compliance sob a perspectiva do Cyber Compliance. O percurso passa pelos fundamentos conceituais do tema, pelos instrumentos práticos de implementação e pelo papel decisivo da alta administração e da cultura organizacional nesse processo. A análise combina a literatura técnica e acadêmica internacional com a experiência regulatória brasileira, na tentativa de oferecer subsídios úteis a líderes corporativos e a profissionais de compliance, governança, auditoria e gestão de riscos.

1. Desenvolvimento

1.1 Evolução do conceito de *Cyber Compliance*

O termo "Cyber Compliance" ainda não encontrou uma definição única na literatura. É possível compreendê-lo, contudo, como o conjunto integrado de políticas, controles, processos, tecnologias e comportamentos voltado a garantir que a organização opere em conformidade com as obrigações legais e regulatórias aplicáveis ao ambiente digital, protegendo seus ativos de informação, respeitando os direitos dos titulares de dados e preservando sua integridade ética.

Nem sempre foi assim. Compliance e segurança da informação se desenvolveram, historicamente, como disciplinas independentes. O compliance, de matriz norte-americana e consolidado após os escândalos corporativos das décadas de 1990 e 2000, concentrava-se na prevenção de fraudes, corrupção e violações normativas. A segurança da informação, por sua vez, nasceu como subdisciplina da Tecnologia da Informação, organizada em torno da tríade clássica de Confidencialidade, Integridade e Disponibilidade (CID).

Esse modelo foi se rompendo aos poucos, na medida em que os dados pessoais e corporativos se tornaram o ativo mais valioso, e mais visado, das organizações. O Regulamento Geral de Proteção de Dados da União Europeia (GDPR, 2016) representou um ponto de inflexão:

com sua lógica de *accountability* e de responsabilização dos controladores, aprofundou e tornou mais explícita a integração entre obrigações técnicas e organizacionais na proteção de dados, já delineada na Diretiva 95/46/CE, obrigando as áreas jurídica, de TI e de compliance a trabalharem de maneira coordenada.

No plano dos *frameworks* de boas práticas, o "NIST Cybersecurity Framework" já apontava, desde a versão original de 2014, para a necessidade de integração entre governança, riscos e controles técnicos. A versão 2.0, publicada em fevereiro de 2024, deu um passo além ao introduzir a função "governança" como eixo central do *framework*, deixando claro que a gestão de riscos cibernéticos é responsabilidade de toda a organização, e não apenas das equipes técnicas.

Segundo o NIST, o CSF 2.0 "oferece uma taxonomia de resultados de cibersegurança de alto nível que pode ser utilizada por qualquer organização, independentemente de seu tamanho, setor ou maturidade, para melhor compreender, avaliar, priorizar e comunicar seus esforços de cibersegurança" (Pascoe; Quinn; Scarfone, 2024, tradução livre)[1]. A escolha não é trivial: ao empregar o verbo comunicar, o documento admite que a gestão de riscos cibernéticos tem uma dimensão de governança que vai além da técnica e se aproxima do campo do compliance e da gestão estratégica.

1.2 A convergência entre compliance, segurança da informação e proteção de dados

Essa convergência não é um exercício acadêmico; ela é empurrada por forças bastante concretas. No campo regulatório, LGPD, GDPR, NIS2 e DORA criam obrigações que nenhuma área consegue cumprir sozinha: jurídico, TI, compliance e operações precisam atuar em conjunto. No campo dos riscos, um mesmo incidente, um ataque de *ransomware*, por exemplo, poderia configurar ao mesmo tempo violação de segurança da informação, incidente com dados pessoais sujeito a notificação regulatória e evento com potencial repercussão em matéria de integridade e anticorrupção, quando envolve terceiros ou a cadeia de fornecimento de uma organização.

A ISO 37301:2021, que estabelece os requisitos para Sistemas de Gestão de Compliance, reconhece que as obrigações de conformidade de uma organização não se limitam aos requisitos legais e regulatórios, alcançando também normas técnicas e compromissos voluntários (ISO, 2021)[2]. Quando lida em conjunto com a ISO/IEC 27001:2022 e a ISO/IEC 27701:2025, o resultado é um sistema integrado de gestão capaz de cobrir conformidade regulatória, segurança da informação e privacidade sob uma mesma arquitetura.

A ISO 27701 talvez seja o exemplo mais claro da materialização normativa dessa convergência. Concebida em 2019 como extensão da ISO 27001 voltada à gestão de informações de privacidade (Privacy Information Management System – PIMS), a norma foi profundamente revisada e, na edição publicada em outubro de 2025, tornou-se um padrão autônomo e certificável de forma independente, sem exigir a implementação prévia de um Sistema de Gestão de Segurança da Informação (SGSI) baseado na ISO 27001. Em qualquer de suas versões, a norma constrói pontes explícitas entre os controles de segurança da informação e as obrigações de proteção de dados pessoais, e sua adoção por empresas brasileiras é um caminho concreto para evidenciar governança e *accountability* perante a ANPD, ainda que não constitua, por si só, demonstração de conformidade com a LGPD.

Na prática, a convergência aparece quando o processo de resposta a incidentes de segurança passa a incluir, de forma automática, a avaliação de impacto sobre dados pessoais, a ativação do fluxo de notificação regulatória e a comunicação corporativa integrada. Funções que antes eram acionadas em silos, uma após a outra, passam a operar como um único processo.

[1] PASCOE, C.; QUINN, S.; SCARFONE, K. The NIST cybersecurity framework (CSF) 2.0. Gaithersburg, MD: National Institute of Standards and Technology, 2024. DOI: https://doi.org/10.6028/NIST.CSWP.29.

[2] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). *ISO 37301:2021*: compliance management systems — requirements with guidance for use. Geneva: International Organization for Standardization, 2021.

1.3 LGPD como instrumento de governança digital

A Lei nº 13.709/2018 não deve ser lida apenas como um diploma regulatório de privacidade. Em sua estrutura e em seus mecanismos, a LGPD é um instrumento de governança digital: impõe às organizações um ciclo contínuo de gestão, que envolve planejar o tratamento de dados com base legal adequada, implementar medidas técnicas e organizacionais de segurança, monitorar riscos e incidentes e, por fim, demonstrar conformidade, como determina o princípio da responsabilização e prestação de contas, associado à noção de *accountability* (artigo 6º, X, da LGPD).

Danilo Doneda, um dos principais teóricos brasileiros da proteção de dados, já advertia que a privacidade, em sua evolução contemporânea, transcende a dimensão individual para se constituir em valor social e coletivo, a exigir proteção sistêmica, e não apenas reativa (Doneda, 2019)[3]. Essa perspectiva ajuda a entender por que o cumprimento da LGPD não pode ficar restrito à área jurídica: ele pede uma abordagem organizacional sistêmica, muito próxima do que se espera de um programa de compliance maduro.

Laura Schertel Mendes, outra referência central no debate brasileiro, sustenta que a proteção de dados pessoais constitui direito fundamental autônomo, ligado à autodeterminação informativa, à dignidade e à liberdade (Mendes, 2014)[4]. Esse enquadramento constitucional, confirmado pelo Supremo Tribunal Federal no julgamento das ADIs 6387, 6388, 6389, 6390 e 6393 e depois incorporado ao texto da Constituição pela Emenda Constitucional nº 115/2022, impõe ao setor empresarial o reconhecimento de que a conformidade com a LGPD é, antes de tudo, uma responsabilidade ética, e não apenas técnica ou jurídica.

A Resolução CD/ANPD nº 15/2024, que aprovou o Regulamento de Comunicação de Incidente de Segurança, deu contornos mais precisos às obrigações dos controladores. O regulamento define incidente de segurança como qualquer evento adverso confirmado que viole as propriedades de confidencialidade, integridade, disponibilidade e autenticidade dos dados pessoais, e determina a comunicação à ANPD e aos titulares sempre que o incidente puder acarretar risco ou dano relevante (ANPD, 2024)[5]. Cria-se, assim, uma interface direta entre o programa de segurança da informação e o programa de compliance, que passam a depender de protocolos conjuntos de resposta a incidentes.

1.4 Integridade corporativa e riscos cibernéticos

A integridade corporativa, pilar dos programas de compliance anticorrupção construídos a partir da Lei nº 12.846/2013 e das recomendações da OCDE (Organização para a Cooperação e Desenvolvimento Econômico), encontra no ambiente cibernético um campo novo e complexo de desafios. Riscos cibernéticos não são apenas riscos tecnológicos: podem se materializar como vetores de corrupção, lavagem de dinheiro, desvio de ativos e comprometimento de processos decisórios.

O "Data Breach Investigations Report" de 2026, publicado pela Verizon a partir da análise de mais de 31 mil incidentes e 22 mil violações confirmadas em 145 países, mostrou que o fator humano esteve presente em 62% das violações analisadas, que 48% delas envolveram terceiros da cadeia de fornecimento digital, e que a engenharia social e o abuso de credenciais permanecem entre os principais vetores de ataque, ainda que a exploração de vulnerabilidades tenha se tornado, pela primeira vez, a

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

[4] MENDES, L. S. *Privacidade, proteção de dados e defesa do consumidor*. São Paulo: Saraiva, 2014.

[5] AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Resolução CD/ANPD nº 15, de 24 de abril de 2024. Aprova o Regulamento de Comunicação de Incidente de Segurança. *Diário Oficial da União*: seção 1, Brasília, DF, n. 81, p. 114-115, 26 abr. 2024. Disponível em: https://bibliotecadigital.mj.gov.br/bitstream/1/12879/2/RES_ANPD_2024_15.html. Acesso em: 22 out. 2026.

principal porta de entrada das violações (Verizon, 2026)[6]. Para quem olha o tema pela lente da integridade, o dado diz muito: *phishing*, comprometimento de e-mail corporativo e fraudes digitais exploram a vulnerabilidade humana e, ao fazê-lo, expõem deficiências de cultura ética e de capacitação dos colaboradores.

A interface entre integridade corporativa e riscos cibernéticos aparece em situações bastante concretas: no uso indevido de sistemas corporativos para desvio de informações confidenciais; na infiltração de agentes mal-intencionados na cadeia de fornecimento digital; no emprego de *ransomware* por grupos criminosos com possíveis conexões com redes de corrupção; e no comprometimento de sistemas de controles internos, com reflexos sobre a confiabilidade das demonstrações financeiras.

Não por acaso, o programa de Cyber Compliance dialoga diretamente com os controles anticorrupção. Segregação de funções, controle de acessos privilegiados, trilhas de auditoria e monitoramento contínuo de anomalias são instrumentos que servem, ao mesmo tempo, à prevenção de fraudes corporativas e à detecção precoce de incidentes cibernéticos.

1.5 O papel da alta administração e das três linhas de defesa

A responsabilidade da alta administração pelo risco cibernético tornou-se tema central da governança corporativa. O IBGC (Instituto Brasileiro de Governança Corporativa), na 6ª edição do "Código das Melhores Práticas de Governança Corporativa" (2023), reconhece a segurança cibernética como pauta obrigatória dos conselhos de administração, dada sua capacidade de afetar diretamente a continuidade dos negócios, o valor das companhias e os direitos de múltiplos *stakeholders* (IBGC, 2023)[7]. Nos Estados Unidos, a Securities and Exchange Commission (SEC) exige, desde 2023, a divulgação de informações sobre governança e gestão de riscos cibernéticos nos relatórios anuais das companhias abertas (SEC, 2023), tendência que deve alcançar também o mercado brasileiro.

O Modelo das Três Linhas, atualizado pelo Institute of Internal Auditors (IIA) em 2020, oferece um arcabouço consistente para a distribuição de responsabilidades em um programa de Cyber Compliance. Vale notar que, nessa atualização, o IIA abandonou a antiga nomenclatura "três linhas de defesa": as linhas existem tanto para proteger valor quanto para criá-lo, e a colaboração e o alinhamento entre elas são condição de sucesso organizacional (IIA, 2020)[8].

Aplicado ao Cyber Compliance, o modelo classifica responsabilidades, e não áreas de forma fixa. Os papéis de primeira linha, tipicamente desempenhados pelas unidades de negócio e pela área de TI/operações, correspondem à operação dos controles técnicos e processuais no dia a dia. Os papéis de segunda linha envolvem o monitoramento e a orientação quanto à efetividade desses controles, bem como a condução do programa de Cyber Compliance propriamente dito; funções como CISO, DPO, compliance e gestão de riscos costumam exercê-los, mas seu enquadramento dependerá das atribuições efetivamente desempenhadas em cada estrutura de governança. A terceira linha, exercida pela Auditoria Interna, oferece avaliação independente e objetiva sobre a adequação das duas primeiras, com reporte direto ao Conselho de Administração ou ao Comitê de Auditoria.

[6] VERIZON. *2026 Data Breach Investigations Report*. Basking Ridge: Verizon Business, 2026. Disponível em: https://www.verizon.com/business/resources/reports/dbir/. Acesso em: 14 ago. 2026.

[7] INSTITUTE OF INTERNAL AUDITORS. *The IIA's Three Lines Model*: An Update of the Three Lines of Defense. Lake Mary: IIA, 2020. Disponível em: https://www.theiia.org/globalassets/documents/resources/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense-july-2020/three-lines-model-updated-english.pdf. Acesso em: 01 jun. 2026.

[8] INSTITUTE OF INTERNAL AUDITORS. *The IIA's Three Lines Model:* An Update of the Three Lines of Defense. Lake Mary: IIA, 2020. Disponível em: https://www.theiia.org/globalassets/documents/resources/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense-july-2020/three-lines-model-updated-english.pdf. Acesso em: 01 jun. 2026.

O COSO ERM (2017) complementa esse arranjo: ao integrar a gestão de riscos à estratégia e ao desempenho, o *framework* coloca os riscos cibernéticos no mesmo patamar de prioridade dos riscos estratégicos, financeiros e de conformidade (COSO, 2017)[9].

Na prática, isso significa que o apetite de risco cibernético deve ser formulado pela administração e submetido à aprovação ou à supervisão do Conselho, conforme a estrutura de governança de cada organização, e não simplesmente delegado à área de TI.

1.6 Cultura organizacional e comportamento humano como fator de risco

De todos os componentes de um programa de Cyber Compliance, a dimensão humana é, ao mesmo tempo, a mais crítica e a mais negligenciada. Bruce Schneier, um dos mais influentes especialistas mundiais em segurança da informação, sustenta que a segurança é, no fundo, um problema humano: tecnologias falham porque pessoas as configuram mal, contornam controles inconvenientes ou são manipuladas por engenharia social (Schneier, 2015)[10].

Os dados empíricos confirmam a tese: o Verizon DBIR 2026 aponta o *phishing* e o abuso de credenciais furtadas entre os principais vetores de comprometimento inicial.

A engenharia social, entendida como o conjunto de técnicas que exploram vieses cognitivos e emocionais para obter acesso não autorizado a sistemas e informações, é o maior desafio para programas de segurança apoiados exclusivamente em controles técnicos. Simulações periódicas de *phishing*, treinamentos ajustados ao perfil de risco de cada público e canais seguros de reporte de incidentes são medidas de eficácia comprovada para reduzir a superfície de ataque humana.

Do ponto de vista do compliance, a cultura organizacional é o terreno sobre o qual os programas de integridade são construídos. Uma cultura que tolera atalhos, pune o erro honesto ou marginaliza quem reporta irregularidades é, por definição, vulnerável a riscos cibernéticos. Funcionários que temem represálias não reportam incidentes; equipes sobrecarregadas ignoram alertas; líderes que não dão o exemplo em boas práticas digitais transmitem a mensagem de que segurança é um fardo burocrático, e não um valor da organização.

Programas de Cyber Compliance bem-sucedidos investem, por isso, na construção de uma cultura de segurança que seja também uma cultura de integridade, na qual o comportamento ético e a responsabilidade digital sejam reconhecidos, valorizados e continuamente reforçados em todos os níveis hierárquicos, a começar pela alta liderança.

1.7 Inteligência Artificial, riscos emergentes e desafios regulatórios

Para o Cyber Compliance, a Inteligência Artificial (IA) representa oportunidades e riscos em igual medida. No campo das oportunidades, sistemas de IA já são amplamente utilizados na detecção de anomalias comportamentais (UEBA – User and Entity Behavior Analytics), na análise de *logs* em tempo real, na automação de respostas a incidentes e na triagem de vulnerabilidades, ampliando a capacidade de detecção e resposta das equipes de segurança.

No campo dos riscos, a IA generativa abre novos vetores de ameaça: campanhas de *spear phishing* altamente personalizadas produzidas por modelos de linguagem, *deepfakes* de voz e vídeo aplicados a fraudes de engenharia social e o uso de IA para acelerar a descoberta de vulnerabilidades em sistemas críticos. Além disso, os próprios sistemas de IA adotados pelas organizações podem tratar dados pessoais de forma pouco transparente, criando desafios adicionais de conformidade com a LGPD e o GDPR.

[9] COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION. *Enterprise Risk Management* – Integrating with Strategy and Performance. New York: COSO, 2017.

[10] SCHNEIER, B. *Secrets and Lies*: Digital Security in a Networked World. Indianapolis: Wiley, 2015.

No plano regulatório, o AI Act europeu (Regulamento (UE) 2024/1689), adotado em 2024, estabeleceu um regime regulatório baseado em risco, classificando os sistemas de IA em categorias de risco inaceitável (práticas proibidas), alto risco, risco limitado, sujeito a obrigações de transparência e risco mínimo (European Parliament; Council of the European Union, 2024)[11].

Sistemas classificados como de alto risco, caso daqueles empregados em infraestruturas críticas, gestão de pessoal ou controle de acesso, ficam sujeitos a requisitos rigorosos de transparência, documentação, supervisão humana e gestão de riscos. A aplicação do regulamento é escalonada: as práticas proibidas vigoram desde fevereiro de 2025 as obrigações para modelos de IA de propósito geral, desde agosto de 2025, e as obrigações de transparência do artigo 50, inclusive a rotulagem de conteúdo gerado por IA, desde agosto de 2026; já as exigências aplicáveis aos sistemas de alto risco, originalmente previstas para agosto de 2026, foram adiadas para dezembro de 2027 pelo Regulamento (UE) 2026/1744 (Digital Omnibus on AI), primeira alteração substantiva do AI Act. Embora o AI Act tenha aplicação direta apenas na União Europeia, sua influência sobre empresas brasileiras que operam ou se relacionam com o mercado europeu já é uma realidade.

Para os programas de Cyber Compliance, a IA exige governança própria: políticas de uso aceitável de IA generativa, avaliações de impacto específicas, análogas aos Relatórios de Impacto à Proteção de Dados Pessoais previstos na LGPD, controles sobre o treinamento de modelos com dados corporativos sensíveis e mecanismos de auditabilidade das decisões automatizadas. Entre os referenciais específicos de governança de IA, destacam-se o NIST AI Risk Management Framework (NIST AI RMF 1.0, 2023) e a ISO/IEC 42001:2023, norma certificável de sistemas de gestão de inteligência artificial; COBIT 2019 e NIST CSF 2.0, por sua vez, seguem úteis para a governança geral de TI e segurança, oferecendo o ecossistema mais amplo de controles ao qual a governança de IA deve se integrar (NIST, 2023; ISO, 2023; ISACA, 2018)[12].

1.8 Boas práticas e aplicações nas empresas brasileiras

O mercado brasileiro apresenta estágios bastante desiguais de maturidade em Cyber Compliance. Grandes conglomerados financeiros (grupo de instituições financeiras interligadas, geralmente por meio de participações acionárias ou controle operacional), empresas de tecnologia e multinacionais com presença global avançaram de forma consistente na integração entre compliance, segurança da informação e privacidade. O setor financeiro, em particular, está sujeito a obrigações específicas de governança cibernética estabelecidas pela Resolução CMN nº 4.893/2021 e pela Resolução BCB nº 85/2021, recentemente atualizadas pelas Resoluções CMN nº 5.274/2025 e BCB nº 538/2025 (CMN, 2025; BCB, 2025), o que impulsionou investimentos relevantes. Na outra ponta, médias e pequenas empresas e organizações do terceiro setor ainda enfrentam o desafio de estruturar programas integrados com recursos limitados.

Algumas práticas de mercado merecem registro: empresas do setor financeiro têm adotado o NIST CSF como referência principal de avaliação de maturidade cibernética, associando seus resultados ao COBIT 2019 na dimensão de governança de TI; organizações de grande

[11] EUROPEAN PARLIAMENT; COUNCIL OF THE EUROPEAN UNION. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). *Official Journal of the European Union*, Luxembourg, 12 July 2024. Disponível em: https://eur-lex.europa.eu/eli/reg/2024/1689/oj. Acesso em: 22 out. 2026.

[12] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). *Artificial intelligence risk management framework* (AI RMF 1.0). Gaithersburg, MD: National Institute of Standards and Technology, 2023. (NIST AI 100-1). Disponível em: https://doi.org/10.6028/NIST.AI.100-1.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO); INTERNATIONAL ELECTROTECHNICAL COMMISSION (IEC). *ISO/IEC 42001:2023*: information technology -- artificial intelligence -- management system. Geneva: International Organization for Standardization, 2023.

INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION (ISACA). *COBIT 2019 framework*: introduction and methodology. Rolling Meadows, IL: ISACA, 2018.

porte têm integrado a função de DPO ao organograma de compliance, criando uma área unificada de compliance e privacidade em diálogo direto com o CISO; e os treinamentos de segurança cibernética e compliance vêm sendo incorporados aos programas de integridade, tratando a segurança digital como parte do comportamento ético esperado de todos os colaboradores.

No âmbito da proteção de dados, a adoção da ISO 27701:2025 por controladores e operadores brasileiros pode servir como evidência relevante de governança e de *accountability* perante a ANPD, embora não demonstre, isoladamente, conformidade com a LGPD, que segue dependendo do atendimento efetivo às obrigações legais em cada operação de tratamento. A norma mapeia seus controles diretamente para os requisitos do GDPR e, em termos estruturais, para a LGPD, aproximando as obrigações legais dos controles técnicos de segurança da informação. Com a edição de 2025, que a transformou em padrão autônomo, sua adoção tornou-se viável inclusive para organizações que ainda não possuem um Sistema de Gestão de Segurança da Informação (SGSI) certificado pela ISO 27001 (ISO, 2025)[13].

Conclusão

O Cyber Compliance não é modismo de gestão nem resposta improvisada a episódios de crise. É um modelo de governança que amadureceu ao longo de décadas de evolução normativa, técnica e cultural, e que responde a uma realidade da qual nenhuma organização escapa: riscos digitais são, hoje, riscos de negócio da mais alta magnitude.

A convergência entre compliance, segurança da informação e proteção de dados é um caminho sem volta. LGPD, GDPR, NIST CSF 2.0, ISO 27001:2022, ISO 27701, ISO 37301 e o Modelo de Três Linhas do IIA formam um ecossistema normativo e técnico que, adotado de forma integrada, dá às organizações as bases de uma governança digital robusta, ética e sustentável.

Para as empresas brasileiras, os próximos anos serão decisivos. A atuação fiscalizatória da ANPD tende a se intensificar; o Marco Legal da Inteligência Artificial (PL 2338/2023), aprovado pelo Senado Federal em dezembro de 2024 e atualmente em análise na Câmara dos Deputados, deverá consolidar no país um regime de responsabilidade baseado em risco, inspirado no AI Act europeu; os ataques cibernéticos continuarão crescendo em sofisticação e impacto com o uso da IA; e investidores, clientes e parceiros internacionais cobrarão, cada vez mais, evidências de maturidade em Cyber Compliance. As organizações que tratarem o tema como prioridade estratégica e não como obrigação burocrática, estarão mais bem posicionadas para criar valor, proteger seus *stakeholders* e construir uma reputação duradoura.

Se este artigo puder ser resumido em uma única ideia, que seja esta: Cyber Compliance não é apenas conformidade regulatória, nem apenas proteção tecnológica. É um modelo de governança capaz de alinhar ética, integridade, proteção de dados, segurança da informação, gestão de riscos e estratégia empresarial. E o protagonismo desse alinhamento cabe, necessariamente, à alta liderança.

[13] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO); INTERNATIONAL ELECTROTECHNICAL COMMISSION (IEC). *ISO/IEC 27701:2025*: information security, cybersecurity and privacy protection — privacy information management systems — requirements and guidance. Geneva: International Organization for Standardization, 2025.

Quadro 1 – Principais componentes de um programa de Cyber Compliance

COMPONENTE	DESCRIÇÃO SUMÁRIA
Governança e Patrocínio	Comprometimento formal da alta administração, conselho e C-Suite; políticas de compliance e segurança da informação aprovada; DPO e CISO com reporte direto à liderança.
Mapeamento de Riscos Cibernéticos	Inventário de ativos de informação, classificação de dados, análise de vulnerabilidades, cenários de ameaças e apetite de risco definido.
Políticas e Controles Técnicos	Políticas de Cyber Segurança, controles baseados em boas práticas ISO 27001/27002, gestão de identidade e acesso (IAM), criptografia e segmentação de rede.
Privacidade e LGPD	Relatórios de Impacto a proteção de dados pessoais (RIPD), registros de operações de tratamento (RoPA), base legal definida, DPA com fornecedores, gestão de direitos dos titulares e Privacy by Design sobre novos processos, sistemas com tratamento de dados pessoais e sensíveis.
Resposta a Incidentes	Plano de Resposta a Incidentes (IRP), CSIRT ou CERT interno, playbooks de *ransomware* e vazamento, notificação à ANPD conforme Resolução CD/ANPD nº 15/2024.
Três Linhas de Defesa	Operação (1ª linha), Compliance/DPO/SI (2ª linha) e Auditoria Interna (3ª linha) alinhadas ao Modelo de Três Linhas do IIA (2020).
Treinamento e Cultura	Programas de conscientização, simulações de phishing, treinamentos por perfil de risco, campanhas de cultura de proteção de dados e integridade.
Indicadores (KPIs/KRIs)	Tempo médio de detecção (MTTD), tempo médio de resposta (MTTR), cobertura de treinamento, nº de incidentes notificados, nível de maturidade NIST CSF.
Conformidade Regulatória	Monitoramento contínuo de obrigações legais(quando aplicável) (LGPD, GDPR, Marco Civil, NIS2, DORA, AI Act), auditorias periódicas e reporte ao conselho.
Gestão de Terceiros	Due diligence de fornecedores, cláusulas de segurança e privacidade em contratos, monitoramento de riscos da cadeia de suprimentos.
Continuidade de Negócios	Business Continuity Plan (BCP) e Disaster Recovery Plan (DRP) integrados à segurança cibernética com testes periódicos, RTO/RPO definidos e comunicação de crise estruturada.

Fonte: Elaborado pelo autor (2026), com base em NIST CSF 2.0, ISO 27001:2022, ISO 27701, ISO 37301:2021, COBIT 2019, CIS Controls v8.1 e IIA Three Lines Model.

Quadro 2 – Análise comparativa: compliance tradicional, segurança da informação e Cyber Compliance integrado

DIMENSÃO	COMPLIANCE TRADICIONAL	SEGURANÇA DA INFORMAÇÃO	*CYBER* COMPLIANCE INTEGRADO
Foco principal	Conformidade legal e normativa	Proteção de ativos tecnológicos	Governança integrada: ética, risco, dado e tecnologia
Área responsável	Compliance / Jurídico	TI / CISO	CISO, DPO, Compliance, Jurídico, RH, Auditoria
Reporte	Diretoria Jurídica / CEO	Diretoria de TI / CTO	Conselho / Comitê de Riscos e Compliance
Visão de risco	Riscos de conformidade e reputação	Riscos técnicos e operacionais	Riscos integrados: regulatórios, operacionais, financeiros, reputacionais e éticos
Frameworks de referência	ISO 37301, Lei 12.846/2013, LGPD	ISO 27001, NIST CSF, CIS Controls	ISO 27001, 27701, 37301, NIST CSF 2.0, COBIT 2019, COSO ERM
Tratamento de dados pessoais	Foco em bases legais e direitos dos titulares	Foco em confidencialidade e disponibilidade	Ciclo completo: base legal, segurança, privacidade por design e resposta a incidentes
Alta Administração	Sponsor do programa de compliance	Aprovação de orçamento de TI	Responsabilidade fiduciária e estratégica pelo risco cibernético
Indicadores	N° de não conformidades, treinamentos	N° de vulnerabilidades, MTTR, incidentes	Painel integrado de KPIs/KRIs: conformidade + segurança + privacidade + continuidade

Fonte: Elaborado pelo autor (2026).

Quadro 3 – Dez recomendações práticas de Cyber Compliance para empresas brasileiras

Nº	RECOMENDAÇÃO PRÁTICA
1	Instituir um Comitê de Cyber Compliance multidisciplinar com participação de CISO, DPO, Compliance, Jurídico e RH, com reporte periódico ao Conselho de Administração.
2	Mapear e classificar todos os ativos de informação e bases de dados pessoais, aplicando análise de risco integrada conforme o NIST CSF 2.0 e o COSO ERM, com revisão anual.
3	Implementar controles técnicos alinhados à ISO 27001:2022, priorizando gestão de identidade e acesso (IAM), MFA, segmentação de rede e monitoramento contínuo (SIEM/SOC).
4	Adotar a ISO 27701:2025 para a gestão de informações de privacidade (PIMS), seja de forma integrada ao SGSI (ISO 27001), seja como sistema de gestão autônomo, integrando os registros de operações de tratamento (RoPA) ao inventário de ativos.
5	Elaborar e testar, ao menos anualmente, um Plano de Resposta a Incidentes (IRP) com playbooks específicos para ransomware e vazamento de dados, incluindo fluxos de notificação à ANPD conforme a Resolução CD/ANPD nº 15/2024.
6	Aplicar o Modelo de Três Linhas do IIA (2020) ao programa de Cyber Compliance, definindo papéis claros entre operação (1ª linha), áreas de controle (2ª linha) e auditoria interna independente (3ª linha).
7	Desenvolver um programa robusto de conscientização que inclua programa de integridade, privacidade e proteção de dados, simulações periódicas de phishing, treinamentos por perfil de risco e métricas de efetividade, reconhecendo que o fator humano é o principal vetor de ataques.
8	Inserir cláusulas de ética e anticorrupção, segurança da informação e privacidade em todos os contratos com fornecedores e parceiros, realizando due diligence de integridade e monitoramento contínuo da cadeia de suprimentos digital.
9	Criar um painel integrado de indicadores (KPIs e KRIs) de Cyber Compliance para a alta liderança, com métricas como MTTD, MTTR, nível de maturidade dos principais frameworks escolhidos. (Ex: NIST CSF), percentual de cobertura de treinamento e nº de incidentes notificados.
10	Estabelecer processo de monitoramento regulatório para acompanhar evoluções legislativas de acordo com o setor e abrangência tais como: (LGPD, GDPR, NIS2, DORA, AI Act europeu) e adaptar o programa de Cyber Compliance de forma proativa, evitando reatividade regulatória.

Fonte: Elaborado pelo autor (2026).

Referências

AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Resolução CD/ANPD nº 15, de 24 de abril de 2024. Aprova o Regulamento de Comunicação de Incidente de Segurança. *Diário Oficial da União*: seção 1, Brasília, DF, n. 81, p. 114-115, 26 abr. 2024

BANCO CENTRAL DO BRASIL. Resolução BCB nº 85, de 8 de abril de 2021. Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições de pagamento. Brasília: BCB, 2021. Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?numero=85&tipo=Resolu%C3%A7%C3%A3o+BCB. Acesso em: 22 out. 2026.

BANCO CENTRAL DO BRASIL. Resolução BCB nº 538, de 18 de dezembro de 2025. Altera a Resolução BCB nº 85, de 8 de abril de 2021, que dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições de pagamento. Brasília: BCB, 2025. Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?numero=538&tipo=Resolu%C3%A7%C3%A3o+BCB. Acesso em: 22 out. 2026.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). *Diário Oficial da União*: seção 1, Brasília, DF, p. 59, 15 ago. 2018.

BRASIL. Lei nº 12.846, de 1º de agosto de 2013. Dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira, e dá outras providências. *Diário Oficial da União*: seção 1, Brasília, DF, p. 1, 2 ago. 2013.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. *Diário Oficial da União*: seção 1, Brasília, DF, p. 1, 24 abr. 2014.

BRASIL. Lei nº 15.352, de 25 de fevereiro de 2026. Transforma cargos no âmbito do Poder Executivo federal; altera a Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), para dispor sobre a Agência Nacional de Proteção de Dados (ANPD), a Lei nº 10.871, de 20 de maio de 2004, para criar a Carreira de Regulação e Fiscalização de Proteção de Dados, a Lei nº 15.211, de 17 de setembro de 2025 (Estatuto Digital da Criança e do Adolescente), para dispor sobre o início da vigência da referida Lei; altera as Leis nºs 9.008, de 21 de março de 1995, 11.890, de 24 de dezembro de 2008, 13.326, de 29 de julho de 2016, 13.848, de 25 de junho de 2019, e 14.600, de 19 de junho de 2023; revoga a Medida Provisória nº 1.319, de 17 de setembro de 2025; e dá outras providências. *Diário Oficial da União*: seção 1, edição extra B, Brasília, DF, p. 1-2, 25 fev. 2026.

BRASIL. Senado Federal. Projeto de Lei nº 2.338, de 2023. Dispõe sobre o uso da Inteligência Artificial (Marco Legal da Inteligência Artificial). Aprovado pelo Senado Federal em 10 dez. 2024 e encaminhado à Câmara dos Deputados em 17 mar. 2025, para revisão. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/157233. Acesso em: 14 ago. 2026.

CENTER FOR INTERNET SECURITY (CIS). *CIS Critical Security Controls v8.1*. East Greenbush: CIS, 2024. Disponível em: https://www.cisecurity.org/controls/v8-1. Acesso em: 01 jun. 2026.

COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION (COSO). *Enterprise Risk Management* – Integrating with Strategy and Performance. New York: COSO, 2017.

CONSELHO MONETÁRIO NACIONAL (CMN). Resolução CMN nº 4.893, de 26 de fevereiro de 2021. Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições autorizadas a funcionar pelo Banco Central do Brasil. Brasília: BCB, 2021.

CONSELHO MONETÁRIO NACIONAL (CMN). Resolução CMN nº 5.274, de 18 de dezembro de 2025. Altera a Resolução CMN nº 4.893, de 26 de fevereiro de 2021, que dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições autorizadas a funcionar pelo Banco Central do Brasil. Brasília: BCB, 2025.

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

EUROPEAN PARLIAMENT; COUNCIL OF THE EUROPEAN UNION. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (GDPR). Official Journal of the European Union, Luxembourg, 4 maio 2016.

EUROPEAN PARLIAMENT; COUNCIL OF THE EUROPEAN UNION. Directive (EU) 2022/2555 (NIS2 Directive). Official Journal of the European Union, Luxembourg, 27 dez. 2022.

EUROPEAN PARLIAMENT; COUNCIL OF THE EUROPEAN UNION. Regulation (EU) 2022/2554 (DORA – Digital Operational Resilience Act). Official Journal of the European Union, Luxembourg, 27 dez. 2022.

EUROPEAN PARLIAMENT; COUNCIL OF THE EUROPEAN UNION. Regulation (EU) 2024/1689 (AI Act – Artificial Intelligence Act). Official Journal of the European Union, Luxembourg, 12 jul. 2024.

EUROPEAN PARLIAMENT; COUNCIL OF THE EUROPEAN UNION. Regulation (EU) 2026/1744 (Digital Omnibus on AI). Official Journal of the European Union, Luxembourg, 24 jul. 2026.

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA (IBGC). *Código das Melhores Práticas de Governança Corporativa*. 6. ed. São Paulo: IBGC, 2023.

INSTITUTE OF INTERNAL AUDITORS (IIA). The IIA's Three Lines Model: An Update of the Three Lines of Defense. Lake Mary: IIA, jul. 2020. Disponível em: https://www.theiia.org/globalassets/documents/resources/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense-july-2020/three-lines-model-updated-english.pdf. Acesso em: 01 jun. 2026.

ISACA. COBIT 2019 Framework: Introduction and Methodology. Rolling Meadows: ISACA, 2018.

ISO – INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO/IEC 27001:2022 – Information Security, Cybersecurity and Privacy Protection: Information Security Management Systems – Requirements. Geneva: ISO, 2022.

ISO – INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO/IEC 27002:2022 – Information Security, Cybersecurity and Privacy Protection: Information Security Controls. Geneva: ISO, 2022.

ISO – INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO/IEC 27701:2025 – Information Security, Cybersecurity and Privacy Protection: Privacy Information Management Systems – Requirements and Guidance. Geneva: ISO, 2025.

ISO – INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO 37301:2021 – Compliance Management Systems: Requirements with Guidance for Use. Geneva: ISO, 2021.

ISO – INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO/IEC 42001:2023 – Information Technology – Artificial Intelligence – Management System. Geneva: ISO, 2023.

MENDES, L. S. *Privacidade, proteção de dados e defesa do consumidor*: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). Artificial Intelligence Risk Management Framework (AI RMF 1.0). Gaithersburg: NIST, jan. 2023. (NIST AI 100-1). Disponível em: https://doi.org/10.6028/NIST.AI.100-1. Acesso em: 01 jun. 2026.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD). *Recommendation of the Council for Further Combating Bribery of Foreign Public Officials in International Business Transactions*. Paris: OECD, 2021.

PASCOE, C.; QUINN, S.; SCARFONE, K. The NIST Cybersecurity Framework (CSF) 2.0. Gaithersburg: NIST, fev. 2024. (NIST CSWP 29). Disponível em: https://doi.org/10.6028/NIST.CSWP.29. Acesso em: 01 jun. 2026.

SCHNEIER, B. *Secrets and Lies: Digital Security in a Networked World*. Indianapolis: Wiley, 2015.

SECURITIES AND EXCHANGE COMMISSION (SEC). Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure: Final Rule (Release n° 33-11216; 34-97989). Washington, D.C.: SEC, 26 jul. 2023.

VERIZON. *2026 Data Breach Investigations Report*. Basking Ridge: Verizon Business, 2026. Disponível em: https://www.verizon.com/business/resources/reports/dbir/. Acesso em: 14 ago. 2026.

Capítulo 4

Governança de Inteligência Artificial: equilibrando competitividade e responsabilidade

Inteligência Artificial:

fundamentos técnicos, aplicações e o novo desafio da inovação corporativa

Juliana Oliveira Nascimento

Juliana Oliveira Nascimento é head de Riscos, Compliance e Atuarial da Sompo, com mais de 22 anos de experiência corporativa, com especialidade em governança, riscos, compliance, ESG e AI Governance em multinacionais e Big Four. Mestre em International Business Law (Steinbeis University - Germany), MBA em Inovação Sustentável (USP), formação em Global Leadership (LSE) e ESG (NYU). Cofundadora e chairwoman do Compliance Women Committee (4.000+ membros, atuação internacional e sem fins lucrativos). Professora, coautora de diversas publicações em ESG, GRC e liderança, alternativa board member Allinance for Integrity - Germany. Reconhecida internacionalmente como GRC Educator of the Year (2025), GRC Ambassador (2025), SW50 Global Women Leaders (2025) e SW50 Global Líder (2025).

Introdução

A Inteligência Artificial (IA) deixou de ser um campo restrito à pesquisa acadêmica e passou a operar como uma tecnologia de propósito geral, capaz de reconfigurar processos produtivos, modelos de negócio e estruturas de decisão nas organizações. Esse deslocamento não é apenas técnico: envolve mudanças na forma como as empresas competem, inovam e se relacionam com riscos regulatórios, éticos e reputacionais.

O termo "inteligência artificial" remonta à proposta de pesquisa apresentada por McCarthy, Minsky, Rochester e Shannon em 1955, que buscava investigar se máquinas poderiam simular aspectos da inteligência humana[1]. Desde então, a área atravessou ciclos alternados de entusiasmo e retração, os chamados "invernos da IA", até que, na última década, avanços em aprendizado profundo, disponibilidade de dados e poder computacional convergiram para uma nova fase de maturidade tecnológica e adoção empresarial em escala.

O objetivo deste artigo é duplo. Em primeiro lugar, apresentar, de forma sintética e tecnicamente rigorosa, os fundamentos conceituais e históricos da IA, os principais paradigmas de aprendizado de máquina e aprendizado profundo, e os marcos tecnológicos que ilustram sua trajetória. Em segundo lugar, e de modo complementar, discutir o que se convencionou chamar de "novo desafio da inovação" para as companhias: a necessidade de transformar potencial tecnológico em valor organizacional sustentável, superando barreiras de cultura, governança, talento e gestão de risco.

Metodologicamente, este artigo adota abordagem qualitativa e exploratória, de natureza bibliográfica, apoiada em literatura técnica de referência em ciência da computação e em literatura gerencial sobre inovação e estratégia. Não se pretende esgotar o tema, mas oferecer um panorama estruturado que sirva de base para reflexão e para revisões e complementações posteriores.

O texto está organizado em sete seções, além desta introdução. A seção 2 trata dos fundamentos históricos e conceituais da IA. A seção 3 aborda o aprendizado de máquina e o aprendizado profundo. A seção 4 apresenta marcos tecnológicos emblemáticos. A seção 5 discute a incorporação da IA às organizações. A seção 6 desenvolve o argumento central sobre o novo desafio da inovação para as companhias. A seção 7 trata de ética, governança e regulação. A seção 8 apresenta as considerações finais.

A relevância do tema decorre, em grande medida, da velocidade com que a IA generativa e os modelos de linguagem de grande escala passaram, a partir de 2022 e 2023, de aplicações de nicho para ferramentas de uso cotidiano em áreas tão diversas quanto atendimento ao cliente, produção de conteúdo, análise jurídica e apoio à decisão gerencial. Essa difusão acelerada tensiona a capacidade das organizações de absorver a tecnologia de forma responsável, ao mesmo tempo em que amplia as expectativas de acionistas, reguladores e sociedade quanto ao uso ético e transparente de sistemas algorítmicos. É justamente nesse ponto de tensão, entre a velocidade tecnológica e capacidade organizacional de absorção, que se fundamenta o respectivo artigo.

Diante disso, no próximo capítulo serão apresentados os fundamentos históricos e conceituais do que se conhece por inteligência artificial.

[1] MCCARTHY, J.; MINSKY, M. L.; ROCHESTER, N.; SHANNON, C. E. A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence. *AI Magazine*, [S. l.], v. 27, n. 4, p. 12-14, 2006. DOI: https://doi.org/10.1609/aimag.v27i4.1904.

1. Fundamentos históricos e conceituais da inteligência artificial

Entre os marcos fundadores do campo, destaca-se o artigo publicado por Alan Turing em 1950, no qual o autor propôs substituir a pergunta "as máquinas podem pensar?" por um critério operacional de imitação, posteriormente conhecido como Teste de Turing[2]. A proposta de Turing foi e é relevante não apenas por sua originalidade filosófica, mas por deslocar o debate sobre inteligência artificial de uma discussão puramente especulativa para um terreno passível de avaliação empírica, ainda que indireta.

Diante desse prisma, cinco anos depois, em 1955, John McCarthy, Marvin Minsky, Nathaniel Rochester e Claude Shannon submeteram uma proposta de pesquisa de verão à Universidade de Dartmouth, cunhando formalmente o termo "inteligência artificial" e estabelecendo a hipótese de que todo aspecto da aprendizagem, ou qualquer outra característica da inteligência, poderia, em princípio, ser descrito com precisão suficiente para ser simulado por uma máquina. Esse documento é amplamente reconhecido como o marco de fundação institucional da disciplina.

Do ponto de vista conceitual contemporâneo, a definição consolidada na literatura de referência caracteriza a IA como o estudo de agentes que percebem seu ambiente e atuam de forma racional para maximizar a probabilidade de sucesso em relação a um objetivo determinado[3]. Essa definição, centrada na noção de agente racional, tem a vantagem de acomodar tanto sistemas simbólicos clássicos quanto sistemas estatísticos e conexionistas contemporâneos, sem depender de uma definição fechada de "inteligência", historicamente controversa.

A trajetória histórica da IA pode ser sintetizada em três grandes fases:

I. A primeira, entre as décadas de 1950 e 1980, foi dominada pela chamada IA simbólica, predominante na época, baseada em regras lógicas e sistemas especialistas, que obteve resultados relevantes em domínios restritos, mas encontrou limites significativos diante de tarefas perceptuais e de linguagem natural.

II. A segunda fase, a partir da década de 1990, foi marcada pela ascensão de métodos estatísticos e probabilísticos, que passaram a tratar a aprendizagem como um problema de otimização a partir de dados.

III. A terceira fase, consolidada sobretudo a partir de 2012, corresponde à era do aprendizado profundo, discutida na seção seguinte, caracterizada pela combinação de grandes volumes de dados, capacidade computacional massiva e arquiteturas neurais em múltiplas camadas.

Compreender essa trajetória é relevante não apenas por razões históricas, mas porque cada fase deixou heranças metodológicas que persistem nos sistemas atuais: da lógica simbólica herdam-se estruturas de raciocínio e representação de conhecimento; da estatística, os fundamentos de inferência e otimização; e do aprendizado profundo, a capacidade de extrair representações complexas diretamente de dados não estruturados.

É importante ainda distinguir, conceitualmente, três níveis de ambição frequentemente confundidos no debate público sobre IA. A IA estreita (*narrow AI*) refere-se a sistemas projetados para desempenhar tarefas específicas e bem delimitadas, como reconhecimento de imagem ou classificação de texto, e predominantemente corresponde aos sistemas atualmente empregados nas organizações. A IA geral (*artificial general intelligence*), por sua vez, refere-se a um sistema hipotético capaz de igualar a versatilidade cognitiva humana em qualquer domínio, permanecendo, até o momento, um objetivo de pesquisa de longo prazo e não uma realidade tecnológica disponível. Por fim, discussões sobre superinteligência artificial situam-se em um plano ainda mais especulativo. Para efeitos deste artigo, e para a discussão sobre inovação corporativa desenvolvida nas seções seguintes, interessa exclusivamente a primeira categoria de IA: a IA estreita, de aplicação prática, que já produz impacto econômico mensurável nas organizações.

Na sequência, serão abordadas as bases técnicas do aprendizado de máquina e profundo.

[2] TTURING, A. M. Computing machinery and intelligence. *Mind*, Oxford, v. 59, n. 236, p. 433-460, 1950. DOI: https://doi.org/10.1093/mind/LIX.236.433.

[2] RUSSELL, S.; NORVIG, P. *Artificial Intelligence*: A Modern Approach. 4. ed. Hoboken: Pearson, 2020.

2. Aprendizado de máquina e aprendizado profundo: bases técnicas

O aprendizado de máquina (*machine learning*) pode ser definido como o subcampo da IA dedicado ao desenvolvimento de algoritmos capazes de melhorar seu desempenho em uma tarefa a partir da experiência, isto é, a partir de dados, sem que suas regras de decisão sejam explicitamente programadas para cada caso. Três paradigmas organizam a maior parte das aplicações contemporâneas.

No aprendizado supervisionado, o algoritmo é treinado a partir de exemplos rotulados, associando entradas a saídas conhecidas, como ocorre em tarefas de classificação de risco ou de detecção de fraude. No aprendizado não supervisionado, o algoritmo busca padrões e estruturas latentes em dados não rotulados, como em segmentação de clientes ou detecção de anomalias. Já no aprendizado por reforço, um agente aprende por tentativa e erro, a partir de recompensas associadas às suas ações em um ambiente, paradigma central em sistemas de tomada de decisão sequencial, como se discutirá na seção 4.

O aprendizado profundo (*deep learning*) constitui uma família de métodos de aprendizado de máquina baseada em redes neurais artificiais organizadas em múltiplas camadas de processamento, capazes de aprender representações de dados em diferentes níveis de abstração, sem a necessidade de engenharia manual de atributos[4]. Segundo essa literatura, essa característica, a aprendizagem automática de representações hierárquicas, sendo que é o que distingue o aprendizado profundo de métodos estatísticos tradicionais, e explica seu desempenho superior em tarefas de reconhecimento de imagem, fala e linguagem natural.

A obra de referência sobre o tema descreve em detalhe os fundamentos matemáticos que sustentam essas arquiteturas, incluindo álgebra linear, otimização por gradiente descendente e retropropagação de erro, além dos principais tipos de redes convolucionais, recorrentes e, mais recentemente, baseadas em mecanismos de atenção[5]. A consolidação dessa literatura técnica, ao longo da década de 2010, forneceu a base conceitual comum sobre a qual se desenvolveram praticamente todas as aplicações comerciais de IA da atualidade.

Além dos três paradigmas centrais, a literatura técnica também descreve abordagens híbridas relevantes para o contexto corporativo, como o aprendizado semissupervisionado, que combina pequenas quantidades de dados rotulados com grandes volumes de dados não rotulados, e o aprendizado por transferência (*transfer learning*), no qual um modelo previamente treinado em uma tarefa ampla é adaptado, com custo computacional reduzido, a uma tarefa específica de negócio. Essa última técnica é particularmente relevante para explicar a rápida difusão corporativa da IA generativa: em vez de treinar modelos do zero, processo custoso e intensivo em dados, a maioria das organizações passou a adaptar ou utilizar diretamente modelos de propósito geral já treinados por um número reduzido de provedores especializados, o que reconfigura também a cadeia de valor da indústria de tecnologia.

Do ponto de vista prático, três fatores explicam a viabilização do aprendizado profundo em escala industrial: a disponibilidade de grandes volumes de dados digitais, decorrente da digitalização de processos e da expansão da internet; o barateamento e a paralelização do poder computacional, sobretudo por meio de unidades de processamento gráfico (GPU); e o desenvolvimento de arquiteturas e técnicas de treinamento mais eficientes, que reduziram problemas clássicos como o desaparecimento do gradiente em redes profundas. A convergência desses três fatores, e não apenas o avanço teórico isolado, é o que explica a aceleração observada a partir de 2012.

Cabe destacar, ainda, que o desempenho de qualquer sistema de aprendizado de máquina está diretamente condicionado à qualidade, à representatividade e à governança dos dados utilizados em seu treinamento. Bases de dados incompletas, desatualizadas ou que reproduzam vieses históricos tendem a produzir modelos

[4] LECUN, Yann; BENGIO, Yoshua; HINTON, Geoffrey. Deep learning. *Nature*, [*S. l.*], v. 521, n. 7553, p. 436-444, 2015. DOI: 10.1038/nature14539.

[5] GOODFELLOW, I.; BENGIO, Y.; COURVILLE, A. *Deep Learning*. Cambridge, MA: MIT Press, 2016.

com desempenho enviesado ou instável, independentemente da sofisticação da arquitetura empregada. Por essa razão, a literatura técnica e a literatura gerencial convergem em um ponto: investimentos em infraestrutura de dados, catalogação, linhagem e controle de qualidade da informação constituem pré-requisito, e não etapa acessória, para qualquer iniciativa relevante de IA em ambiente corporativo.

Diante do contexto dos aprendizados compartilhados, serão abordados na próxima seção os marcos tecnológicos e as aplicações emblemáticas.

3. Marcos tecnológicos e aplicações emblemáticas

Um dos marcos mais frequentemente citados na literatura como demonstração pública do potencial do aprendizado profundo combinado ao aprendizado por reforço é o sistema AlphaGo, desenvolvido pela DeepMind, que combinou redes neurais de valor e de política com busca em árvore para derrotar campeões humanos no jogo de Go, um jogo historicamente considerado intratável para abordagens de força bruta, dado seu espaço de estados praticamente ilimitado[6]. O resultado foi relevante não apenas competitivamente, mas porque demonstrou que sistemas de IA poderiam superar especialistas humanos em domínios que dependem fortemente de intuição e avaliação posicional, e não apenas de cálculo combinatório explícito.

Outro marco decisivo foi a introdução da arquitetura Transformer, baseada inteiramente em mecanismos de atenção, dispensando as estruturas recorrentes e convolucionais até então dominantes em tarefas de linguagem[7]. Essa arquitetura tornou-se, ao longo dos anos seguintes, a base técnica dos grandes modelos de linguagem que sustentam a atual onda de IA generativa, por permitir treinamento altamente paralelizável e melhor captura de dependências de longo alcance em sequências de texto.

A partir dessas bases técnicas, observou-se uma expansão progressiva das aplicações de IA para domínios como diagnóstico médico assistido, sistemas de recomendação, precificação dinâmica, detecção de fraude e compliance, automação de atendimento e, mais recentemente, geração de conteúdo textual, visual e sonoro. Essa trajetória evidencia um padrão recorrente: descobertas originadas em domínios relativamente restritos jogos, tradução automática, reconhecimento de imagem tendem a se difundir, em poucos anos, para aplicações de propósito geral em larga escala, o que amplia tanto o potencial de valor quanto a superfície de risco a ser gerida pelas organizações.

4. Inteligência artificial nas organizações: da experimentação ao valor

Estudo de referência sobre a adoção corporativa de IA, conduzido por Davenport e Ronanki (2018), propôs uma classificação ainda amplamente utilizada, segundo a qual a tecnologia tende a apoiar três grandes necessidades de negócio: a automação de processos administrativos e financeiros de retaguarda; a geração de *insights* a partir da análise de grandes volumes de dados; e o engajamento aprimorado com clientes e colaboradores, por meio de interfaces cognitivas[8]. Os autores observaram, com base em pesquisa junto a centenas de executi-

[6] SILVER, D. et al. Mastering the game of Go with deep neural networks and tree search. *Nature*, [*S. l.*], v. 529, n. 7587, p. 484-489, 2016. DOI: 10.1038/nature16961.

[7] VASWANI, A. *et al.* Attention is all you need. *In*: ADVANCES IN NEURAL INFORMATION PROCESSING SYSTEMS, 30., 2017, Long Beach. *Anais* [...]. Long Beach: Curran Associates, Inc., 2017. p. 5998-6008.

[8] DAVENPORT, T. H.; RONANKI, R. Artificial intelligence for the real world. *Harvard Business Review*, [*S. l.*], v. 96, n. 1, p. 108-116, 2018. Disponível em: https://hbr.org/2018/01/artificial-intelligence-for-the-real-world. Acesso em: 26 out. 2026.

vos e projetos, que iniciativas incrementais e não projetos ambiciosos de ruptura total, os chamados "*moonshots*", tendiam a apresentar maior taxa de sucesso, sobretudo quando orientadas à ampliação de capacidades humanas em vez de sua substituição integral.

Pesquisas empresariais mais recentes confirmam a aceleração da adoção: levantamento global conduzido junto a organizações de diferentes setores identificou que a proporção de empresas utilizando IA em pelo menos uma função de negócio ultrapassou três quartos dos respondentes, com uso crescente de sistemas de IA agêntica, capazes de planejar e executar múltiplas etapas de um fluxo de trabalho com autonomia, ainda que a maior parte das organizações não tenha, até o momento, capturado impacto financeiro relevante e generalizado a partir dessas iniciativas[9]. Esse descompasso entre adoção tecnológica e captura efetiva de valor é um dos pontos centrais discutidos na seção seguinte.

Um padrão observado na literatura gerencial é que a maturidade em IA não avança de forma linear com o investimento tecnológico isolado. Organizações que obtêm melhores resultados costumam combinar três frentes de ação simultâneas: redesenho de processos e fluxos de trabalho em torno da tecnologia, e não apenas sua sobreposição a processos preexistentes; investimento em governança de dados e qualidade da informação, pré-requisito frequentemente subestimado; e desenvolvimento de competências organizacionais, tanto técnicas quanto de gestão de mudança, capazes de sustentar a adoção ao longo do tempo.

Esse último ponto merece destaque: pesquisas setoriais indicam que a escassez de competências analíticas e digitais e não apenas a disponibilidade de tecnologia figura de forma recorrente entre as principais barreiras à escala de iniciativas de IA. Programas estruturados de capacitação, revisão de trilhas de carreira e criação de papéis híbridos, que combinem conhecimento de negócio e literacia analítica, tendem a ser tão determinantes para o sucesso das iniciativas quanto a escolha da tecnologia ou do fornecedor. Nesse sentido, a gestão de pessoas e cultura organizacional desloca-se do papel de coadjuvante para o de variável central da estratégia de IA. Isso evidencia um novo desafio da inovação nas organizações, como se verá no tópico seguinte.

5. O novo desafio da inovação para as companhias

Se a seção anterior descreveu como a IA vem sendo incorporada às operações empresariais, esta seção discute por que essa incorporação constitui, para a maioria das companhias, um desafio de inovação de natureza distinta daquela associada a ondas tecnológicas anteriores.

O conceito schumpeteriano de "destruição criadora" oferece um ponto de partida relevante: para Schumpeter, o processo de inovação capitalista opera por meio da substituição contínua de estruturas produtivas, produtos e modelos de negócio estabelecidos por novas combinações mais eficientes, em um processo simultaneamente gerador e destrutivo de valor[10]. A IA contemporânea reatualiza esse processo em velocidade e escala inéditas, na medida em que reconfigura, de forma simultânea, funções administrativas, criativas e analíticas antes consideradas relativamente protegidas da automação.

A esse respeito, a literatura sobre inovação disruptiva descreve como empresas estabelecidas, mesmo quando tecnicamente competentes e atentas ao mercado, podem ser superadas por entrantes que inicialmente atendem segmentos menos exigentes com soluções mais simples e baratas, mas que evoluem rapidamente em capacidade até capturar o mercado principal[11]. O paralelo com a IA é direto: companhias que tratam a tecnologia apenas como uma ferramenta de eficiência incremental sobre processos existentes correm o risco de subestimar concorrentes, inclu-

[9] SINGLA, A.; SUKHAREVSKY, A.; YEE, L.; CHUI, M.; HALL, B. The State of AI: How Organizations Are Rewiring to Capture Value. *McKinsey & Company*, [*S. l.*], 2025. Disponível em: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-state-of-ai. Acesso em: 25 out. 2026.

[10] SCHUMPETER, J. A. *Capitalism, Socialism and Democracy*. Nova York: Harper & Brothers, 1942.

[11] CHRISTENSEN, C. M. *The Innovator's Dilemma*: When New Technologies Cause Great Firms to Fail. Boston: Harvard Business School Press, 1997.

sive entrantes menores que a utilizam para redesenhar por completo a proposta de valor de um produto ou serviço.

Nesse sentido, a literatura sobre economia digital chama atenção para um ponto frequentemente negligenciado: o valor de tecnologias de propósito geral não se realiza automaticamente a partir de sua disponibilidade técnica, mas depende de investimentos complementares em capital organizacional, como novos processos, novas competências e novas estruturas de decisão, que normalmente levam mais tempo para se consolidar do que a própria tecnologia leva para amadurecer[12]. Esse descompasso temporal entre capacidade técnica e capacidade organizacional ajuda a explicar por que, como indicado na seção 5, grande parte das organizações ainda não observa impacto financeiro proporcional ao nível de investimento e adoção declarados.

O "novo desafio da inovação" para as companhias pode, assim, ser sintetizado em quatro dimensões inter-relacionadas.

- A primeira é estratégica: decidir onde e como competir com IA, evitando tanto a subutilização conservadora quanto a adoção dispersa e sem foco.
- A segunda é organizacional: redesenhar processos, papéis e métricas de desempenho em torno da nova capacidade tecnológica, e não apenas automatizar tarefas isoladas dentro de fluxos preexistentes.
- A terceira é humana: desenvolver competências digitais e analíticas em todos os níveis hierárquicos, e não apenas em áreas técnicas especializadas, além de gerir ativamente a transição de funções impactadas.
- A quarta é de governança: assegurar que a velocidade de adoção não supere a capacidade da organização de gerir riscos éticos, regulatórios, reputacionais e de qualidade de dados associados à tecnologia, tema desenvolvido na seção seguinte.

Retomando a literatura sobre adoção corporativa de IA, observa-se que companhias mais maduras tendem a tratar a governança de risco não como uma etapa posterior à inovação, mas como parte constitutiva do próprio processo de inovação responsável — o que reforça a ideia de que o desafio contemporâneo da inovação em IA é, antes de tudo, um desafio de integração entre tecnologia, estratégia e governança[13].

5.1 Desafios práticos em setores intensivos em regulação

Em setores fortemente regulados, como serviços financeiros, seguros e saúde, o novo desafio da inovação assume contornos ainda mais exigentes, pois a companhia precisa equilibrar simultaneamente três variáveis: velocidade de adoção tecnológica, robustez de controles internos e conformidade com exigências regulatórias que, com frequência, ainda estão em processo de atualização para tratar especificamente de sistemas baseados em IA. Nesses contextos, decisões automatizadas ou assistidas por IA que afetam clientes como subscrição de risco, precificação, concessão de crédito ou definição de sinistros tendem a exigir níveis adicionais de documentação, explicabilidade e supervisão humana proporcional ao risco envolvido.

Esse cenário tem levado organizações desses setores a estruturar funções específicas de governança de modelos e de IA, frequentemente integradas às estruturas já existentes de gestão de riscos, controles internos e compliance, em vez de tratadas como iniciativas isoladas conduzidas exclusivamente por áreas de tecnologia. Essa integração tende a reduzir o risco de descolamento entre a velocidade da inovação e a capacidade da segunda e da terceira linhas de defesa de acompanhar, avaliar e validar os modelos em produção um dos pontos mais sensíveis do novo desafio da inovação em ambientes regulados.

[12] DBRYNJOLFSSON, E.; McAFEE, A. *The Second Machine Age*: Work, Progress, and Prosperity in a Time of Brilliant Technologies. Nova York: W. W. Norton & Company, 2014.

[13] BRYNJOLFSSON, E.; McAFEE, A. *The Second Machine Age*: Work, Progress, and Prosperity in a Time of Brilliant Technologies. Nova York: W. W. Norton & Company, 2014

6. Ética, governança e regulação da inteligência artificial

No plano internacional, um dos marcos mais relevantes de governança é a Recomendação do Conselho sobre Inteligência Artificial, adotada pela Organização para a Cooperação e Desenvolvimento Econômico (OCDE) em 2019. Essa recomendação estabeleceu o primeiro conjunto de princípios intergovernamentais voltados à promoção de uma IA confiável, centrada no ser humano, e que já conta com adesão de países além do bloco de membros da organização[14]. Entre os princípios estabelecidos, destacam-se o crescimento inclusivo e o bem-estar sustentável, o respeito a valores centrados no ser humano e à equidade, a transparência e explicabilidade dos sistemas, a robustez e segurança técnica, e a responsabilização (*accountability*) dos atores envolvidos ao longo de todo o ciclo de vida da tecnologia.

Para as companhias, esses princípios internacionais tendem a se traduzir, na prática operacional, em exigências como documentação e explicabilidade de modelos utilizados em decisões que afetam pessoas; mecanismos de supervisão humana proporcionais ao nível de risco da aplicação; avaliação e mitigação de vieses discriminatórios em dados e modelos; e transparência quanto ao uso de sistemas de IA em interações com clientes, empregados e demais partes interessadas.

A convergência entre inovação e governança discutida na seção anterior encontra, portanto, respaldo direto nesse arcabouço internacional: organizações que constroem capacidade de governança de IA como parte de seus processos de inovação — e não como controle externo e posterior a ela — tendem a estar mais bem posicionadas tanto para capturar valor quanto para atender a exigências regulatórias que se intensificam em diferentes jurisdições.

Do ponto de vista da estrutura interna das companhias, a operacionalização desses princípios costuma passar pela criação de instâncias formais de governança de IA comitês, comissões ou fóruns multidisciplinares que reúnam representantes de tecnologia, risco, compliance, jurídico e áreas de negócio, responsáveis por aprovar o uso de novos modelos, definir níveis de criticidade e risco por caso de uso e acompanhar indicadores de desempenho e de eventuais desvios ao longo do ciclo de vida do sistema. Complementarmente, políticas internas de uso responsável de IA, códigos de conduta específicos e programas de capacitação em ética algorítmica têm se tornado componentes cada vez mais frequentes da arquitetura de governança corporativa, funcionando como elo entre os princípios internacionais de alto nível e a prática cotidiana das equipes que desenvolvem, contratam ou operam sistemas de IA.

Considerações finais

Este artigo procurou articular, de forma integrada, os fundamentos técnicos da Inteligência Artificial e o desafio organizacional que sua adoção impõe às companhias contemporâneas. A revisão histórica e conceitual evidenciou que a atual fase de maturidade da IA resulta da convergência entre avanços em aprendizado profundo, disponibilidade de dados e capacidade computacional, e não de um único avanço teórico isolado.

No plano organizacional, a discussão indicou que o principal gargalo para a criação de valor a partir da IA não é predominantemente tecnológico, mas organizacional: a capacidade das companhias de redesenhar processos, desenvolver competências e estruturar governança de risco em ritmo compatível com a velocidade de adoção da tecnologia. Esse é, em síntese, o "novo desafio da inovação" referido ao longo do texto, um desafio que

[14] ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD). *Recommendation of the Council on Artificial Intelligence*. OECD/LEGAL/0449. Paris: OECD, 2019.

desloca o centro de gravidade da discussão sobre IA da esfera puramente técnica para a esfera da estratégia, da cultura organizacional e da governança.

Desse modo, a discussão desenvolvida ao longo deste artigo sugere que companhias em estágio inicial de maturidade em IA tendem a se beneficiar de uma sequência de prioridades relativamente estável: primeiro, organizar e assegurar a qualidade dos dados que sustentarão qualquer iniciativa futura; segundo, priorizar casos de uso com valor de negócio claro e mensurável, em vez de iniciativas dispersas orientadas apenas pela disponibilidade da tecnologia; terceiro, estabelecer, desde o início, estruturas mínimas de governança e supervisão proporcionais ao risco de cada aplicação; e quarto, investir de forma deliberada no desenvolvimento de competências e na gestão da mudança organizacional necessária para sustentar a adoção ao longo do tempo. Essa sequência não elimina a complexidade do tema, mas oferece um roteiro razoável para transformar potencial tecnológico em valor efetivo e sustentável para a companhia.

Referências

BRYNJOLFSSON, E.; McAFEE, A. *The Second Machine Age:* Work, Progress, and Prosperity in a Time of Brilliant Technologies. Nova York: W. W. Norton & Company, 2014.

CHRISTENSEN, C. M. *The Innovator's Dilemma:* When New Technologies Cause Great Firms to Fail. Boston: Harvard Business School Press, 1997.

DAVENPORT, T. H.; RONANKI, R. Artificial intelligence for the real world. *Harvard Business Review*, [*S. l.*], v. 96, n. 1, p. 108-116, 2018. Disponível em: https://hbr.org/2018/01/artificial-intelligence-for-the-real-world. Acesso em: 25 out. 2026.

GOODFELLOW, I.; BENGIO, Y.; COURVILLE, A. *Deep Learning*. Cambridge, MA: MIT Press, 2016.

LECUN, Y.; BENGIO, Y.; HINTON, G. Deep learning. Nature, [*S. l.*], v. 521, n. 7553, p. 436-444, 2015. DOI: 10.1038/nature14539.

McCARTHY, J.; MINSKY, M. L.; ROCHESTER, N.; SHANNON, C. E. A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence. *AI Magazine*, [*S. l.*], v. 27, n. 4, p. 12-14, 2006. DOI: 10.1609/aimag.v27i4.1904.

SINGLA, A.; SUKHAREVSKY, A.; YEE, L.; CHUI, M.; HALL, B. The State of AI: How Organizations Are Rewiring to Capture Value. *McKinsey & Company*, [*S. l.*], 2025. Disponível em: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-state-of-ai. Acesso em: 25 out. 2026.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD). *Recommendation of the Council on Artificial Intelligence.* OECD/LEGAL/0449. Paris: OECD, 2019.

RUSSELL, S.; NORVIG, P. *Artificial Intelligence:* A Modern Approach. 4. ed. Hoboken: Pearson, 2020.

SCHUMPETER, J. A. *Capitalism, Socialism and Democracy*. Nova York: Harper & Brothers, 1942.

SILVER, D. et al. Mastering the game of Go with deep neural networks and tree search. *Nature*, [*S. l.*], v. 529, n. 7587, p. 484-489, 2016. DOI: https://doi.org/10.1038/nature16961.

TURING, A. M. Computing Machinery and Intelligence. *Mind*, [*S. l.*], v. 59, n. 236, p. 433-460, 1950. DOI: https://doi.org/10.1093/mind/LIX.236.433.

VASWANI, A. *et al.* Attention is all you need. *In*: ADVANCES IN NEURAL INFORMATION PROCESSING SYSTEMS, 30., 2017, Long Beach. *Anais* [...]. Long Beach: Curran Associates, Inc., 2017. p. 5998-6008.

Governantes ou governadas?

Os impactos da inteligência artificial na competitividade das empresas brasileiras

Humberto Mota Filho

Humberto Mota Filho é doutor em Ciência Política (IUPERJ), mestre em Direito (UCAM). Certificated Official. MOFCOM International Business Officials (Shanghai Business School). Pós-Graduado em Direito da Empresa e da Economia (FGV). Pós-Graduado em Projetos Financeiros (UERJ). Bacharel em Direito (PUC/Rio). Consultor Jurídico Sênior do BNDES. Presidente do Conselho Empresarial de Governança, Compliance e Diversidade da Associação Comercial do Rio de Janeiro. Ex-Presidente da Comissão de Estudos da Transparência Pública da OAB/RJ. Pesquisador do CEBRAD/UERJ. Membro Fundador do IC Rio e idealizador da Revista Compliance Rio. Professor Convidado da FGV Direito Rio. Ex-membro do Conselho de Governança da Autoridade Pública Olímpica da Rio 2016. Ex-Assessor Sênior da Presidência do BNDES. Autor de livros, artigos e periódicos sobre Democracia, Transparência Pública e Desenvolvimento Sustentável.

Introdução

A inteligência artificial (IA), especialmente por meio do *aprendizado de máquina*, tem se consolidado como um dos principais vetores de transformação da competitividade empresarial contemporânea, impactando estruturas produtivas, modelos de negócio e processos decisórios. No Brasil, o uso de IA na indústria cresceu de 16,9% em 2022 para 41,9% em 2024. Nesse período, 63% das médias e grandes empresas já utilizam IA, enquanto nas pequenas e microempresas esse índice cai para 46% (IBGE, 2025).

Entretanto, sua adoção crescente suscita desafios relevantes relacionados à governança, ética e responsabilidade corporativa. A incorporação acelerada dessas tecnologias ocorre, frequentemente, sem a devida estruturação de mecanismos de governança, o que amplia riscos jurídicos, operacionais e reputacionais (Floridi *et al.*, 2025). Nesse cenário, a governança de IA emerge como elemento central para o alinhamento entre competitividade e responsabilidade.

O presente artigo explora criticamente a relação entre governança de IA e competitividade empresarial, com ênfase no contexto brasileiro, com base na análise das Teorias de Porter (vantagens competitivas) e Teece (capacidades dinâmicas) e uma revisão bibliográfica recente, a fim de compreender melhor como a governança de IA influencia a competitividade empresarial.

Sugere-se que a implementação de estruturas robustas de governança não apenas mitiga riscos, mas também constitui vantagem competitiva. Nesse sentido, em economias emergentes, como a brasileira, a governança de IA pode assumir papel estratégico na promoção do desenvolvimento econômico e na redução de dependências tecnológicas.

1. Inteligência artificial e vantagem competitiva

De início, cabe indagar: como as empresas se diferenciam pelo uso da tecnologia dos algoritmos? Para tanto, é preciso ir além dos pressupostos da teoria econômica clássica, sem abandonar seus *insights* valiosos.

Nos últimos anos, a IA tem impulsionado ganhos de produtividade e está associada a aumentos de desempenho, especialmente ao nível microeconômico. Além disso, estudos destacam que a IA está reconfigurando modelos de negócio e que a adoção de IA está impulsionando o crescimento das empresas, embora os benefícios não se distribuam de forma igual (Chaar *et al.*, 2025).

Muitos afirmam que a IA influencia a competitividade empresarial por meio de três dimensões principais. Primeiramente, no âmbito da eficiência operacional, a automação de processos permite a redução de custos e o aumento da produtividade, promovendo maior escalabilidade das operações (Xia *et al.*, 2026). Em segundo lugar, a IA aprimora a qualidade da tomada de decisão, por meio de sistemas preditivos capazes de analisar grandes volumes de dados com elevado grau de precisão. Por fim, destaca-se seu papel na inovação, possibilitando o desenvolvimento de novos produtos, serviços e modelos de negócio, o que reforça a diferenciação competitiva.

Pela teoria econômica clássica (Nelson, 2006), a produtividade de uma empresa é simplesmente determinada pelas tecnologias disponíveis e pelas condições de mercado (fatores externos às firmas). Entretanto, com a IA, há uma percepção difusa de que a vantagem competitiva surge porque, em ambientes de alta intensidade de dados, as empresas que utilizam inteligência artificial conseguem identificar padrões, tendências e oportunidades com mais rapidez e precisão. Isso permite decisões mais informadas, redução de custos operacionais, personalização de produtos e serviços e ciclos de inovação mais curtos. Assim, as organizações se diferenciam, conseguem antecipar mudanças no mercado e entregam valor de forma mais eficiente, dificultando a imitação por concorrentes (Bughin, 2018).

Mas será que a forma como os economistas definem as vantagens competitivas realmente mudou com a IA? Segundo sua teoria das vantagens competitivas, Porter (1985) explora como as empresas podem diferenciar-se

ou obter custos mais baixos para assegurar uma posição sustentável no mercado, definindo estratégias baseadas em diferenciação ou liderança em custos. Essa teoria enfatiza o papel do posicionamento estratégico no setor industrial.

Na Teoria de Porter prevalecem estratégias genéricas básicas para superar os concorrentes e sustentar as vantagens competitivas: produzir com menor custo setorial via eficiência operacional e escala (liderança em custo); ofertar algo único que seja amplamente valorizado pelos clientes, permitindo cobrar um preço *premium* (diferenciação); e concentrar-se em um nicho específico de mercado, em vez de tentar atingir todo o setor (enfoque). A lógica central é evitar o estado de "meio-termo", no qual a organização tenta ser tudo para todos e acaba sem uma vantagem clara. Ao focar na redução sistemática de custos ou na oferta de algo único que o cliente perceba como valioso, a empresa altera o equilíbrio de poder a seu favor em relação a fornecedores, clientes e rivais. Assim, a vantagem competitiva é, essencialmente, a capacidade de uma organização de se posicionar de forma única e valiosa, apoiada por um sistema de atividades perfeitamente integradas que reforçam sua proposta estratégica.

Essa Teoria originalmente focada em diferenciação e custos, necessita ser repensada na era da inteligência artificial, com a IA ampliando a capacidade de análise de dados, personalização e automação. Enquanto o modelo clássico privilegia a estrutura e o posicionamento setorial, a IA redefine a competitividade ao oferecer vantagens dinâmicas, especialmente no uso adaptativo de dados. Essa releitura, porém, deve ser contextualizada nos países emergentes, como o Brasil, onde a capacidade de adaptação tecnológica, a inserção em cadeias globais de valor e a apropriação do conhecimento local podem reconfigurar o conceito de vantagem competitiva, promovendo uma oportunidade de salto competitivo.

Com a releitura da teoria de Porter à luz da inteligência artificial, as empresas passam a focar na capacidade (interna) de processar e analisar grandes volumes de dados, personalizar ofertas e automatizar processos. Em vez de se basearem apenas na estrutura ou no posicionamento setorial, as empresas buscam vantagens competitivas por meio da agilidade na inovação, da capacidade de adaptação e da experimentação contínua. Assim, a vantagem não é mais estática, mas um processo dinâmico, sustentado pela capacidade analítica e pela inovação guiada por IA.

Ao repensar as teorias econômicas sobre as vantagens competitivas, vale notar que o uso da inteligência artificial, por si só, não gera uma vantagem competitiva sustentável, pois a tecnologia tende a se disseminar e nivelar o campo de jogo, ao se tornar acessível a todos paulatinamente. A vantagem se sustenta ao amplificar vantagens já existentes (Bughin *et al.*, 2018). Contudo, quando todas as empresas usam modelos similares de IA, a vantagem competitiva se desloca para o contexto institucional, organizacional e operacional. Ao criticar a visão estática da teoria econômica clássica, Nelson (2006) já enfatizava a importância de analisar as firmas como sistemas sociais, que reagem diferentemente a uma mesma tecnologia, com estratégias e resultados diversos.

Em resumo, a IA pode potencializar vantagens empresariais existentes. Mas, como toda tecnologia, o uso da IA não é neutro, carrega implicações sociais e contextuais desde o seu *design*, e tais implicações e seus riscos precisam ser levados em conta pelas empresas em suas operações internas (Kranzberg, 1986). A governança da IA pode contribuir nessa tarefa.

Para endereçar os riscos da IA na atividade empresarial, é preciso cuidar dos algoritmos e prevenir ou mitigar os riscos advindos do seu uso. Indo mais além, é preciso chegar a uma governança da IA que controle os algoritmos e sustente as vantagens, sob pena das empresas acabarem sendo administradas por eles. Sem esse cuidado, o que se vislumbra como vantagem empresarial pode se tornar um risco sistêmico.

2. A governança da IA e a competitividade empresarial

A governança da IA pode ser definida como o conjunto de princípios, normas e práticas voltadas à orientação e supervisão do desenvolvimento e uso de sistemas de IA (Writz *et al.*, 20220). Trata-se de um campo interdisciplinar que integra aspectos tecnológicos, jurídicos e organizacionais.

A literatura recente enfatiza que uma governança robusta deve operar em múltiplos níveis — técnico, organizacional e institucional —, garantindo transparência, *accountability* e alinhamento ético (Floridi *et al.*, 2025). Ademais, a IA tem sido associada à redução de custos de agência ao ampliar a capacidade de monitoramento e controle dentro das organizações (Yang *et al.*, 2026).

A releitura da teoria de Porter pode conduzir a uma interpretação mais potente do papel da governança aplicada aà IA. Essa interpretação do papel da governança orienta-se pelo reconhecimento da transformação da infraestrutura tecnológica em um ativo estratégico. Nesse sentido, a governança da IA deixa de ser apenas uma camada de conformidade ética ou jurídica para se tornar um componente crítico da cadeia de valor, ao assegurar que a inovação seja segura, escalável e alinhada aos objetivos de diferenciação da empresa. Uma governança robusta permite que a organização mitigue riscos reputacionais e operacionais que poderiam destruir o valor criado, assegurando que o uso de algoritmos e dados proprietários constitua uma barreira de entrada difícil de ser superada pelos concorrentes, fortalecendo assim o posicionamento estratégico proposto por Porter.

Sob a ótica das estratégias genéricas, a governança da IA atua como um catalisador tanto para a liderança em custo quanto para a diferenciação. Ao estabelecer diretrizes claras para a automação inteligente e o processamento de dados, as empresas podem otimizar processos internos com uma precisão que reduz desperdícios de forma sistêmica, mantendo a eficiência operacional. Simultaneamente, a governança ética e transparente pode ser utilizada como um diferencial competitivo, gerando confiança e lealdade em mercados cada vez mais preocupados com a privacidade e o viés algorítmico. Portanto, a integração da governança de IA à estratégia de Porter significa que o controle e a responsabilidade sobre a tecnologia não são custos adicionais, mas investimentos essenciais para proteger e expandir a margem de lucro em um ambiente digital dinâmico.

Em síntese, sob a perspectiva estratégica, a IA constitui recurso crítico para a geração de vantagem competitiva, especialmente em ambientes caracterizados por alta intensidade de dados e inovação contínua. Porém, o aumento da eficiência operacional só será traduzido em mais competitividade se o processamento expandido obtido pela IA não estiver vinculado a um canal de "decisões cegas" tomadas por um algoritmo autoreferenciado, sem possibilidade de uma explicação sujeita ao escrutínio e controle humano. Uma governança falha leva à dependência de modelos que podem "alucinar" ou apresentar erros sistemáticos. A governança robusta garante que a IA seja uma ferramenta de auxílio à decisão humana (*human-in-the-loop*), assegurando que os ganhos de produtividade sejam reais e não baseados em dados enviesados ou errôneos.

Ao ser percebida como um ativo estratégico, a governança passa a ser mais valoriza pelas empresas. A IA pode fornecer ferramentas para informações estrategicamente relevantes e necessárias na consolidação das vantagens competitivas das empresas. Portanto, essa tecnologia pode potencializar a governança corporativa. Mas, ao mesmo tempo, a governança corporativa também é ameaçada pela IA, pois esse aprendizado por máquina pode se tornar um agente autônomo e sem controle, caso os cuidados com a sua *accountability* não sejam bem desenhados e executados, tornado as empreasas "vítimas do seu sucesso". Nossas empresas serão governantes ou governadas pela IA? Ao menos parte dessa pergunta pode ser respondida ao encararmos a governança da IA como uma governança de capacidades dinâmicas. Assim, aquelas empresas mais capacitadas institucionalmente para controlar os algoritmos seriam mais governantes do que governandas, como será visto em seguida.

3. Governantes ou governados?

3.1 A Governança como capacidade dinâmica

Simplesmente definir a governança de IA como um conjunto de processos, políticas e ferramentas que garantem que os sistemas de IA sejam éticos, seguros e transparentes pode não ser suficiente para compreeder a importância das relações institucionais e dos recursos internos na dinâmica da competitividade empresarial. Para amplificar nossa compreensão sobre o real potencial da governança da IA, é preciso tratar a governança como capacidade dinâmica, como indica Teece (1997).

Na estratégia competitiva de Porter, o foco da visão recai sobre a posição externa ou sobre a estrutura das indústrias. Contudo, uma visão encorpada da governança da IA demanda uma estratégia que persiga uma inovação segura, escalável e alinhada aos objetivos de diferenciação da empresa, para controlar o ciclo de vida dos dados relevantes para o seu negócio. Por isso, é preciso buscar uma visão baseada em recursos institucionais. Nesse sentido, é preciso agregar à estratégia mais geral de competição de Porter à Visão Baseada em Recursos (*Resource-Based View*) proposta por Teece (1997), especificamente em sua extensão para as capacidades dinâmicas..

A Visão Baseada em Recursos (RBV) tradicional propõe que a vantagem competitiva de uma empresa não deriva apenas de sua posição externa no mercado, mas principalmente de seus recursos internos (Barney, 1991). Enquanto a análise de Porter foca na "estratégia de fora para dentro", a RBV adota uma perspectiva de "dentro para fora", sugerindo que o desempenho superior é alcançado por meio da posse e controle de ativos estratégicos que os concorrentes não conseguem copiar ou adquirir facilmente. Para que um recurso seja considerado uma fonte de vantagem competitiva sustentável, ele deve atender aos critérios do modelo VRIO: ser valioso (neutraliza ameaças ou explora oportunidades), raro (controlado por poucas empresas), de difícil imitação (caro ou complexo de replicar) e organizado (a empresa possui processos para extrair seu valor). Esses recursos podem ser tangíveis, como infraestrutura e capital, ou intangíveis, como patentes, cultura organizacional, reputação da marca e o conhecimento tácito acumulado pelos colaboradores (Teece, 1997).

A visão de Teece expande a Resource-Based View (RBV) tradicional ao introduzir o conceito de c*apacidades dinâmicas*, argumentando que, em mercados de rápida transição tecnológica, possuir recursos valiosos não basta; é preciso saber reconfigurá-los.

Nesse sentido, a governança da IA deixa de ser um "freio" burocrático e passa a ser a própria capacidade organizacional de sentir, aprender e transformar (*sense, seize and transform*) as oportunidades tecnológicas. A base de raciocínio é que os algoritmos e dados, por si só, são replicáveis; o que gera vantagem é a governança como capacidade dinâmica, ou seja, a habilidade institucional de gerenciar o ciclo de vida dos dados com ética e agilidade, permitindo que a empresa (ou nação) se adapte a mudanças rápidas sem perder a integridade operacional.

No contexto da IA, a capacidade de sentir (*sensing*) refere-se à habilidade da organização em monitorar constantemente o horizonte tecnológico e regulatório. Isso envolve identificar não apenas novas ferramentas de IA, mas também antecipar riscos éticos, vieses algorítmicos e mudanças estratégias antes que se tornem crises, permitindo que a empresa se posicione proativamente em vez de apenas reagir às pressões externas.

A capacidade de aprender (*seizing*) manifesta-se na mobilização de recursos para validar e implementar sistemas de IA de forma segura. Sob uma governança sólida, o aprendizado organizacional foca em transformar *insights* de dados em modelos de decisão que respeitem a integridade e a transparência. Isso exige que a liderança estabeleça protocolos de experimentação onde o aprendizado sobre o comportamento do algoritmo seja compartilhado entre as áreas técnica e jurídica, garantindo que o investimento em IA seja capturado de maneira ética e escalável, evitando a criação de "caixas-pretas" que a própria empresa não consiga gerir.

Por fim, a capacidade de transformar (*transforming*) é o estágio onde a governança da IA se torna parte do DNA estrutural da firma. Trata-se da reconfiguração contínua de ativos tangíveis e intangíveis para alinhar a operação com o novo paradigma digital. Na prática, significa reformar processos internos para que a supervisão hu-

mana e a auditoria algorítmica sejam contínuas, e não apenas uma etapa final. Essa orquestração de recursos permite que a organização mude sua trajetória estratégica com agilidade, mantendo a conformidade regulatória e a legitimidade social enquanto explora novas fronteiras de automação e inteligência.

Essas três capacidades formam um ciclo de *feedback* essencial para a sobrevivência na economia da IA. Enquanto o "sentir" e o "aprender" preparam o terreno para a inovação responsável, a "transformação" garante que a estrutura de governança não se torne rígida ou obsoleta. Em um ambiente no qual os algoritmos evoluem exponencialmente, a vantagem competitiva reside na flexibilidade da organização em manter sua base de recursos alinhada tanto com a eficiência produtiva quanto com os imperativos éticos e legais da governança algorítmica.

Isso posto, vale levar em conta como as estratégias de Porter (2014) podem se complementar com as estratégias de governança da IA. Em um mercado saturado de ferramentas opacas de IA, a diferenciação ocorre por meio da "IA ética". Uma governança ética e com os vieses apurados e corrigidos pode constituir um diferencial reputacional. Se a sua IA explica por que tomou uma decisão (ao contrário do concorrente), você oferece um valor único (transparência e explicabilidade). Além disso, empresas que adotam práticas presentes em *frameworks*, como o NIST ou EU AI Act podem atrair clientes e fornecedores que priorizam a segurança de dados e a responsabilidade social e/ou que estão submetidos a regulações fortes (NIST, 2023; EU AI Act, 2024).

Ao desenvolver capacidades dinâmicas, uma organização pode se tornar a líder de nicho em soluções de IA para diagnóstico médico ou análise de crédito, por exemplo, áreas em que concorrentes generalistas não conseguem operar.

Nos *frameworks* de governança robusta da inteligência artificial, a mitigação do risco de opacidade se dá por meio de princípios como *explicabilidade* e *confiabilidade*. Isso inclui o uso de modelos interpretáveis, a documentação detalhada dos algoritmos, a realização de testes de viés e a criação de comitês de ética. Além disso, *frameworks* como o do NIST recomendam a transparência, ou seja, a publicidade de como os resultados são gerados, e a participação de *stakeholders*, garantindo que os impactos deletérios sejam avaliados e corrigidos.

O *framework* de gestão de riscos de inteligência artificial do NIST, chamado AI RMF 1.0, foi estruturado em princípios de confiança e quatro funções principais: governar, mapear, medir e gerenciar. Ele orienta políticas, identificação de riscos, mensuração e controle. Os princípios de confiança podem ser emulados pelas empresas nas suas estratégias corporativas, sinalizando uma governança mais robusta, independentemente do modelo regulatório adotado por cada país.

Tendo ilustrado como as capacidades dinâmicas das firmas podem afetar a incorporação da tecnologia algorítmica, cabe propor, em linhas gerais, algumas estratégias para que as empresas brasileiras sejam mais governantes do que governadas pela IA.

3.2 A governança como capacidade dinâmica no Brasil

3.2.1 Estratégias

Muitas empresas brasileiras ainda lidam com dados fragmentados, desestruturados e silos de informação, o que impede que modelos de IA gerem *insights* confiáveis. Além disso, a dependência de tecnologias externas pode gerar vulnerabilidades estratégicas, especialmente em economias emergentes como a nossa. O risco de o Brasil ser apenas um "consumidor de ferramentas" em vez de um desenvolvedor de soluções adaptadas à sua realidade econômica alerta para o perigo da IA nas empresas brasileiras acentuar nossa dependência tecnológica em relação aos centros do capitalismo mundial.

As principais barreiras para a governança da inteligência artificial no Brasil incluem falta de infraestrutura de dados, escassez de profissionais qualificados, existência de uma regulação fragmentada e resistência cultural nas organizações. De acordo com o IPEA, a maior necessidade é investir em infraestrutura e capacitação, enquanto o "Plano Brasileiro de Inteligência Artificial" reforça a importância de harmonizar a regulação e incentivar parcerias público-privadas (IPEA, 2023; Brasil, 2025).

Do ponto de vista macroeconômico, o país apresenta baixa produtividade e elevada desigualdade, o que limi-

ta sua competitividade global, mas também cria oportunidades para ganhos expressivos com a adoção de IA. No âmbito microeconômico, observa-se forte heterogeneidade entre empresas, com grande parte das pequenas e médias organizações apresentando baixa maturidade digital.

Esses riscos e barreiras evidenciam a necessidade de uma governança robusta da IA pelas empresas brasileiras.

Estudos da Softex (2025, 2026) e da Estratégia Brasileira de Inteligência Artificial (Brasil, 2021) fornecem elementos para uma análise de impacto da IA. O Brasil possui janelas de oportunidade em setores estratégicos no agronegócio (IA para agricultura de precisão), saúde (IA para diagnósticos preditivos) e segurança eletrônica. Além disso, a capacidade de processar dados locais para oferecer produtos financeiros e de varejo adaptados à diversidade regional brasileira permite cogitar uma personalização de serviços e comércio.

Para mitigar riscos e maximizar benefícios, as empresas devem adotar estratégias integradas de governança de IA. Entre as principais estratégias, destacam-se a implementação de *frameworks* de governança, a realização de auditorias algorítmicas, o desenvolvimento de programas de compliance digital e a criação de estruturas multidisciplinares de supervisão.

Vale reiterar que a governança dinâmica deve ser integrada à estratégia empresarial, sendo tratada como elemento central da competitividade, e não como mera exigência regulatória.

Uma governança dinâmica de IA começa no nível técnico, com práticas de desenvolvimento responsáveis: os modelos precisam ser auditados, explicáveis e testados para reduzir vieses. No nível organizacional, a liderança deve criar políticas claras, com responsabilidades definidas e mecanismos de revisão contínua. Já no nível institucional, a IA deve estar alinhada aos valores da organização e às normas externas, além de se integrar a um sistema de governança maior, com comitês de ética, monitoramento contínuo e canais de transparência. Assim, a confiança dos *stakeholders* é preservada e o alinhamento ético, com responsabilidade social, é garantido.

No mercado de trabalho brasileiro, a IA tem potencial de elevar a produtividade, especialmente em setores como tecnologia, serviços e indústria. Por outro lado, há um risco elevado de aumento da desigualdade salarial no Brasil, com um achatamento salarial em funções técnicas de nível superior e uma valorização desproporcional de uma "elite digital".

Indo além, com uma estratégia dinâmica das responsabilidades no uso da IA, se obtém mais segurança jurídica e conformidade das empresas, antecipadamente ao marco regulatório brasileiro. Isso evita multas e paralisações de operações por uso indevido de dados pessoais ou algoritmos opacos. A conformidade algorítmica torna-se um selo de qualidade para atrair investidores internacionais.

No mercado de capitais, a engenharia institucional das empresas listadas pode mitigar o risco ético. Nesse sentido, conselhos de administração que incorporem comitês de ética em IA estarão mais adaptados para gerir o valor da marca.

Para países emergentes como o Brasil, a ampliação da vantagem competitiva por meio da governança algorítmica ocorreria ao se transformar o ambiente regulatório em um *locus* de confiança e estabilidade, atraindo investimentos e facilitando a inserção em cadeias globais de valor. Uma governança bem estruturada não deve apenas restringir riscos, mas atuar como um mecanismo de renovação adaptativa que permite ao país e as empresas dar saltos tecnológicos ao focar na apropriação do conhecimento local e na soberania de dados. Ao estabelecer padrões éticos e técnicos claros, o Estado e as empresas criam um ecossistema no qual a inovação é incentivada de forma segura, permitindo que setores estratégicos, como o agronegócio e a bioeconomia, utilizem a IA para converter dados regionais em diferenciais competitivos globais, tornando a tecnologia uma alavanca para superar a dependência de *commodities*, por exemplo.

Essa transformação tecnológica em um processo dinâmico depende fundamentalmente do uso estratégico de dados e da celebração de parcerias internacionais que foquem na transferência de tecnologia e no codesenvolvimento. O salto competitivo deixa de ser uma meta estática e passa a ser uma capacidade de resposta contínua, na qual o desenvolvimento tecnológico é tratado como uma necessidade de sobrevivência e, simultaneamente, uma janela de oportunidade para redefinir o papel do país no comércio mundial. Por meio da colaboração entre o setor público e privado, o Brasil pode utilizar a IA para otimizar suas vantagens comparativas naturais, transformando-as em vantagens competitivas

de alto valor agregado. Assim, a governança da IA funciona como o motor de uma estratégia nacional que não apenas consome tecnologia estrangeira, mas a adapta e a integra de forma inteligente para fortalecer a resiliência econômica e a produtividade no longo prazo.

Em seguida, sugere-se que a governança como capacidade dinâmica pode ser aplicada no contexto nacional, para diferenciar positivamente as organizações brasileiras.

3.2.2 Capacidades dinâmicas

A aplicação das capacidades dinâmicas de Teece à realidade das empresas brasileiras exige uma "tropicalização" da teoria, especialmente devido à nossa condição de economia emergente e à dependência tecnológica de centros globais (como o Vale do Silício ou a China). Em contextos de dependência, a vantagem competitiva não nasce necessariamente da invenção de uma nova tecnologia, mas da agilidade em orquestrar recursos externos. Nesse sentido, os três pilares de Teece (sentir, aprender e transformar) são traduzidos para o cenário brasileiro.

Para uma empresa brasileira, "sentir" raramente significa descobrir uma nova fronteira da física ou da IA generativa. Significa ter uma *capacidade de absorção* aguçada para identificar quais tecnologias desenvolvidas no exterior podem ser adaptadas aos gargalos locais. Nomeadamente, o sucesso das *fintechs* brasileiras veio da *sensibilidade* acerca do engessamento do sistema bancário centralizado no Brasil. Elas não inventaram o cartão de crédito ou o *app*, mas "sentiram" a oportunidade de aplicar essas tecnologias para resolver o problema da desbancarização e das altas taxas de juros locais.

Em economias dependentes, o "apreender" está fortemente ligado à capacidade de integrar tecnologias importadas em modelos de negócio locais. Como as empresas brasileiras muitas vezes não possuem o capital para desenvolver *hardware* de ponta, a estratégia foca em integração e parcerias estratégicas. Nesse cenário, "apreender" uma oportunidade de IA, por exemplo, exige uma governança de dados que permita o uso de infraestruturas de nuvem estrangeiras, sem perder a soberania ou a conformidade com a Lei Geral de Proteção de Dados (2018), adquirindo conhecimento a partir e além das plataformas de terceiros, para gerar serviços eficientes e úteis em nossos mercados.

A capacidade dinâmica de transformação em países como o Brasil é marcada pelo que Teece chama de reconfiguração de ativos para lidar com a volatilidade institucional (mudanças bruscas de câmbio, impostos e leis). Assim, essa capacidade traz resiliência, pois, enquanto empresas de países desenvolvidos focam em otimizar processos estáveis, as brasileiras usam a transformação para criar flexibilidade. Para fins de ilustração, a empresa precisa ser capaz de abandonar processos defasados rapidamente e adotar automação algorítmica para manter a margem de lucro, quando o custo de importação de tecnologia sobe devido ao câmbio ou ao aumento de impostos.

Nessa leitura, a governança da inteligência artificial no Brasil deve ser vista como uma capacidade organizacional de curadoria: saber o que importar, como governar algoritmos "comprados" para que atendam à nossa realidade ética/social e como manter a empresa ágil para trocar de fornecedor tecnológico se as condições econômicas mudarem.

Conclusão

A IA constitui elemento central da competitividade empresarial contemporânea, mas sua adoção eficiente depende da existência de estruturas robustas de governança, baseadas nas capacidades institucionais dinâmicas das firmas.

No contexto brasileiro, essa necessidade é ainda mais relevante, diante das limitações estruturais e das oportunidades de transformação digital.

Conclui-se que a governança de IA deve ser compreendida como ativo estratégico essencial, capaz de promover não apenas eficiência e inovação, mas também sustentabilidade e legitimidade empresarial.

Referências

BARNEY, Jay. Firm Resources and Sustained Competitive Advantage. *Journal of Management*, [*S. l.*], v. 17, n. 1, p. 99-120, 1991. DOI: https://doi.org/10.1177/014920639101700108.

BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 abr. 2026.

BRASIL. *Portaria MCTI nº 4.979, de 13 de julho de 2021*. Altera o Anexo da Portaria MCTI nº 4.617, de 6 de abril de 2021, que institui a Estratégia Brasileira de Inteligência Artificial e seus eixos temáticos. Brasília, DF: Ministério da Ciência, Tecnologia e Inovações, 2021. Disponível em: https://www.in.gov.br/web/dou/-/portaria-mcti-n-4.979-de-13-de-julho-de-2021-332164912. Acesso em: 26 out. 2026.

BRASIL. Ministério da Ciência, Tecnologia e Inovação. *IA para o bem de todos*: Plano Brasileiro de Inteligência Artificial. Brasília, DF: MCTI; CGEE, 2025. Disponível em: https://www.gov.br/mcti/pt-br/centrais-de-conteudo/publicacoes-mcti/plano-brasileiro-de-inteligencia-artificial/pbia_mcti_2025.pdf. Acesso em: 14 abr. 2026.

BUGHIN, Jacques; SEONG, Jeongmin. How Competition Is Driving AI's Rapid Adoption. Harvard Business *Review*, [*S. l.*], 17 out. 2018. Disponível em: https://hbr.org/2018/10/how-competition-is-driving-ais-rapid-adoption. Acesso em: 17 abr. 2026.

CHAAR, T. et al. AI and the global productivity divide: fuel for the fast or a lift for the laggards? *OECD Artificial Intelligence Papers*, [*S. l.*], n. 51, p. 1-45, 2025. DOI: https://doi.org/10.1787/c315ea90-en.

BRASIL. Ministério da Ciência, Tecnologia e Inovações. *Estratégia Brasileira de Inteligência Artificial*: Pilares de Inovação e Governança Ética. Brasília, DF: MCTI, 2021. Disponível em: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/estrategia-brasileira-de-inteligencia-artificial. Acesso em: 26 out. 2026.

UNIÃO EUROPEIA. *Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024*. Estabelece regras harmonizadas em matéria de inteligência artificial e altera os Regulamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e as Diretivas 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (Regulamento Inteligência Artificial). Jornal Oficial da União Europeia, Bruxelas, L 2024/1689, 12 jul. 2024. Disponível em: https://eur-lex.europa.eu/eli/reg/2024/1689/oj. Acesso em: 26 out. 2026.

BATOOL, Amna; ZOWGHI, Didar; BANO, Muneera. AI governance: a systematic literature review. *AI and Ethics*, [*S. l.*], v. 5, n. 3, p. 3265-3279, 2025. DOI: https://doi.org/10.1007/s43681-024-00653-w.

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA (IBGE); AGÊNCIA BRASILEIRA DE DESENVOLVIMENTO INDUSTRIAL (ABDI); UNIVERSIDADE FEDERAL DO RIO DE JANEIRO (UFRJ). *Pesquisa de Inovação Semestral*: indicadores básicos 2024. Rio de Janeiro: IBGE, 2026. Disponível em: https://biblioteca.ibge.gov.br/visualizacao/livros/liv102260.pdf. Acesso em: 14 abr. 2026.

INSTITUTO DE PESQUISA ECONÔMICA APLICADA. *IA*: Infraestrutura e capacitação são as maiores necessidades atualmente, alertam especialistas em debate no Ipea. Brasília, DF: Ipea, 2024. Disponível em: https://www.ipea.gov.br/portal/categorias/45-todas-as-noticias/noticias/15371-ia-infraestrutura-e-capacitacao-sao-as-maiores-necessidades-atualmente-alertam-especialistas-em-debate-no-ipea. Acesso em: 26 out. 2026.

INSTITUTO DE PESQUISA ECONÔMICA APLICADA. Ocupações com maior qualificação e especialização são mais suscetíveis aos impactos da IA, diz estudo. *Ipea*, Brasília, DF, 9 out. 2023. Disponível em: https://www.ipea.gov.br. Acesso em: 14 abr. 2026.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. *Information technology – Artificial intelligence – Guidance on risk management*. ISO/IEC 23894:2023. Genebra: ISO, 2023. 26 p.

KRANZBERG, Melvin. Technology and History: 'Kranzberg's Laws'. *Technology and Culture*, [*S. l.*], v. 27, n. 3, p. 544-560, jul. 1986. DOI: https://doi.org/10.2307/3105385.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*. Gaithersburg: NIST, 2023. Disponível em: https://www.nist.gov/AIRMFramework. Acesso em: 17 abr. 2026.

NELSON, Richard R. *As fontes do crescimento econômico*. Tradução: Adriana Gomes de Freitas. Campinas, SP: Ed. Unicamp, 2006.

PORTER, Michael E.; HEPPELMANN, James E. How Smart, Connected Products Are Transforming Competition. Harvard *Business Review*, [*S. l.*], v. 92, n. 11, p. 64-88, nov. 2014.

PORTER, Michael E. *Competitive Advantage:* Creating and Sustaining Superior Performance. New York: Free Press, 1985.

TEECE, David J.; PISANO, Gary; SHUEN, Amy. Dynamic capabilities and strategic management. Strategic *Management Journal*, [*S. l.*], v. 18, n. 7, p. 509-533, 1997. DOI: https://doi.org/10.1002/(SICI)1097-0266(199708)18:7<509::AID-SMJ882>3.0.CO;2-Z.

WIRTZ, Bernd W.; WEYERER, Jan C.; GEYER, Carolin. *Toward AI governance: best practices and barriers.* Information Systems Frontiers, 2022.

SOFTEX. *Panorama IA* – Caderno 2: Estratégia e Competitividade. [*S. l.*]: Observatório Softex, 2026. Disponível em: https://observatorio.softex.br/publicacao-geral/ia-na-estrategia-de-negocios/. Acesso em: 26 out. 2026.

XIA, Huosong; CHEN, Hao; ZHANG, Justin Zuopeng; KAMAL, Muhammad Mustafa. Exploring the impact of responsible AI governance on corporate performance: a quasi-natural experiment. *Technological Forecasting and Social Change*, [*S. l.*], v. 223, art. 124425, 2026. DOI: https://doi.org/10.1016/j.techfore.2025.124425.

YANG, Jingxuan. How artificial intelligence improves corporate governance: evidence from the ERNIE large model. *Finance Research Letters*, [*S. l.*], v. 96, p. 109782, 2026. DOI: https://doi.org/10.1016/j.frl.2026.109782.

Inteligência Artificial, algoritmos e ética:

o novo desafio do compliance

Igor Mateus Lopes da Silva

Igor Mateus Lopes da Silva é Compliance Officer e DPO na SBM Offshore no Brasil. Atua com compliance corporativo, privacidade, investigações internas, due diligence de terceiros e gestão de riscos, com experiência anterior empresas de consultoria e auditoria e escritórios de advocacia, além de formação complementar EXIN em proteção de dados e CPIIC em investigações internas. Além de sua atuação profissional na área de compliance e proteção de dados, é escritor e autor de romance publicado.

Introdução

Recentemente, ficou cada vez mais constatado que estamos, definitivamente, na era da Inteligência Artificial (IA). De um "*summer camp*" em 1956[1] até tornar-se ajudante de um estudante comum em 2026 com temáticas triviais, é notável o quanto a IA já está presente na vida cotidiana, seja em meio a nossos trabalhos, relações ou até mesmo no âmbito de governos nacionais. Essa expansão, impulsionada sobretudo pelo avanço de modelos generativos e pelo investimento massivo[2] de empresas desenvolvedoras, promete ganhos expressivos de eficiência, inovação e produtividade.

Contudo, são também crescentes os questionamentos sobre a forma como tal expansão da IA pode vir a afetar ou, em última análise, guiar decisões humanas e, na medida em que estas máquinas forem capazes de substituir parte da atuação humana, como estas poderão impactar também as organizações.

Nesse cenário, o presente artigo busca discutir o fator ético com relação à adoção de mecanismos de inteligência artificial pelas organizações. Quanto desejamos que a ética dessas microssociedades seja influenciada pela IA, com a contrapartida de ganhos tecnológicos ou econômicos? A análise ética dessas máquinas precisa levar em conta que sua atuação não é neutra. Ao contrário, são construídas com base em algoritmos que podem trazer consigo graves distorções à cultura organizacional, tanto do ponto de vista individual como do que a organização deseja como modelo ético.

A problemática torna-se ainda mais relevante quando se observa que muitas organizações, ao adotarem soluções de inteligência artificial desenvolvidas por terceiros, trazem para dentro de si modelos éticos de terceiros que podem estar em descompasso com seus modelos éticos construídos ao longo de anos. A pergunta fica: devemos nós confiar em uma máquina que nos ajuda a decidir e a formular nossos pensamentos e análises a tal ponto que esta ajuda se confunde com a tomada de decisão em si?

Dessa forma, após breve apresentação conceitual, este artigo buscará discutir a ética na adoção de mecanismos de IA nas organizações e, por fim, discutir o papel do compliance nessa empreitada com vistas a uma governança eficaz, tentando visualizar como essa função tão relevante para a ética das organizações deverá se adaptar a essa nova era.

1. Inteligência artificial e sua aplicabilidade

Conceitos essenciais

Nos últimos anos foi notório o aumento da adoção da inteligência artificial no Brasil, sendo esta visualizada de maneira significativa em contextos diversos, tais como na implementação em empresas e governos[3], assim como na utilização por usuários individuais até mesmo de maneira trivial, já que é possível encontrar usuários que utilizam a inteligência artificial em aplicativos simples de *smartphones* para tarefas diversas.

Dessa forma, a fim de elucidar a discussão futura, entende-se como proveitoso trazer o conceito de quatro atores-chave desse ramo, para que não haja entendimentos variados acerca do que é essa tecnologia. Tais atores são: a) inteligência artificial; b) algoritmos; c) aprendizado de máquina; d) inteligência artificial generativa.

---

[1] SOBREIRA, Victor. Um panorama da História da Inteligência Artificial e suas aplicações na pesquisa histórica. Varia Historia, Belo Horizonte, v. 41, e25035, 2025. DOI: https://doi.org/10.1590/0104-87752025v41e25035.

[2] GARTNER. Gartner says worldwide AI spending will total $2.5 trillion in 2026. *Gartner*, Stamford, 15 jan. 2026. Disponível em: https://www.gartner.com/en/newsroom/press-releases/2026-1-15-gartner-says-worldwide-ai-spending-will-total-2-point-5-trillion-dollars-in-2026. Acesso em: 11 jun. 2026.

[3] BARBOSA, Leonardo Figueiredo; PINHEIRO, Caroline da Rosa. Inteligência artificial no Brasil: avanços regulatórios. *Revista de Informação Legislativa*: RIL, Brasília, DF, v. 60, n. 240, p. 11-41, out./dez. 2023. Disponível em: https://www12.senado.leg.br/ril/edicoes/60/240/ril_v60_n240_p11. Acesso em: 26 out. 2026.

Inteligência Artificial ("IA") é, segundo Russel e Norvig (2013 *apud* Barbosa *et al.*, 2023)[4], a capacidade que a máquina tem de interpretar dados de forma racional e humana, a fim de tomar decisões autônomas fundamentadas em padrões. Ademais, o EU IA Act define um sistema de IA como:

> um sistema baseado em máquinas projetado para operar com diferentes níveis de autonomia e que pode demonstrar capacidade de adaptação após a implantação; além disso, com base em objetivos explícitos ou implícitos, o sistema infere, a partir dos dados de entrada que recebe, como gerar resultados, tais como previsões, conteúdos, recomendações ou decisões, que podem influenciar ambientes físicos ou virtuais[5] (EU IA Act, 2024).

Dessa forma, percebe-se que a IA e um sistema de IA são tecnologias que buscam espelhar ou permitir a execução de tarefas que normalmente seriam realizadas por nós, humanos, tais como tomada de decisão, escrita, pesquisa etc. Contudo, para tal, tais máquinas necessitam de uma forma de programação para que possam cumprir com sua função. Esta dita forma de programação trata-se dos algoritmos, que são instruções complexas realizadas pela máquina e que definem as formas de funcionamento dos modelos de IA[6]. Para Kaufman, os algoritmos são a matemática da IA[7] e constituem um conjunto de instruções que permite que uma sequência de tarefas alcance um resultado em um tempo limitado.

Conforme exposto, portanto, os algoritmos povoam as IAs a fim de que estas possam, de fato, executar os propósitos envisionados em seu desenvolvimento.

Soma-se a esses conceitos o campo do aprendizado de máquina, que se refere a, segundo Géron[8], a ciência da programação de computadores de modo que eles possam aprender com os dados. Ou seja, o aprendizado de máquina é uma subcategoria da inteligência artificial, que permite a dispensação da programação para uma tarefa específica e que as máquinas aprendam sozinhas, a partir de dados.

Tal brilhante ciência permite o conceito de IA generativa, que transforma as IAs em máquinas que conseguem realizar previsões a adaptações de padrões a tecnologias que desenvolvam conteúdos completamente novos, fundamentados nos dados com os quais foram treinados[9]. São possíveis diversas formas de ensinar esta IA generativa e fazê-la se desenvolver. Contudo, tais formas não serão o ponto deste artigo. A ideia principal é nos atermos aos conceitos-base para que possamos elucidar as discussões futuras.

[4] IDEM, p. 12.

[5] UNIÃO EUROPEIA. Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024. Estabelece regras harmonizadas em matéria de inteligência artificial e altera os Regulamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e as Diretivas 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (Regulamento da Inteligência Artificial). *Official Journal of the European Union*: série L, v. 2024/1689, 12 jul. 2024.

[6] BORDIGNON, Gabriel Barros. Algoritmos, inteligência artificial e software livre na contemporaneidade: reflexões a partir de Fundação de Isaac Asimov. *Aurora*. Revista de Arte, Mídia e Política, São Paulo, v. 15, n. 43, p. 24-44, 2022. DOI: https://doi.org/10.23925/1982-6672.2022v15i43p24-44.

[7] KAUFMAN, Dora. Inteligência artificial: repensando a mediação / Artificial intelligence: rethinking mediation. *Brazilian Journal of Development*, Curitiba, v. 6, n. 9, p. 67621-67639, 2020. DOI: https://doi.org/10.34117/bjdv6n9-264.

[8] GÉRON, Aurélien. *Mãos à obra*: aprendizado de máquina com Scikit-Learn, Keras & TensorFlow: conceitos, ferramentas e técnicas para a construção de sistemas inteligentes. 3. ed. Tradução de Eveline Machado. Rio de Janeiro: Alta Books, 2025.

[9] CARLE, Eben. Ask a Techspert: what is generative AI? *Google Blog*, [*S. l.*], 10 abr. 2023. Disponível em: https://blog.google/company-news/inside-google/googlers/ask-a-techspert/what-is-generative-ai/. Acesso em: 11 jun. 2026.

2. Adoção de mecanismos de IA nas organizações

A fim de reforçar o argumento acima de que a adoção da inteligência artificial no Brasil e no mundo foi notória nos últimos anos, é necessário trazer dados que demonstrem essa massiva adoção. Importante destacar, contudo, que adoção não significa maturidade.

Uma pesquisa realizada em 2025 pela McKinsey & Company, com 1.993 empresas, concluiu que 88% das organizações dos mais diferentes setores estão reportando que utilizam IA de maneira regular, e que 79% das organizações estão utilizando a IA generativa de maneira regular. Além disso, cerca de 33% das organizações desse estudo responderam que estão escalando a adoção de agentes de IA dentro de suas organizações[10].

Em pesquisa realizada pela Microsoft, foi identificado que nos Emirados Árabes Unidos cerca de 64% da população em idade produtiva utilizava IA no final de 2025. Países europeus como a França e a Noruega não se encontram muito atrás nessa estatística, com cerca de 44% e 46,4%, respectivamente[11].

No Brasil, especificamente, uma pesquisa conduzida pela Associação Brasileira de Inteligência Artificial e Ecommerce (ABIACOM), que contou com a participação de mais de 200 organizações, demonstrou que a adoção no Brasil ainda é relativamente baixa. Cerca de 38,4% das empresas responderam que utilizam ferramentas de IA de forma oficial, enquanto 40,1% informaram que não utilizam[12].

Um contraste interessante é que, apesar do número ainda não tão elevado nas organizações brasileiras, é surpreendente a adoção de maneira individual, principalmente das IAs generativas, como ChatGPT, Gemini, Copilot etc. A adoção do ChatGPT, por exemplo, é maior no Brasil do que nos Estados Unidos[13], diz um relatório do Fórum Mundial acerca da adoção de IA na América Latina. Ademais, o mesmo relatório conclui que um grande desafio nacional é transformar essa adoção individual em práticas reais de produtividade no mercado de trabalho[14].

É claro, portanto, que a adoção de IA está em rápida ascensão no mundo, com desafios na transformação da adoção individual em modelos de negócios e na democratização dessa adoção em países ainda em desenvolvimento e que possuem diversos desafios internos.

[10] SINGLA, Alex; SUKHAREVSKY, Alexander; YEE, Lareina; CHUI, Michael; HALL, Bryce; BALAKRISHNAN, Tara. *The state of AI in 2025*: agents, innovation, and transformation. [*S. l.*]: McKinsey & Company, 5 nov. 2025. Disponível em: https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai. Acesso em: 26 out. 2026.

[11] MICROSOFT. *Global AI adoption in 2025*: a widening digital divide. [*S. l.*]: Microsoft AI Economy Institute, jan. 2026. Disponível em: https://www.microsoft.com/en-us/research/wp-content/uploads/2026/01/Microsoft-AI-Diffusion-Report-2025-H2.pdf. Acesso em: 11 jun. 2026.

[12] ASSOCIAÇÃO BRASILEIRA DE INTELIGÊNCIA ARTIFICIAL E E-COMMERCE; BRAZIL PANELS; LIDERES.AI. *Pesquisa Inteligência Artificial nas empresas brasileiras*. São Paulo: ABIACOM, 2025. Disponível em: https://abiacom.org/wp-content/uploads/2026/01/Pesquisa-ABIACOM-IA-2025.pdf. Pg. 2. Acesso em: 11 jun. 2026.

[13] WORLD ECONOMIC FORUM; McKINSEY & COMPANY. *Latin America in the Intelligent Age*: a new path for growth. Geneva: World Economic Forum, jan. 2026. Disponível em: https://www.weforum.org/publications/latin-america-in-the-intelligent-age-a-new-path-for-growth/. Pg. 13. Acesso em: 11 jun. 2026.

[14] Ibidem.

3. Ética e Modelos Organizacionais

3.1 A IA na tomada de decisões e a problemática dos algoritmos

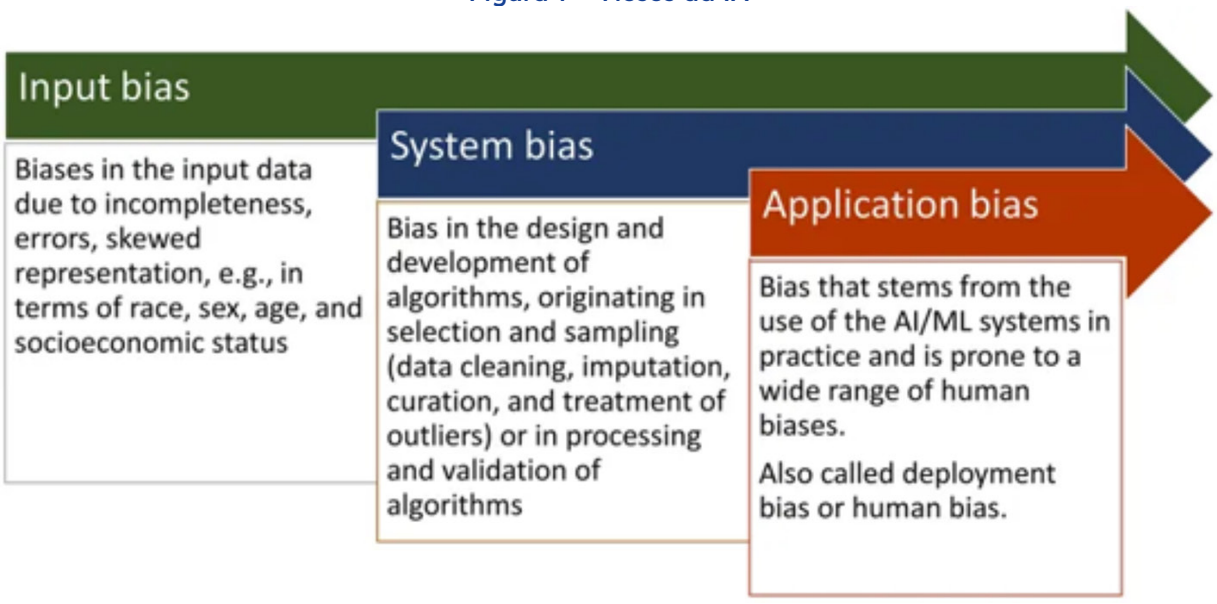
Considerando os principais conceitos explicitados acima, precisamos entender que a IA não somente traz resultados de desempenho. A IA tem a capacidade de impactar organizações, dar suporte ou influenciar decisões humanas e, consequentemente, pender o padrão ético de uma organização. É crescente o número de debates acerca até mesmo do quanto esse novo impacto tecnológico pode mudar todo o conceito ou essência do trabalho humano.

A reflexão sobre o impacto das IAs é necessária, portanto, principalmente no processo de tomada de decisão, e nasce do seguinte questionamento: como as IAs de fato pensam? Devemos nós confiar em uma máquina que nos ajuda a decidir e a formular nossos pensamentos e análises a tal ponto que essa ajuda se confunde com a tomada de decisão em si? Tais perguntas somente podem encontrar alguma espécie de resposta se nos debruçarmos sobre o que está por trás das IAs, sua forma de aprendizado e os chamados algoritmos, mencionados no capítulo anterior.

Os algoritmos de IA, ao popularizarem e desenvolverem cada vez mais essas máquinas inteligentes, possuem a capacidade de impactar drasticamente a mediação e a comunicação dos seres humanos[15]. Isso fica evidente quando analisamos mecanismos de inteligência artificial na sugestão de conteúdo em redes sociais ou em aplicativos de *streaming*.

Contudo, é preciso perceber que esses algoritmos não são construídos de maneira perfeita, ou seja, sem nenhuma sombra de erro ou falha. Existem extensas pesquisas sobre a conceituação de vieses e até mesmo sobre sua classificação em vieses chamados de *input biases*, *system biases* e *application biases*[16]. A Figura 1 abaixo conceitua a diferença entre eles.

Figura 1 – Vieses da IA



Fonte: Hofmann B (2025) Biases in AI: acknowledging and addressing the inevitable ethical issues. Front. Digit. Health 7:1614105. doi: 10.3389/fdgth.2025.1614105. pg 4.

[15] KAUFMAN, Dora. Inteligência artificial: repensando a mediação / Artificial intelligence: rethinking mediation. *Brazilian Journal of Development*, Curitiba, v. 6, n. 9, p. 67621-67639, 2020. DOI: https://doi.org/10.34117/bjdv6n9-264.

[16] HOFMANN, Bjørn. Biases in AI: acknowledging and addressing the inevitable ethical issues. Frontiers in *Digital Health*, [*S. l.*], v. 7, artigo 1614105, 2025. DOI: https://doi.org/10.3389/fdgth.2025.1614105.

De forma prática, podemos utilizar vários exemplos de vieses aplicados em IAs que se tornaram notórios, como, por exemplo, o da IA generativa de imagens *Midjourney*. Uma pesquisa conduzida identificou diversos vieses no processo de geração de imagens, com resultados que reforçam estereótipos ou fortalecem vieses de gênero ou raciais[17].

Em resumo, essas tecnologias estão se tornando mais e mais como atores ativos em nossas vidas, capazes de influenciar ou até mesmo tomar decisões que eram, anteriormente, somente feitas por humanos[18]. Como vamos lidar com esse fato será objetivo de discussão futura deste artigo.

3.2 Qual ética desejamos aceitar em nossas organizações?

Já que, conforme demonstrado, não podemos falar de uma IA infalível ou neutra, precisamos compreender que essa mesma máquina causará impactos nas tomadas de decisão, como já tem sido identificado.

Segundo Madanchian e Therdoost, a adoção de IA envolve responsabilidades sociais, éticas e regulatórias. Conforme a IA for sendo implementada, organizações precisam lidar com problemas éticos significativos[19]. Dessa forma, tendo em vista todo esse impacto e a necessidade de mudanças rápidas e constantes, precisamos refletir sobre isso em nossas organizações e perguntarmos: qual é a IA e a ética por trás daquelas que desejamos aceitar?

Como a maioria das organizações não irá desenvolver ou construir sistemas de IA[20], seja por decisões internas, setor de mercado ou dificuldades próprias para geração de infraestrutura e construção, precisamos lidar com o fato de que estamos, na maioria dos casos, abrindo as portas de nossas organizações para uma máquina com potencial de impactar nossa cultura interna e as decisões tomadas por cada um de nossos funcionários. Máquinas estas que, conforme exposto acima, podem estar recheadas de vieses ou, até mesmo, de algoritmos propositalmente errôneos ou mal-intencionados.

Imaginemos um cenário hipotético em que uma empresa que luta contra uma espécie de discriminação específica venha a perceber que muitos de seus funcionários passaram, inadvertidamente, a replicar esse traço comportamental indesejado por estarem dependendo ou confiando demais nas próprias decisões tomadas com auxílio de uma IA mal construída e adaptada sem restrições no dia a dia da empresa. Imagine pequenos jargões, e-mails, comentários e revisões tendenciosas realizadas sem que se percebesse claramente o que estava gerando a perpetuação e piora do problema. Anos de esforços direcionados a conter esse comportamento podem ser desperdiçados por uma falta de cuidado ao entender o que estava sendo trazido para dentro de casa.

Ou seja, é de extrema importância que as organizações tenham a capacidade de frear por um segundo a onda massiva de adoção de IA e refletir de maneira genuína sobre o que desejam trazer para dentro de suas organizações, considerando não somente os aspectos de melhoria de performance, redução de custos, inovação ou desenvolvimento, mas também quanto a adoção dessas máquinas pensantes irá modificar seu ambiente interno, a ética de seus funcionários, sua cultura e capacidade de cumprir com as legislações aplicáveis e, em última análise, seus produtos, seus serviços e até mesmo sua reputação.

---

[17] THOMSON, T. J.; THOMAS, Ryan J. Ageism, sexism, classism and more: 7 examples of bias in AI-generated images. *The Conversation*, [*S. l.*], 9 jul. 2023. Disponível em: https://theconversation.com/ageism-sexism-classism-and-more-7-examples-of-bias-in-ai-generated-images-208748. Acesso em: 11 jun. 2026.

[18] MADANCHIAN, M.; TAHERDOOST, H. Ethical theories, governance models, and strategic frameworks for responsible AI adoption and organizational success. *Frontiers in Artificial Intelligence*, [*S. l.*], v. 8, artigo 1598979, 16 jul. 2025. DOI: https://doi.org/10.3389/frai.2025.1598979.

[19] IDEM.

[20] TULLY, Tim; REDFERN, Joff; DAS, Deedy; XIAO, Derek. *2025*: the state of generative AI in the enterprise. [*S. l.*]: Menlo Ventures, 8 dez. 2025. Disponível em: https://menlovc.com/perspective/2025-the-state-of-generative-ai-in-the-enterprise/. Acesso em: 11 jun. 2026.

4. O papel do *compliance*

O compliance nas empresas, geralmente concentrado em departamentos de compliance independentes ou atrelados hierarquicamente a outros departamentos, como o departamento jurídico, construíram-se ao longo da história como um balizador da ética empresarial e das normas e regulações internas, construindo uma espécie de regulador da ética dentro dessa pequena sociedade que chamamos de organização empresarial. Os esforços desse departamento, portanto, promovem uma atuação ilibada, buscando a melhor forma de combater inconformidades dentro das organizações, seja por meio de aplicação de políticas, promoção de cultura ou outras formas palpáveis, como treinamentos e auditorias[21].

Francisco José Turra também ensina que o programa de compliance opera em dois sentidos: como um instrumento de prevenção ao descumprimento de regras da empresa, em especial as de cunho ético e as que servem de parâmetro à governança corporativa[22] e também no combate anticorrupção.

Ademais, foi notável nos últimos anos o alargamento do escopo dos programas de compliance e, consequentemente, da atuação dos departamentos internos e do profissional relacionado ao compliance. Devido à sua premissa relativamente aberta de cumprimento de normas e legislações, mas também da guarda ética, a função do compliance estendeu-se para além do combate anticorrupção e do estabelecimento e da aplicação de políticas para se tornar, também, um ator estratégico na implementação e no fortalecimento da cultura da organização, assim como também um promotor de iniciativas de igualdade e diversidade, iniciativas ESG, com um olhar relevante para sustentabilidade. Mais recentemente, o compliance também passou a adicionar em seus quadros especialistas de privacidade e proteção de dados e a atuar como um guardião e operador da LGPD e da segurança da informação. E, dentro dessa toada, também a adicionar a salvaguarda com relação à IA e suas aplicações éticas.

É claro que, do ponto de vista técnico e operacional, os departamentos de TI são *stakeholders* importantes para lidar com essas máquinas. Contudo, não é possível ignorar o papel do compliance no desdobramento ético e comportamental das IAs.

Assim, fica evidente que o profissional e a função em si do compliance estão passando por mudanças constantes e que se demandará uma forte capacidade de adaptação, inovação e influência nas organizações[23].

Além disso, quanto ao desafio específico do compliance com relação às IAs, estes estarão situados na dimensão ética de lidar com uma potencial mudança no comportamento e na tomada de decisão de seus funcionários, que pode ser causada pelas questões técnicas explicadas e exemplificadas nos tópicos anteriores deste artigo. Dessa forma, caberá ao compliance pavimentar a ética desejada da organização no que tange à adoção da IA. Auxiliada pela alta liderança, a função de compliance deverá coordenar um trabalho que permita estabelecer uma governança capaz de, primeiramente, entender os preceitos éticos adotados nas IAs, estabelecer os limites desejados e não desejados, adaptar procedimentos

[21] SOBREIRA FILHO, Enoque Feitosa; LEITE, Flavia Piva Almeida; MARTINS, José Alberto Monteiro. Ética empresarial como base de sustentação do programa de compliance: uma breve análise sobre a ética, a integridade e o compliance. *Relações Internacionais no Mundo Atual*, Curitiba, v. 2, n. 23, p. 99-125, 2019. DOI: https://doi.org/10.21902/Revrima.v2i26.3891.

[22] TURRA, Francisco José. *O uso da Inteligência Artificial no compliance anticorrupção corporativo*. Ponta Grossa: Atena Editora, 2024. Disponível em: https://educapes.capes.gov.br/bitstream/capes/744825/1/o-uso-da-inteligencia-artificial-no-compliance-anticorrupcao-corporativo.pdf. Acesso em: 12 jun. 2026.

[23] VON ANCKEN, Hugo Alberto. Os profissionais do futuro em legal e compliance. *JOTA*, [*S. l.*], 15 maio 2025. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/legal-business/os-profissionais-do-futuro-em-legal-e-compliance. Acesso em: 11 jun. 2026.

já existentes, tais como processos de *due diligence* e investigações internas, e também a adaptação da própria forma de análise, questionando-se sobre o impacto real dessas máquinas no comportamento humano e na tomada de decisão. Qual IA desejamos? O que desejamos que ela impacte? Quais dados precisamos flexibilizar? Qual o nosso objetivo real com a adoção desse instrumento?

Todas essas perguntas são imprescindíveis para que este momento de adoção de mecanismos de IA seja realizado de maneira racional, direcionada e, sobretudo, ética.

Conclusão

Tendo em vista o exposto ao longo deste artigo, a IA já faz parte da vida cotidiana, tanto no aspecto do uso individual como dentro das organizações. Assim, é evidente que sua utilização crescente tenderá a impactar, cada vez mais, a tomada de decisão e as atividades conduzidas.

Foi possível visualizar também, a partir da análise dos conceitos essenciais de inteligência artificial, que essas máquinas não podem ser encaradas de maneira leviana. Ao contrário, são sistemas desenvolvidos de maneira complexa, com grande contexto em seus bastidores de desenvolvimento, que podem refletir vieses, falhas, limitações e objetivos nem sempre alinhados aos desejos dos usuários.

Nesse sentido, a principal preocupação das organizações não deve ser apenas identificar como a IA pode gerar ganhos de produtividade ou econômicos, mas compreender qual tipo de influência essas ferramentas exercerão sobre seus processos internos, sua cultura, suas decisões e seus colaboradores. A depender da IA escolhida e da forma como ela é utilizada pela organização, pode haver um descompasso entre a cultura organizacional e suas escolhas éticas e a forma como a IA pode impactar a organização.

Com isso em mente, a função de compliance assume papel relevante. Se historicamente a função de compliance consolidou-se como guardiã da ética empresarial, evoluindo sua abordagem além das normas de combate à corrupção, passando por outras áreas, como ESG e proteção de dados, o avanço da IA gera a necessidade que essa função reforce sua principal característica, a fim de executar a análise dos impactos éticos da adoção das IAs.

Dessa forma, caberá ao compliance, em conjunto com a alta liderança e demais áreas relevantes, auxiliar na construção de uma governança de IA que seja capaz de avaliar não apenas a funcionalidade das ferramentas adotadas, mas também seus possíveis efeitos sobre a cultura organizacional, a tomada de decisão, os processos internos e a reputação da empresa.

Por fim, a adoção da inteligência artificial nas organizações deve ser acompanhada de uma reflexão ética responsável. A pergunta central não deve ser apenas se a IA pode ser utilizada, mas qual IA se deseja permitir dentro da organização, sabendo-se que ela já está sendo utilizada, e discutir quais finalidades, sob quais controles e em alinhamento com quais valores se adotará tal tecnologia.

Due diligence de Inteligência Artificial:

uma nova vertente da integridade empresarial

Reinaldo Oliveira Ferreira Junior

Reinaldo Oliveira Ferreira Junior é advogado, mestre em Direito Empresarial Internacional (LL.M.) pela Universidade de Liverpool (Reino Unido), onde foi agraciado com o Prêmio de Aluno do Ano. Possui MBA Executivo em Gestão e Direito Empresarial pela FGV e pós-graduações em Direito Constitucional e em Direito Digital, Proteção de Dados e Cibersegurança. Atua como consultor jurídico da Federação das Indústrias do Estado do Rio de Janeiro (Firjan) e como conselheiro do Conselho de Contribuintes do Estado do Rio de Janeiro.

Introdução

A evolução dos programas de integridade corporativa representa, em grande medida, um reflexo das transformações dos próprios riscos inerentes à atividade empresarial. Originalmente focados na prevenção de fraudes e corrupção[1], os mecanismos de compliance foram expandidos, em um primeiro momento, para abarcar a proteção de dados[2] e, mais recentemente, passam por uma nova reconfiguração, dessa vez provocada pela crescente adoção de sistemas baseados em Inteligência Artificial (IA) no ambiente de negócios.

Nesse novo contexto, a tecnologia deixa de ser um acessório de automação e passa a operar como infraestrutura decisória (recomendando, priorizando e pontuando riscos), cada vez mais influenciando temas sensíveis (como alocação de recursos, seleção de pessoas e resposta a incidentes). A consequência é que riscos clássicos[3] não deixam de existir, mas se tornam mais difíceis de refutar, uma vez que a "causa" de um dano pode agora estar relacionada a elementos tecnológicos invisíveis ao usuário[4]. A integridade migra, assim, para um campo mais complexo, no qual evidências técnicas auditáveis referentes ao funcionamento de sistemas de IA deixam de ser um simples diferencial e passam a ser requisito essencial[5].

Dados recentes evidenciam que o uso de IA na indústria brasileira cresce em ritmo acelerado[6], e pesquisas setoriais indicam que a maioria das empresas já considera a IA como uma prioridade estratégica inadiável, visando a redução de custos e otimização de processos[7]. Contudo, essa rápida assimilação tecnológica traz consigo vulnerabilidades ocultas que, se não geridas, podem resultar em passivos jurídicos, danos reputacionais e sanções regulatórias.

Não por outra razão, o Allianz Risk Barometer de 2026 posicionou a IA como o principal risco empresarial no Brasil, superando até mesmo as preocupações tradicionais com incidentes cibernéticos[8]. Essa percepção decorre da complexidade inerente aos algoritmos, que operam frequentemente como "caixas-pretas"[9], dificultando a explicabilidade de suas decisões, a identificação de vieses

[1] Cf. Duarte e Alencar (2024).

[2] Com destaque para o advento da Lei nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD), que impôs às organizações a criação de estruturas de compliance voltadas à proteção de dados pessoais.

[3] Como fraude, conflito de interesses, corrupção, discriminação e violação de deveres.

[4] Para um estudo aprofundado sobre como a extração e o processamento de dados em larga escala criam estruturas de influência comportamental que precedem e condicionam a tomada de decisões, tornando essencial a governança algorítmica como contrapeso institucional, ver Zuboff (2019).

[5] Essa mudança é particularmente sensível porque o risco não se restringe ao eventual ilícito, mas alcança a própria incapacidade de explicar decisões, justificar critérios e demonstrar diligência quando a tecnologia participa do processo decisório. A IA, ao automatizar processos, pode reduzir a transparência, funcionando sem que o usuário consiga demonstrar "por que" funcionou, "com que dados" e "com que salvaguardas". Assim, o compliance passa a operar como um sistema de verificação contínua, capaz de produzir evidências defensáveis perante conselhos, auditorias e, quando necessário, autoridades.

[6] Aumento 5% em apenas 2 anos (2022-2024), tendo 57,5% das indústrias informado fazer uso expressivo de sistemas de IA já em 2024. No cenário internacional, pesquisas setoriais corroboram essa tendência. O McKinsey Global Survey on AI apurou que, em 2024, 72% das empresas adotavam IA em ao menos uma função de negócios, ante 50% em 2022. E, em 2025, esse percentual chegou a 88%. Cf. IBGE (2024) e Singla, Sukharevsky, Yee, Chui e Hall (2024).

[7] Cf. Intel Corporation (2024).

[8] ALLIANZ COMMERCIAL. Allianz Risk Barometer 2026: identifying the major business risks for 2026. Munique: Allianz SE, jan. 2026. Disponível em: https://commercial.allianz.com/news-and-insights/reports/allianz-risk-barometer.html. Acesso em: 21 mar. 2026.

[9] A expressão "caixa-preta" (black box) diz respeito a sistemas cujo funcionamento interno é opaco, tornando impossível a compreensão dos mecanismos que levam às suas respostas/saídas. Cf. Lu (2020).

discriminatórios e a verificação de que os dados utilizados em seu treinamento respeitam direitos autorais e a privacidade de seus titulares.

O país vive, então, simultaneamente, pressão por um avanço prático e a tensão de uma incerteza normativa. Na prática, empresas são (e serão cada vez mais) cobradas a demonstrar governança de IA, rastreabilidade de dados e controles de risco[10]. No plano normativo, a regulação interna permanece em debate. O PL nº 2.338/2023, que institui o Marco Regulatório da Inteligência Artificial, está em tramitação na Câmara dos Deputados após aprovação no Senado Federal[11], e seu texto ainda abriga pontos controvertidos, cujo desfecho poderá impactar significativamente não apenas direitos individuais e coletivos, mas também a capacidade da Administração Pública e do setor produtivo de fazerem uso de IAs como vetor de competitividade.

Em paralelo, a ausência de uma legislação específica sobre o tema não exime as empresas da responsabilidade civil e administrativa decorrente do uso de IA, mas cria um vácuo normativo que deixa dúvida sobre como estruturar programas de compliance com diretrizes claras e uniformes. A LGPD, como se verá adiante, já impõe obrigações aplicáveis a sistemas que tomam decisões automatizadas com base em dados pessoais, representando, consequentemente, um piso normativo já exigível no Brasil, independentemente da possível sanção do PL nº 2.338/2023.

Nesse contexto de incerteza regulatória, a comunidade internacional tem fornecido parâmetros importantes. Em fevereiro de 2026, a Organização para a Cooperação e Desenvolvimento Econômico (OCDE) publicou o "Due Diligence Guidance for Responsible AI", documento que consolida diretrizes práticas para a conduta empresarial responsável no uso de sistemas de IA[12]. Para as empresas brasileiras, a adoção antecipada de parâmetros internacionais não é apenas medida de mitigação de riscos, é uma importante estratégia para assegurar inserção competitiva no mercado global e para conquistar a segurança jurídica em operações que envolvam desenvolvimento ou contratação de fornecedores de tecnologia.

1. A bússola internacional na governança algorítmica

O desafio imposto às empresas reside em conciliar a necessidade premente de inovação tecnológica e a busca por conformidade ética e legal. Nesse contexto, a análise comparada das abordagens adotadas por precursores tecnológicos do Ocidente[13] funciona como uma "bússola", orientando as corporações na adoção de boas práticas que, com elevada probabilidade, serão adaptáveis ao desfecho do processo legislativo brasileiro.

[10] A concepção de que rastreabilidade, explicabilidade e controle são pilares de uma IA confiável caminha para um consenso internacional. Cf. Floridi e outros (2018), Jobin e outros (2019), Mora-Cantallops e outros (2021).

[11] BRASIL. Câmara dos Deputados. *Projeto de Lei nº 2.338, de 2023*: dispõe sobre o desenvolvimento, o fomento e o uso ético e responsável da inteligência artificial com base na centralidade da pessoa humana. Brasília, DF: Câmara dos Deputados, 2023. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2487262. Acesso em: 21 mar. 2026.

[12] ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD). *OECD Due Diligence Guidance for Responsible AI*. Paris: OECD Publishing, 2026. Disponível em: https://www.oecd.org/en/publications/oecd-due-diligence-guidance-for-responsible-ai_41671712-en.html. Acesso em: 21 mar. 2026.

[13] Notadamente União Europeia, Reino Unido e Estados Unidos, que, em conjunto, respondem pela quase totalidade do desenvolvimento e exportação de tecnologias no Ocidente.

1.1 União Europeia

A União Europeia optou por um modelo regulatório prescritivo, materializado no Artificial Intelligence Act (AI Act), que entrou em vigor em agosto de 2024[14]. Baseada em uma classificação de risco (inaceitável, alto, limitado e mínimo), a norma impõe obrigações severas para sistemas considerados de "alto risco". O artigo 9°, por exemplo, exige a implementação de um sistema contínuo de gestão de riscos, enquanto o artigo 17 determina a manutenção de um sistema de gestão de qualidade que abrange desde a estratégia de conformidade regulatória até as técnicas de concepção do algoritmo.

O descumprimento dessas obrigações inerentes aos sistemas de alto risco pode acarretar sanções de até 15 milhões de euros ou 3% do faturamento global anual[15], ao passo que as sanções mais severas, de até 35 milhões de euros ou 7% do faturamento global, ficam restritas aos casos envolvendo práticas expressamente proibidas pelo artigo 5°[16].

Todavia, é importante registrar que, embora o modelo europeu garanta elevado patamar de proteção aos direitos fundamentais, ele tem sido alvo de críticas do setor produtivo global (que aponta o alto custo de conformidade e o potencial efeito inibidor sobre a inovação[17]) e de intenso debate acadêmico quanto à sua eficácia[18].

1.2 Reino Unido

Em oposição ao rigor do bloco europeu, o Reino Unido adotou uma abordagem pró-inovação[19]. Recusando a criação de uma legislação abrangente e de uma autoridade reguladora específica, o White Paper "A pro-innovation approach to AI regulation"[20] propõe a orientação de agências já existentes[21] na aplicação e adaptação de cinco princípios transversais de IA em seus respectivos domínios de atuação: segurança, transparência, equidade, responsabilização e contestabilidade[22].

A consequência prática é deslocar a *due diligence* do *checklist* normativo para o *assurance case*, ou seja, a própria empresa não apenas declara conformidade, mas demonstra, de forma contextualizada, que o sistema é seguro, justo e explicável.

Um pilar fundamental dessa estratégia é a criação do AI Safety Institute (AISI) em novembro de 2023[23]. Estabelecido como um órgão de excelência técnica, o AISI fica dedicado à avaliação científica de modelos e à mitiga-

[14] Embora tenha entrado em vigor em agosto de 2024, sua aplicação ocorre de forma gradual para permitir a adequação progressiva do mercado. As primeiras obrigações, referentes às práticas proibidas de risco inaceitável e à alfabetização em IA, tornaram-se exigíveis em 2 de fevereiro de 2025, enquanto as regras para modelos de propósito geral e IA generativa passaram a valer em 2 de agosto de 2025. A aplicação integral da norma está prevista para 2 de agosto de 2026, com exceção dos sistemas de alto risco incorporados em produtos já regulamentados, para os quais o prazo final foi estendido até 2 de agosto de 2027. Cf. União Europeia (2024).

[15] AI Act, art. 99, "4".

[16] EAI Act, art. 99, "3".

[17] Importante registrar que a questão não é apenas de custo interno. O AI Act opera com abrangência extraterritorial indireta por meio das cadeias de fornecimento que internalizam seus requisitos. Ou seja, qualquer fabricante que exporte produtos com IA integrada ou que forneça componentes tecnológicos a empresas europeias estará, na prática, submetido às exigências do regulamento.

[18] EBERS, Martin. Truly risk-based regulation of artificial intelligence: how to implement the EU's AI Act. *European Journal of Risk Regulation*, Cambridge, v. 16, n. 2, p. 684-703, 2025. DOI: https://doi.org/10.1017/err.2024.78.

[19] Para um estudo aprofundado sobre o contraste entre as abordagens da União Europeia e Reino Unido, ver Gikay (2024).

[20] Os cinco princípios transversais são: (i) *safety, security and robustness*; (ii) *appropriate transparency and explainability*; (iii) *fairness*; (iv) *accountability and governance*; e (v) *contestability and redress* (Reino Unido, 2023).

[21] Entre as principais autoridades setoriais orientadas pelo White Paper destacam-se: a Information Commissioner's Office (ICO), para a proteção de dados; a Financial Conduct Authority (FCA), para o setor financeiro; e a Competition and Markets Authority (CMA), para a defesa da concorrência.

[22] Cabe registrar que, desde a publicação do White Paper, a política britânica de IA continuou a sofrer modificações, com novos compromissos firmados na Bletchley Park Declaration (em 2023) e nos processos subsequentes de 2024 e 2025.

[23] Cujo nome foi alterado, em 2025, para AI Security Institute.

ção de riscos sistêmicos. Sua atuação concentra-se na pesquisa e no teste de sistemas avançados, sem impor, contudo, a burocracia legislativa característica do modelo europeu[24]. Para as empresas que interagem com o mercado britânico, a *due diligence* de sistemas de IA é, portanto, guiada por guias técnicos dinâmicos e melhores práticas setoriais, com foco na efetividade operacional da segurança em detrimento da mera conformidade formal (o chamado *tick-box compliance*)[25].

1.3 Estados Unidos

Os Estados Unidos, por sua vez, apresentam um cenário regulatório fragmentado, marcado pela colisão entre a desregulação em nível federal e o ativismo legislativo dos estados[26]. A administração federal, em janeiro de 2025, fixou a priorização da competitividade tecnológica sobre a cautela regulatória ao publicar a Ordem Executiva 14.179 que, revogando a ordem executiva aprovada pela administração anterior, reorientou as agências federais a eliminar barreiras ao desenvolvimento de IA[27]. Em sequência, com a publicação do AI Action Plan[28], em julho de 2025, o governo reafirmou sua posição ao explicitamente confrontar abordagens estaduais consideradas restritivas ao desenvolvimento da tecnologia.

Na ausência de uma lei federal unificada de caráter impositivo, o mercado norte-americano tem se apoiado em *frameworks* voluntários, com destaque para o AI Risk Management Framework (AI RMF 1.0) do National Institute of Standards and Technology (NIST)[29]. Esse documento estabelece quatro funções centrais para a governança de IA: *govern*, *map*, *measure* e *manage* (governar, mapear, medir e gerenciar)[30]. Embora voluntário, o AI RMF tem sido progressivamente invocado

[24] Cf. UK AI Safety Institute (2023, 2025).

[25] A expressão *tick-box compliance* designa uma abordagem superficial de conformidade, orientada pelo mero preenchimento formal de listas de verificação, sem a correspondente efetividade operacional dos controles. Cf. Quelle (2018).

[26] A fragmentação regulatória norte-americana decorre da ausência de lei federal sobre IA, o que abriu espaço para um forte ativismo legislativo nos estados. Califórnia, Colorado, Connecticut e Illinois, por exemplo, aprovaram legislações setoriais que, em certas medidas, se aproximam de modelos mais rígidos, como o do bloco europeu. O Colorado representa, até o momento, a experiência mais próxima de uma lei horizontal e abrangente sobre o tema, ao impor deveres voltados à prevenção de discriminação algorítmica. A Califórnia, por sua vez, concedeu ênfase à transparência, IA generativa e dados de treinamento. Illinois concentrou sua regulação no uso de IA em relações de emprego. E Connecticut, por fim, apresenta uma abordagem centrada no uso de IA pelo setor público.

[27] ESTADOS UNIDOS. Presidente (2025-2029: Donald J. Trump). *Executive Order 14179*: removing barriers to American leadership in artificial intelligence. Washington, DC: Federal Register, v. 90, n. 20, p. 8741-8742, 31 jan. 2025. Disponível em: https://www.federalregister.gov/documents/2025/01/31/2025-02172/removing-barriers-to-american-leadership-in-artificial-intelligence. Acesso em: 26 out. 2026.

[28] ESTADOS UNIDOS. The White House. *Winning the AI Race: America's AI Action Plan*. Washington, DC, 23 jul. 2025. Disponível em: https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf. Acesso em: 25 mar. 2026.

[29] O AI RMF foi desenvolvido por meio de um processo colaborativo com a indústria, meio acadêmico e governo, com vistas a fornecer uma estrutura voluntária, mas robusta, para a gestão de riscos associados a sistemas de IA ao longo de seu ciclo de vida. Cf. NIST (2023).

[30] As quatro funções do NIST AI RMF - govern (governar), map (mapear), measure (medir) e manage (gerenciar) - correspondem a um ciclo iterativo de gestão de riscos: a função Govern estabelece as estruturas organizacionais de responsabilidade; Map identifica e classifica os riscos do sistema; Measure avalia sua probabilidade e impacto; e Manage implementa respostas e acompanha resultados (NIST, 2023, p. 20).

por agências reguladoras como parâmetro de conduta razoável, tendência que, se consolidada, pode influenciar o *standard of care* exigido em litígios envolvendo danos causados por sistemas de IA[31].

A dimensão que mais pressiona operações comerciais com IA generativa, porém, é a incerteza quanto à propriedade intelectual e à origem dos dados de treinamento. Decisões e acordos nos EUA vêm apontando uma possível maior tolerância ao uso de obras para treinamento quando os materiais são licitamente adquiridos/acessados, mas revelam risco jurídico elevado quando os dados são obtidos de *shadow libraries*[32]. Casos como Bartz v. Anthropic[33] indicam essa distinção ao admitir a plausibilidade do *fair use* para treinamento, mas negar proteção à formação de bibliotecas permanentes com cópias piratas, ao passo que os casos Kadrey v. Meta e Thomson Reuters v. Ross Intelligence[34] demonstram que o tema permanece instável e dependente dos fatos concretos.

[31] A Federal Trade Commission (FTC), em seu *advance notice of proposed rulemaking* (ANPR) de 2022 sobre vigilância comercial e em relatórios e orientações subsequentes sobre IA passou a tratar erro algorítmico, viés, discriminação, falta de transparência e insuficiência de monitoramento como fatores importantes para a avaliação de práticas desleais. Embora o relatório de 2022 não tenha referenciado formalmente o NIST AI RMF 1.0 - visto que este foi publicado apenas em 2023 -, as preocupações nele apontadas alinham-se ao *framework* do NIST. Relatórios posteriores da FTC, como o de 2024 sobre mídia social e serviços de *streaming* de vídeo, passaram a citar expressamente o NIST AI RMF 1.0 ao tratar de vieses e discriminação em IA. A Equal Employment Opportunity Commission (EEOC), por sua vez, adotou o AI RMF como referencial em sua orientação de maio de 2023 sobre o uso de software de seleção de candidatos, explicitando que empregadores devem conhecer e controlar os riscos de discriminação de ferramentas algorítmicas que adotem. A tendência confirma, assim, que o *framework*, ainda que voluntário na prática, ganha força normativa indireta quando há litígio regulatório. Cf. United States (2022, 2023, 2024) e Davtyan (2025).

[32] A expressão refere-se a repositórios digitais, em regra mantidos fora dos canais formais de licenciamento, e que oferecem acesso gratuito a livros, artigos acadêmicos e outros conteúdos. Apesar de serem por vezes tratadas como infraestruturas informais de acesso ao conhecimento (em suposta resposta a barreiras econômicas), tornam-se um agente juridicamente problemático por permitirem a distribuição não autorizada de obras protegidas. Cf. BODÓ, Balázs. The genesis of Library Genesis: the birth of a global scholarly shadow library. In: KARAGANIS, Joe (ed.). Shadow libraries: access to knowledge in global higher education. Cambridge: MIT Press, 2018. p. 25.

[33] Em *Bartz v. Anthropic*, os autores alegaram que a Anthropic teria copiado livros protegidos por direitos autorais para treinar modelos e formar uma biblioteca interna. A decisão, de 23 de junho de 2025, é relevante porque distinguiu o uso de obras para treinamento (considerado, em condições pontuais, compatível com fair use) da manutenção de uma biblioteca baseada em cópias pirateadas. Assim, o caso demonstra que a licitude da origem dos dados pode ser decisiva para a avaliação de risco jurídico em IA generativa. Cf. United States District Court for the Northern District of California (2025a).

[34] Em *Kadrey v. Meta*, a Corte do Distrito Norte da Califórnia reconheceu o fair use no contexto de treinamento de modelos de IA com livros protegidos, mas a controvérsia permaneceu marcada por discussões sobre aquisição de tais dados, impacto de mercado e suficiência probatória. Já em *Thomson Reuters v. Ross Intelligence*, a Corte do Distrito de Delaware rejeitou o fair use em situação envolvendo uso de conteúdos editoriais para desenvolver ferramenta concorrente de pesquisa jurídica, atribuindo peso ao caráter competitivo e ao potencial impacto sobre o mercado da titular dos direitos. Esses processos demonstram que as Cortes norte-americanas não oferecem autorização genérica para treinamento com obras protegidas, sendo a análise casuística, especialmente quanto à finalidade do uso e origem dos dados (United States District Court for the Northern District of California, 2025b; United States District Court for the District of Delaware, 2025).

2. O framework em seis etapas da OCDE

Diante do quadro traçado até aqui, as empresas brasileiras se deparam com um dilema prático. Como importar tecnologia de ponta e/ou desenvolver soluções próprias garantindo o compliance sem comprometer a competitividade? A resposta não reside em aguardar a sanção do PL nº 2.338/2023, mas em se antecipar aos riscos por meio de uma autorregulação inspirada nas melhores práticas internacionais.

E, apesar da leitura comparada dos três sistemas tratados nos tópicos anteriores revelar convergências[35], nenhum deles, isoladamente, parece ser adequado para operar como guia efetivo ao sistema brasileiro. Isso porque cada um dos precitados modelos foi desenhado para atender a especificidades estruturais de mercados diferentes entre si e que se diferenciam do brasileiro tanto em aspectos formais[36] quanto materiais[37].

O *framework* publicado pela OCDE em fevereiro de 2026 ocupa, nesse contexto, uma posição de destaque. Não porque seja o mais/menos rigoroso ou porque imponha mais/menos sanções. Sua vantagem comparativa reside em três características que o tornam compatível com o momento atual do ordenamento brasileiro: (i) é tecnologicamente neutro (no sentido de ser aplicável a qualquer sistema de IA, independentemente do setor ou da escala de operação); (ii) é compatível com os três modelos já analisados (podendo ser aplicado sem conflito com o AI Act, com os princípios britânicos e com o NIST AI RMF, funcionando como denominador comum); e (iii) é orientado para a conduta empresarial responsável, e não para a formulação de políticas públicas. Além disso, o *framework* ancora-se nos OECD AI Principles, que o Brasil endossou em 2019[38], o que transforma sua adoção não em uma importação acrítica de norma estrangeira, mas sim na materialização de um compromisso que o país assumiu no plano internacional.

Assim, para as empresas brasileiras, a adoção do *framework* da OCDE opera em dois planos simultâneos. No plano interno, oferece uma estrutura de governan-

[35] A exemplo da: (i) obrigação de conhecer os riscos dos sistemas de IA utilizados — seja por exigência legal (UE), seja por orientação setorial (UK), seja por expectativa regulatória (EUA); (ii) necessidade de documentar e demonstrar a diligência adotada — seja por meio de sistemas de gestão de qualidade (UE, art. 17 do AI Act), seja por assurance cases (UK), seja por risk profiles (NIST AI RMF); e (iii) responsabilização progressiva pelo uso de sistemas que causem danos, independentemente de culpa direta do operador.

[36] A exemplo do modelo britânico, que distribui responsabilidades por agências setoriais em um sistema de common law que não encontra equivalente no ordenamento jurídico brasileiro.

[37] A operacionalização do NIST AI RMF no mercado norte-americano é fortemente favorecida por características próprias dos EUA, em especial a tradição de governança por *standards* voluntários, participação privada na formulação de parâmetros técnicos e maturidade prévia em práticas de *enterprise risk management* e autorregulação corporativa. Cf. Davtyan (2025).

[38] Os OECD AI Principles, adotados em 2019 e revisados em 2024, constituem um conjunto de princípios sobre IA endossado por mais de quarenta países, incluindo o Brasil. O Due Diligence Guidance for Responsible AI de 2026 operacionaliza esses princípios para o contexto empresarial, traduzindo compromissos em procedimentos e verificações concretas. Cf. ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD). *Recommendation of the Council on Artificial Intelligence*. OECD/LEGAL/0449. Paris: OECD, 2019, atualizado em 2024. Disponível em: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449. Acesso em: 21 mar. 2026.

ça compatível com o que a LGPD[39] exige implicitamente (especialmente nos artigos 20[40] e 38[41]) e que a futura regulação, decorrente do avanço do PL nº 2.338/2023, provavelmente deverá exigir (antecipando, em ambos os casos, o ônus da adequação). No plano externo, funciona como credencial de governança perante parceiros comerciais e investidores que já avaliam seus fornecedores à luz de parâmetros como os do AI Act e do NIST RMF.

Adotar tais diretrizes desde logo, portanto, não deve ser encarado como uma conformidade antecipada com norma futura, mas sim como planejamento estratégico antecipando-se a um movimento que será necessário em todos os cenários. As seis etapas são:

(i) Incorporar a conduta empresarial responsável: a primeira etapa consiste na atualização de códigos de conduta e políticas de compliance para incluir diretrizes claras sobre o uso aceitável de IA[42]. Afinal, sem uma política interna que defina o que é uso autorizado, com quais ferramentas, para quais finalidades e com quais salvaguardas, qualquer controle subsequente será frágil. Essa medida também é relevante para combater o chamado *shadow AI*[43].

(ii) Identificar e avaliar impactos adversos[44]: a segunda etapa exige a realização de avaliações de impacto prévias à implementação de sistemas de IA, especialmente em áreas sensíveis, com foco na detecção de vieses discriminatórios e vulnerabilidades de segurança da informação. Essa etapa corresponde, em analogia ao previsto na LGPD, à elaboração do Relatório de Impacto à Proteção de Dados Pessoais (RIPD). A diferença está na necessidade de examinar também riscos que não derivam de dados pessoais, como reprodução de conteúdo protegido por direitos autorais, desvios de desempenho ao longo do tempo (*model drift*) e comportamentos não previstos no desenho original do sistema.

[39] Embora a LGPD não trate de sistemas baseados em IA de forma explícita, impõe obrigações diretamente aplicáveis a ferramentais digitais que realizam tratamento automatizado de dados pessoais (o que abrange, senão todos, a maioria dos sistemas de IA utilizados em operações empresariais). O episódio envolvendo a Meta Platforms em julho de 2024 (quando a ANPD determinou a suspensão cautelar do tratamento de dados pessoais para treinamento de IA por ausência de base legal adequada e riscos a grupos vulneráveis) demonstrou exatamente a atuação preventiva e célere da autoridade pautada na LGPD, ou seja, uma atuação que ocorre mesmo diante da inexistência de lei específica para tratar dos sistemas baseados em IA. Para as empresas, isso significa que uma série de adaptações se materializa como condicionante para a imersão e uso (responsável) das novas ferramentas tecnológicas — ou seja, obrigações imediatas, não condicionadas à futura norma. Cf. ANPD (2024).

[40] O art. 20 assegura ao titular o direito de solicitar a revisão de decisões tomadas com base unicamente em tratamento automatizado de dados pessoais que afetem seus interesses, incluindo decisões voltadas à definição de perfis profissionais, de consumo, de crédito ou de personalidade. Essa previsão impõe obrigação análoga à explicabilidade e rastreabilidade de modelos decisórios, um pré-requisito técnico da due diligence algorítmica previsto em lei já em vigor. Cf. Hosni (2020).

[41] O art. 38 autoriza a ANPD a exigir do controlador relatório de impacto à proteção de dados pessoais para os tratamentos que, por sua natureza, alcance ou finalidade, possam representar riscos às liberdades civis. Em sistemas de IA, esse relatório equivale, em certa medida, à avaliação de impacto pré-implementação exigida tanto pelo NIST AI RMF quanto pelo AI Act.

[42] Dependendo da estrutura organizacional e do volume de adoção de sistemas de IA, pode ser mais adequado criar uma política interna autônoma de uso responsável de IA, integrada ao programa de compliance geral, em vez de apenas incluir diretrizes nos códigos de conduta existentes.

[43] O termo "*shadow AI*" refere-se ao uso de ferramentas de inteligência artificial por colaboradores sem autorização, conhecimento ou supervisão das áreas competentes, expondo a organização a riscos de vazamento de dados, violação de sigilo industrial e responsabilidade rregulatório (Up Guard, 2025).

[44] Para se ter acesso a um referencial conceitual e estruturante que permita organizar, identificar e categorizar diferentes tipos de danos/risco em questão, ver Mittelstadt e outros (2016).

(iii) Cessar, prevenir e mitigar impactos adversos: identificados os riscos, a terceira etapa exige a adoção de controles técnicos[45] e organizacionais[46] para reduzir a probabilidade de sua ocorrência. Nesse ponto, o *framework* da OCDE dialoga diretamente com os requisitos do artigo 9º do AI Act (que exige um sistema contínuo de gestão de riscos para sistemas de alto risco) e com a lógica do *assurance case* britânico (que demanda que a empresa demonstre, e não apenas declare, que o sistema é seguro). Para as empresas brasileiras, a implementação desses controles cria o registro documental sem o qual qualquer argumento de diligência perante a ANPD, o Judiciário ou um parceiro comercial internacional será necessariamente frágil.

(iv) Monitorar a implementação e os resultados: considerando que os modelos de IA evoluem e podem sofrer desvios de desempenho ao longo do tempo (*model drift*), a *due diligence* deve ser contínua, com auditorias periódicas para garantir que o algoritmo continue operando dentro dos parâmetros éticos e legais predefinidos. O monitoramento contínuo é a condição para que as demais etapas do *framework* não se tornem, com o tempo, obsoletas.

(v) Comunicar ações para endereçar impactos: a empresa deve ser capaz de explicar como suas decisões apoiadas em IAs são tomadas e quais medidas de segurança estão em vigor, para, caso necessário, prestar contas a acionistas, clientes/consumidores e, eventualmente, à ANPD. Essa etapa conecta-se ao que dispõe o artigo 20 da LGPD e ao que os três modelos regulatórios precitados exigem sob nomenclaturas distintas — transparência e explicabilidade (AI Act, artigo 13), *appropriate transparency and explainability* (*white paper* britânico) e *trustworthy and explainable AI* (NIST AI RMF). O *framework* da OCDE, como se vê, sintetiza essas exigências em um dever de comunicação verificável e, portanto, auditável.

(vi) Prover ou cooperar em remediação quando apropriado: a sexta etapa fecha o ciclo. Caso um sistema de IA cause algum dano, o programa de integridade deve prever mecanismos de resposta a incidentes e reparação aos afetados, o que também poderá servir como atenuante em eventuais sanções administrativas. A remediação eficaz opera como mecanismo que retroalimenta o próprio ciclo de governança, ou seja, incidentes bem documentados e bem tratados geram aprendizado que torna possível o aperfeiçoamento de cada etapa do *framework*.

Além das etapas, a implementação das diretrizes da OCDE recomenda a consolidação de evidências em um dossiê de diligência do sistema (*AI Diligence File*), contendo, conforme o risco e o contexto de uso, elementos como finalidade do sistema, classificação por risco, mapa de dados, testes de robustez/viés, decisão de compra/uso, cláusulas contratuais e plano de remediação. Embora a OCDE não imponha esse dossiê como *checklist* obrigatório, tal instrumento traduz operacionalmente suas recomendações de governança, rastreabilidade e monitoramento. Além disso, o dossiê tende a reduzir o custo marginal de auditorias subsequentes, na medida em que concentra e organiza informações que, de outro modo, precisariam ser reconstruídas a cada nova demanda.

[45] Entre os controles técnicos recomendados pela OCDE estão: filtros de segurança e conteúdo, testes de robustez adversarial, monitoramento de mudanças de desempenho e de *data/model drift*, bem como mecanismos de documentação e rastreabilidade capazes de registrar dados, processos, decisões técnicas, métricas, limiares e estratégias de monitoramento.

[46] Entre os controles organizacionais destacam-se: supervisão humana significativa nas decisões de maior impacto, a designação de um responsável pela governança de IA, a realização de treinamentos periódicos sobre uso responsável de IA e a criação de canais de denúncia para relato de usos inadequados de sistemas algorítmicos.

Conclusão

O uso de sistemas de IA em empresas brasileiras cresce em ritmo acelerado, enquanto a regulação interna ainda está em formação. A incorporação da *due diligence* algorítmica aos programas de compliance não deve ser vista como uma simples adaptação incremental ao que já existe, mas sim como uma reconfiguração do próprio critério de integridade empresarial.

A análise comparada das abordagens da União Europeia, do Reino Unido e dos Estados Unidos confirma que, independentemente do modelo regulatório adotado, a responsabilização pelo uso de sistemas de IA é progressiva, crescente e cada vez menos condicionada à existência de culpa direta do operador. O AI Act europeu impõe tal responsabilização via norma expressa, ao passo que o modelo britânico a operacionaliza por meio de *assurance cases* monitorados por agências setoriais, enquanto o *framework* voluntário do NIST adquire, progressivamente, força normativa indireta via orientações da FTC e da EEOC. Em nenhum caso a ausência de regulação específica é interpretada como ausência de obrigação. E, no Brasil, a atuação da ANPD já vem demonstrando raciocínio análogo baseado na LGPD mesmo antes da conclusão do debate legislativo sobre o tema.

Nesse cenário, o *framework* da OCDE revela sua utilidade para o caso brasileiro. Não porque seja, em qualquer métrica, superior aos modelos examinados, mas porque é o único desenhado para orientar a conduta empresarial em contextos de múltiplos sistemas jurídicos simultâneos (desafio que as empresas que integram cadeias globais de fornecimento enfrentam). Adotá-lo é, portanto, ao mesmo tempo conformidade com compromisso assumido pelo Brasil ao aderir ao OECD AI Principles, preparação para as inovações do PL nº 2.338/2023 e credencial de governança perante parceiros e investidores externos. Empresas capazes de demonstrar rastreabilidade, explicabilidade e controle sobre seus sistemas de IA não apenas mitigam passivos: constroem confiança, acessam mercados regulados e reduzem os custos de transação que, no Brasil, historicamente encarecem a atividade produtiva. A governança algorítmica passa a ser, nessa perspectiva, um ativo competitivo e um redutor estrutural de custos, não um encargo adicional sobre uma atividade já onerosa.

A *due diligence* de inteligência artificial deve ser compreendida, portanto, como um novo padrão de diligência empresarial, cujo alcance transcende o cumprimento normativo para se afirmar como pilar da sustentabilidade jurídica, econômica e ética das organizações.

Referências

AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD). *ANPD determina suspensão cautelar do tratamento de dados pessoais para treinamento da IA da Meta*. Brasília: ANPD, 2024. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-determina-suspensao-cautelar-do-tratamento-de-dados-pessoais-para-treinamento-da-ia-da-meta. Acesso em: 25 mar. 2026.

ALLIANZ. *Allianz Risk Barometer 2026*. Munique: Allianz SE, 2026. Disponível em: https://commercial.allianz.com/news-and-insights/reports/allianz-risk-barometer.html. Acesso em: 21 mar. 2026.

BODÓ, Balázs. The genesis of Library Genesis: the birth of a global scholarly shadow library. In: KARAGANIS, Joe (ed.). *Shadow libraries:* access to knowledge in global higher education. Cambridge: MIT Press, 2018. p. 25-51.

BRADFORD, Anu. *The Brussels effect:* how the European Union rules the world. Oxford: Oxford University Press, 2020.

BRASIL. Câmara dos Deputados. *Projeto de Lei nº 2.338, de 2023*. Dispõe sobre o uso da Inteligência Artificial. Brasília, DF: Presidência da República, 2023. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2487262. Acesso em: 21 mar. 2026.

BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 22 out. 2026.

CALO, Ryan. Artificial intelligence policy: a primer and roadmap. *UC Davis Law Review*, v. 51, n. 2, p. 399-435, 2017. DOI: https://doi.org/10.2139/ssrn.3015350.

DAVTYAN, Tatevik. The U.S. approach to AI regulation: federal, state, and industry-led initiatives. *Journal of Law, Technology, & the Internet*, v. 16, n. 2, 2025.

DUARTE, Cláudia Türner Pereira; ALENCAR, Matheus de. Trajetória de compliance no Brasil e sua importância para o Ministério Público brasileiro. *Revista do Ministério Público do Estado do Rio de Janeiro,* n. 91, p. 43-66, 2024. Disponível em: https://www.mprj.mp.br/servicos/revista-do-mp/revista-91/artigo-das-pags-43-66. Acesso em: 22 out. 2026.

EBERS, Martin. Truly risk-based regulation of artificial intelligence: how to implement the EU's AI Act. *European Journal of Risk Regulation*, [*S. l.*], v. 16, n. 2, p. 684-703, 2025. DOI: https://doi.org/10.1017/err.2024.78.

ESTADOS UNIDOS. Presidente (2025-2029: Donald J. Trump). *Executive Order 14179*: removing barriers to American leadership in artificial intelligence. Washington, DC: Federal Register, v. 90, n. 20, p. 8741-8742, 31 jan. 2025. Disponível em: https://www.federalregister.gov/documents/2025/01/31/2025-02172/removing-barriers-to-american-leadership-in-artificial-intelligence. Acesso em: 26 out. 2026.

ESTADOS UNIDOS. The White House. *Winning the AI Race*: America's AI Action Plan. Washington, DC, 23 jul. 2025. Disponível em: https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf. Acessado em 25/03/2026.

FLORIDI, Luciano; COWLS, Josh; BELTRAMETTI, Monica; CHATILA, Raja. An ethical framework for a good AI society: opportunities, risks, principles, and recommendations. *Minds and Machines*, [*S. l.*], v. 28, n. 4, p. 689-707, 2018. DOI: https://10.1007/s11023-018-9482-5.

GIKAY, Asress Adimi. Risks, innovation, and adaptability in the UK's incrementalism versus the European Union's comprehensive artificial intelligence regulation. *International Journal of Law and Information Technology,* [*S. l.*], v. 32, n. 1, eaae013, 2024. DOI: https://doi.org/10.1093/ijlit/eaae013.

HOSNI, David Salim Santos; MARTINS, Pedro Bastos Lobo. Tomada de decisão automatizada e a regulamentação da proteção de dados: alternativas coletivas oferecidas pela Lei Geral de Proteção de Dados. *Internet & Sociedade,* [*S. l.*], v. 1, n. 2, p. 77-101, 2020.

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA (IBGE). *Pesquisa de Inovação Semestral (PINTEC Semestral) 2024:* indicadores temáticos: tecnologias digitais avançadas, teletrabalho e cibersegurança. Rio de Janeiro: IBGE, 2024. Disponível em: https://biblioteca.ibge.gov.br/index.php/biblioteca-catalogo?view=detalhes&id=2102203. Acessado em 21/03/2026.

INTEL CORPORATION. *97% de empresas nas Américas colhem resultados concretos com IA*. Intel Newsroom, 2024. Disponível em: https://newsroom.intel.com/pt/inteligencia-artificial/976-empresas-nas-americas-colhem-resultados-concretos-com-ia. Acessado em 21/03/2026.

JOBIN, Anna; IENCA, Marcello; VAYENA, Effy. The global landscape of AI ethics guidelines. *Nature Machine Intelligence,* [*S. l.*], v. 1, n. 9, p. 389-399, 2019. DOI: https://doi.org/10.1038/s42256-019-0088-2.

LU, Sylvia. Algorithmic opacity, private accountability, and corporate social disclosure in the age of artificial intelligence. *Vanderbilt Journal of Entertainment and Technology Law*, [*S. l.*], v. 23, n. 1, p. 1-84, 2020. Disponível em: https://doi.org/10.1038/s42256-019-0088-2. Acesso em: 22 out. 2026.

MITTELSTADT, Brent Daniel *et al*. The ethics of algorithms: mapping the debate. *Big Data & Society,* [*S. l.*], v. 3, n. 2, P. 1-21, 2016. DOI: https://doi.org/10.1177/205395171667967.

MORA-CANTALLOPS, Marçal; SÁNCHEZ-ALONSO, Salvador; GARCÍA-BARRIOCANAL, Elena; SICILIA, Miguel-Angel. Traceability for trustworthy AI: a review of models and tools. *Big Data and Cognitive Computing*, [*S. l.*], v. 5, n. 2, p. 1-14, 2021. DOI: https://doi.org/10.3390/bdcc5020020.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). *Artificial Intelligence Risk Management Framework (AI RMF 1.0).* Gaithersburg: NIST, jan. 2023. (NIST AI 100-1). Disponível em: https://airc.nist.gov/airmf-resources/airmf/. Acesso em: 25 mar. 2026.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD). *OECD Due Diligence Guidance for Responsible AI*. Paris: OECD Publishing, 2026. Disponível em: https://www.oecd.org/en/publications/oecd-due-diligence-guidance-for-responsible-ai_41671712-en.html. Acesso em: 21 mar. 2026.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD). *Recommendation of the Council on Artificial Intelligence.* OECD/LEGAL/0449. Paris: OECD, 2019, atualizado em 2024. Disponível em: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449. Acesso em: 21 mar. 2026.

QUELLE, Claudia. Enhancing compliance under the General Data Protection Regulation: the risky upshot of the accountability- and risk-based approach. *European Journal of Risk Regulation,* [*S. l.*], v. 9, n. 3, p. 502-526, 2018. DOI: https://doi.org/10.1017/err.2018.47.

REINO UNIDO. Department for Science, Innovation and Technology (DSIT). *A pro-innovation approach to AI regulation:* White Paper. London: DSIT, 2023. Disponível em: https://www.gov.uk/government/publications/ai-regulation--a-pro-innovation-approach/white-paper. Acesso em: 23 mar. 2026.

SINGLA, Alex; SUKHAREVSKY, Alexander; YEE, Lareina; CHUI, Michael; HALL, Bryce. *The state of AI in early 2024*: gen AI adoption spikes and starts to generate value. [*S. l.*]: McKinsey & Company, 30 maio 2024. Disponível em: https://www.mckinsey.com/capabilities/quantumblack/our--insights/the-state-of-ai. Acesso em: 21 mar. 2026.

REINO UNIDO. Department for Science, Innovation and Technology (DSIT). *AI Safety Summit 2023:* The Bletchley Declaration. Policy paper. London: DSIT, 2023. Disponível em: https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration. Acesso em: 23 mar. 2026.

SINGLA, Alex; SUKHAREVSKY, Alexander; YEE, Lareina; CHUI, Michael; HALL, Bryce. *The state of AI in early 2024*: gen AI adoption spikes and starts to generate val ue. [*S. l.*]: McKinsey & Company, 30 maio 2024. Disponível em: https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai. Acesso em: 21 mar. 2026.

UK AI SAFETY INSTITUTE. *Frontier AI*: capabilities and risks – discussion paper. London: AISI, 2023.

UK AI SAFETY INSTITUTE. *Frontier AI Trends Report*. London: AISI, 2025. Disponível em: https://www.aisi.gov.uk/frontier-ai-trends-report. Acesso em: 23 mar. 2026.

UNIÃO EUROPEIA. *Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024 (AI Act)*. Jornal Oficial da União Europeia, L 2024/1689, 12 jul. 2024. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32024R1689. Acesso em: 21 mar. 2026.

UNITED STATES. Equal Employment Opportunity Commission (EEOC). *Select Issues:* assessing adverse impact in software, algorithms, and artificial intelligence used in employment selection procedures. Washington, DC: EEOC, 2023. Disponível em: https://data.aclum.org/storage/2025/01/EOCC_www_eeoc_gov_laws_guidance_select-issues-assessing-adverse-impact-software-algorithms-and-artificial.pdf. Acesso em: 26 mar. 2026.

UNITED STATES. Federal Trade Commission. *A Look Behind the Screens:* examining the data practices of social media and video streaming services. Washington, DC: FTC, 2024. Disponível em: https://www.ftc.gov/system/files/ftc_gov/pdf/Social-Media-6b-Report-9-11-2024.pdf Acesso em: 26 mar. 2026.

UNITED STATES. Federal Trade Commission. Trade Regulation Rule on Commercial Surveillance and Data Security. Washington, DC: FTC, 2022. Disponível em: https://www.federalregister.gov/documents/2022/08/22/2022-17752/trade-regulation-rule-on-commercial-surveillance-and--data-security. Acesso em: 26 mar. 2026.

UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF CALIFORNIA. Bartz et al. v. Anthropic PBC. No. 3:24-cv-05417-WHA. *Order on Motion for Summary Judgment*, 23 jun. 2025a.

UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF CALIFORNIA. Kadrey et al. v. Meta Platforms, Inc. No. 3:23-cv-03417-VC, 2025 WL 1752484. *Order on Motion for Summary Judgment*, 25 jun. 2025b.

UNITED STATES DISTRICT COURT FOR THE DISTRICT OF DELAWARE. Thomson Reuters Enterprise Centre GmbH et al. v. ROSS Intelligence Inc. No. 1:20-cv-00613-SB, 2025 WL 458520. *Memorandum Opinion*, 11 fev. 2025.

UPGUARD. *The state of shadow AI*. UpGuard, 2025. Disponível em: https://content.upguard.com/hubfs/resources/The-State-Of-Shadow-AI-Report-2025.pdf. Acesso em: 24 mar. 2026.

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

Capítulo 5

Inovação com Inteligência Artificial: riscos, responsabilidades e transparência no uso de algoritmos

Inteligência Artificial como ferramenta humana

Pedro Nachbar Sanches

Pedro Nachbar Sanches é advogado especialista em direito digital e proteção de dados pela UERJ/ITS. Fellow of Information Privacy pela International Association of Privacy Professionals (IAPP), além de certificado pela IAPP como Certified Information Privacy Manager (CIPM) e Certified Information Privacy Professional / Europe (CIPP/E). Sócio do escritório Prado Vidigal Advogados.

Introdução

Quando o computador pessoal começou a entrar nas casas e nos escritórios ao longo dos anos 1980 e, com força, na década de 1990, quase ninguém previu o tamanho das mudanças que ele traria. A princípio parecia apenas uma máquina para acelerar contas e guardar arquivos. Em poucos anos, porém, mudou a forma como as pessoas trabalham, estudam, se comunicam, compram, guardam suas memórias e se relacionam. Junto com as facilidades vieram perguntas que a sociedade nunca tinha precisado responder. O que acontece quando um documento importante existe apenas na tela e não no papel? Quem é o dono de um arquivo que pode ser copiado infinitas vezes sem perder qualidade? De quem é a culpa quando um sistema falha e alguém sai prejudicado? Cada uma dessas dúvidas pareceu, no seu tempo, um problema sem solução; nenhuma delas era. Aos poucos, aprendemos a conviver com o computador, ajustamos regras e hábitos e seguimos em frente. Hoje ele é tão comum que raramente paramos para pensar nele como aquilo que sempre foi: uma ferramenta a serviço de quem a utiliza.

A Inteligência Artificial (IA) nos coloca diante de um momento parecido, só que em escala maior e a uma velocidade muito superior. As inquietações mudaram de objeto, mas guardam a mesma natureza. Voltamos a perguntar quem é o responsável quando uma máquina erra, como confiar em decisões que nem sempre conseguimos explicar e o que muda quando parte daquilo que produzimos passa a contar com a ajuda de um sistema. A diferença é que a IA já deixou de ser promessa distante para se tornar parte da rotina. Está no aplicativo que recomenda a melhor roupa, no serviço financeiro que aprova ou nega um crédito, no assistente que escreve e traduz, na ferramenta que cria uma imagem a partir de uma frase. Essa presença, para muitos silenciosa, é justamente o que torna o tema tão importante. Convém, portanto, deixar de lado a dúvida sobre se a inteligência artificial vai mudar a vida em sociedade e concentrar a atenção em como ela já a muda e no que podemos fazer para conduzir esse processo com responsabilidade.

Vale explicar desde já a perspectiva que este texto de abertura propõe como fio condutor da leitura. A inteligência artificial é aqui olhada, antes de tudo, como uma ferramenta. Uma ferramenta impressionante, é verdade, e de efeitos que ainda estamos aprendendo a medir, mas que existe para servir a propósitos humanos. Essa escolha de perspectiva muda o foco da conversa. Em vez de concentrar a atenção no que a máquina supostamente decide sozinha, ela ilumina a responsabilidade das pessoas e das organizações que criam, ensinam, colocam em funcionamento e usam esses sistemas. Enquanto parte do debate enxerga uma espécie de mente independente, capaz de decidir, criar e escolher por conta própria, esta introdução enxerga uma tecnologia potente que amplia o que somos capazes de fazer e que, por isso mesmo, exige de nós ainda mais cuidado e atenção. Boa parte do desconforto entre inovação e proteção de direitos tem origem menos em um choque impossível de resolver e mais na dificuldade de compreender como a tecnologia realmente funciona. Quando se parte de uma imagem equivocada do que a inteligência artificial faz, corre-se o risco de combater um perigo que não existe e, no caminho, atrapalhar benefícios concretos.

Reconhecer a IA como ferramenta poderosa não significa fechar os olhos para os seus riscos. Essa mesma tecnologia que potencializa a criatividade humana também pode reproduzir e amplificar preconceitos presentes nos dados que a alimentam. Pode acelerar decisões importantes sem que ninguém consiga explicar com clareza como chegou a elas. Pode gerar resultados convincentes na forma, mas incorretos no conteúdo, apresentando com segurança informações que não correspondem à realidade. Levar a inteligência artificial a sério exige enxergar ao mesmo tempo aquilo que ela viabiliza e aquilo que ela ameaça.

Vale a pena, antes de seguir, olhar para o lado luminoso dessa ferramenta, porque é ele que dá sentido a todo o cuidado que as seções seguintes vão recomendar. Na medicina, um amplo estudo sueco com mais de 100 mil mulheres mostrou que a mamografia apoiada

por inteligência artificial aumentou em 29% a detecção de câncer de mama, sem elevar os falsos positivos[1]. Na pesquisa científica, ferramentas de inteligência artificial permitiram prever a estrutura de praticamente todas as proteínas conhecidas, um feito que abre caminho para o desenvolvimento de novos medicamentos e que foi reconhecido com o Prêmio Nobel de Química de 2024[2]. No dia a dia das pessoas, ferramentas de tradução automática derrubam barreiras de idioma, e recursos de acessibilidade descrevem imagens e o ambiente ao redor para pessoas cegas ou com baixa visão, ampliando a sua autonomia[3]. No trabalho jurídico, do qual tratam os autores desta obra, a tecnologia já auxilia na revisão de contratos e na organização de grandes volumes de documentos, liberando o profissional para se dedicar àquilo que exige julgamento humano.

Nenhum desses exemplos existe sem alguém por trás. O médico continua responsável pelo diagnóstico, o pesquisador pela interpretação dos resultados e o profissional pelo uso que faz das ferramentas à sua disposição. É justamente por reconhecer o quanto a IA pode contribuir que faz sentido discutir com seriedade como usá-la bem.

1. Os fios que atravessam este eixo

Os textos reunidos neste eixo temático conversam entre si em torno de algumas preocupações que reaparecem sempre que a inteligência artificial entra em cena, ainda que cada autor siga o seu próprio percurso. Vale a pena apresentá-las em linhas gerais, porque é na conexão entre elas que este conjunto de reflexões pretende contribuir. São questões que dialogam e se sobrepõem, e nenhuma delas se resolve isoladamente.

Uma dessas preocupações diz respeito aos dados. Sistemas de inteligência artificial aprendem a partir de informações e muitas dessas informações se referem a pessoas. Isso coloca no centro do debate a proteção de dados pessoais e o modo como cada organização coleta, guarda e utiliza aquilo que sabe sobre os indivíduos.

A pergunta que atravessa o tema é como aproveitar o potencial da tecnologia sem descuidar da privacidade e da confiança de quem, no fim das contas, é a razão de existir de qualquer serviço.

Muito próxima dela está a questão da transparência. Boa parte dos sistemas mais avançados funciona de um jeito difícil de acompanhar, mesmo para quem os desenvolve. Nessa linha, compreender minimamente o caminho percorrido pela máquina é o que permite confiar nela, questioná-la quando necessário e corrigi-la quando erra.

Há também o tema dos riscos e dos possíveis efeitos indesejados. Uma tecnologia treinada a partir do retrato do mundo como ele é pode acabar repetindo, e até acentuando, desigualdades e preconceitos que gostaríamos de superar. A esses riscos somam-se preocupações com os impactos sociais e ambientais de sistemas que consomem grande quantidade de dados, energia e atenção. Muitos desses problemas, quando examinados

[1] GOMMERS, J. *et al.* Interval cancer, sensitivity, and specificity comparing AI-supported mammography screening with standard double reading without AI in the MASAI study: a randomised, controlled, non-inferiority, single-blinded, population-based, screening-accuracy trial. *The Lancet*, London, v. 407, n. 10527, p. 505-514, 31 jan. 2026. DOI: https://doi.org/10.1016/S0140-6736(25)02464-X.

LÅNG, K. *et al.* Artificial intelligence-supported screen reading versus standard double reading in the Mammography Screening with Artificial Intelligence (MASAI) trial: a clinical safety analysis of a randomised, controlled, non-inferiority, single-blinded, screening accuracy study. *The Lancet Oncology*, London, v. 24, n. 8, p. 936-944, ago. 2023. DOI: https://doi.org/10.1016/S1470-2045(23)00298-X.

[2] THE ROYAL SWEDISH ACADEMY OF SCIENCES. The Nobel Prize in Chemistry 2024. Estocolmo, 9 out. 2024. Prêmio concedido a David Baker, Demis Hassabis e John M. Jumper. Disponível em: https://www.nobelprize.org/prizes/chemistry/2024/press-release/. Acesso em: 13 jul. 2026.

[3] BE MY EYES. Introducing Be My AI for People who are Blind or Have Low Vision, Powered by OpenAI's GPT-4. 2023. Disponível em: https://www.bemyeyes.com/blog/introducing-be-my-ai. Acesso em: 13 jul. 2026.

de perto, nascem de escolhas humanas sobre como a ferramenta foi construída e para que foi utilizada, o que devolve às pessoas a responsabilidade de enfrentá-los.

Outro fio importante é o da criação. À medida que essas ferramentas passam a auxiliar na produção de textos, imagens, músicas e tantas outras formas de expressão, surgem perguntas sobre autoria e sobre a quem pertence o resultado. São questões novas, ainda em aberto no Brasil e no mundo, que este eixo procura apresentar de forma acessível, sem a pretensão de encerrar um debate que apenas começa.

No fim, todos esses temas convergem para um mesmo desafio prático: o de colocar a inteligência artificial para funcionar com segurança nas mais variadas atividades do dia a dia, do setor privado ao poder público.

2. Para começar a leitura

Voltemos ao computador do início. As perguntas que ele trouxe pareciam, na época, capazes de paralisar setores inteiros da economia e da vida em sociedade. O que as respondeu foi o trabalho paciente de compreender a nova tecnologia e de adaptar a ela as nossas regras e os nossos hábitos, preservando aquilo que realmente importava proteger. Com a inteligência artificial, o caminho tende a ser semelhante. As questões são mais complexas e a velocidade é maior, mas a atitude exigida continua a mesma. Procurar entender antes de julgar, separar o que a tecnologia de fato faz daquilo que apenas se imagina que ela faça e manter a pessoa humana no centro das decisões que produzem consequências.

Este capítulo não oferece um manual de respostas prontas, porque o tema ainda não as comporta, e desconfiar de quem as promete já é um bom começo. O que ele oferece é um modo de olhar. Encarar a inteligência artificial como aquilo que ela de fato é e, a partir daí, discutir com seriedade os caminhos para que ela se some ao que temos de melhor em vez de nos substituir. As páginas seguintes são um convite a esse aprendizado.

Riscos associados à Inteligência Artificial:

vieses, opacidade e impactos sociais e ambientais

Da promessa tecnológica à responsabilidade corporativa: por uma governança de IA orientada a riscos concretos

Gustavo Godinho

Gustavo Godinho é executivo jurídico e de P&PD. Responsável por implementar programa de adequação de P&PD em três grandes empresas. Atualmente, está head jurídico e DPO da Foggo Entertainment, além de palestrante e professor convidado em diversas instituições de ensino. É autor e coordenador de livros sobre P&PD e IA. Certificado como DPO(ECPC-B) da Maastricht University. De 22 a 25 foi eleito como um dos cinco profissionais de P&PD mais admirados do Brasil (Compliance on Top).

Introdução

A Inteligência Artificial (IA) deixou de ser tema meramente de inovação para se tornar também tema de governança, risco e responsabilidade jurídica. Sistemas que classificam candidatos a emprego, definem limites de crédito, apoiam decisões judiciais, moderam conteúdo e otimizam cadeias logísticas operam hoje em escala industrial dentro de empresas em diversos países, incluindo as brasileiras, muitas vezes sem que a própria organização tenha plena visibilidade sobre como as decisões são geradas internamente pelo modelo. Esse descompasso entre a velocidade de adoção da tecnologia e a maturidade dos mecanismos de controle é o problema central deste artigo.

Três riscos concentram a atenção de reguladores, tribunais, departamentos jurídicos e de Privacidade e Proteção de Dados ("P&PD") ao redor do mundo, inclusive por aqui no Brasil: (i) o viés algorítmico que reproduz e, por vezes, amplifica desigualdades históricas presentes nos dados de treinamento; (ii) a opacidade, ou o chamado problema da "caixa-preta", que dificulta a explicação de decisões automatizadas e compromete o devido processo; e (iii) os impactos sociais e ambientais, que vão da reconfiguração do mercado de trabalho ao consumo intensivo de energia e água pela infraestrutura de data centers. Cada um desses eixos, isoladamente, já justificaria um programa robusto de compliance. Somados, formam um quadro que exige da liderança jurídica e de P&PD, ao menos, um papel ativo e não meramente reativo na condução dos projetos de IA.

O objetivo deste artigo é examinar esses três riscos a partir de casos concretos e documentados, internacional e nacionalmente, relacioná-los ao arcabouço regulatório já existente (Lei Geral de Proteção de Dados – LGPD, Marco Civil da Internet – MCI), assim como ao que está em construção no Brasil (Projeto de Lei nº 2.338/2023)[1] e, sobretudo, discutir como a governança de IA vem sendo implementada na prática por empresas de diferentes setores. A justificativa é direta: no atual estágio, ainda incompleto, da regulação brasileira específica sobre IA, a governança corporativa não é opcional e muito menos decorativa. Ela é, para o Jurídico e P&PD, o principal instrumento disponível para transformar risco em previsibilidade e inovação em vantagem competitiva sustentável.

Ouso registrar uma advertência metodológica, que considero coerente com o rigor que se espera de um texto técnico-jurídico: o cenário regulatório e os dados quantitativos sobre consumo de recursos por sistemas de IA mudam com grande velocidade e são, em sua maioria, estimativas construídas por metodologias distintas entre si. O detalhamento aqui apresentado pretende refletir sobre o conhecimento existente e disponível até a conclusão da versão final deste artigo.

[1] PL 2338/2023 ou PL da Inteligência Artificial, é uma proposta legislativa apresentada no plenário do Senado Federal que visa estabelecer o marco regulatório para o desenvolvimento e uso de inteligência artificial no Brasil.

1. Desenvolvimento

1.1 Vieses algorítmicos: da promessa de neutralidade à reprodução de desigualdades

A ideia de que sistemas de IA seriam mais "neutros" do que decisões humanas, por não estarem sujeitos a emoções ou preconceitos conscientes, é hoje amplamente contestada pela literatura técnica e jurídica. Um modelo de aprendizado de máquina aprende padrões a partir dos dados com que é treinado; se esses dados refletem desigualdades históricas (de raça, gênero, classe social, região geográfica), o modelo tende a reproduzir e, em certos casos, amplificar essas desigualdades sob uma aparência de objetividade matemática.

O caso mais citado na literatura internacional é o do sistema Correctional Offender Management Profiling for Alternative Sanctions (COMPAS), utilizado por tribunais norte-americanos para estimar o risco de reincidência criminal. Uma investigação da ProPublica revelou que o sistema atribuía taxas de falso-positivo significativamente mais altas para réus negros do que para réus brancos, isto é, classificava com mais frequência pessoas negras como de "alto risco" mesmo quando não reincidiam (Angwin *et al.*, 2016). É importante registrar, com o rigor que o tema exige, que a metodologia da ProPublica foi posteriormente contestada por outros pesquisadores, que questionaram os critérios estatísticos de aferição de viés utilizados (Flores; Bechtel; Lowenkamp, 2016). O episódio, ainda que controverso em seus detalhes técnicos, tornou-se paradigmático por expor uma questão que nenhuma empresa pode mais ignorar: diferentes definições estatísticas de "justiça algorítmica" podem ser, entre si, matematicamente incompatíveis, e a escolha de qual métrica adotar é, em si, uma decisão de política organizacional, e não uma decisão puramente técnica.

No ambiente corporativo, o exemplo mais conhecido é o da ferramenta interna de recrutamento desenvolvida pela gigante *bigtech* Amazon, descontinuada após se constatar que o sistema penalizava currículos que continham a palavra "mulheres" e rebaixava a pontuação de candidatas oriundas de faculdades exclusivamente femininas. O viés decorreu do fato de o modelo ter sido treinado com currículos submetidos à empresa ao longo de dez anos, período em que a maioria dos contratados no setor de tecnologia era do sexo masculino (Dastin, 2018).

No Brasil, a LGPD já oferece uma primeira camada de resposta a esse risco, ao assegurar (em seu artigo 20) o direito do titular de solicitar revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses. O PL 2.338/2023, se aprovado, sancionado e convertido em lei, considerando a última versão "conhecida", pode ampliar esse regime ao tratar expressamente os vieses algorítmicos como categoria de risco e ao prever, para sistemas de alto risco, obrigações de avaliação prévia de impacto e de auditoria periódica.

Na prática corporativa, o enfrentamento do viés não se resolve apenas com cláusulas contratuais. Tal enfrentamento exige (i) testes de equidade estatística antes da entrada em produção; (ii) auditoria periódica de resultados segmentados por grupo demográfico; (iii) times de desenvolvimento diversos e, sobretudo, (iv) supervisão humana significativa sobre decisões de alto impacto. Um caso público e possível de ser mencionado é o do Banco do Brasil que ilustra esse movimento: a instituição financeira estruturou, em parceria com as consultorias globais

IBM e EY, uma governança que incorpora regras, fases e controles de mitigação de viés ao longo de todo o ciclo de vida dos modelos, apoiada na plataforma de gestão de risco de IA da IBM e na metodologia de ciclo de vida de IA generativa da EY.

O caso é relevante porque demonstra que governança de viés não é apenas política escrita: é infraestrutura técnica de monitoramento contínuo, construída com apoio de parceiros estratégicos e especializados[2].

1.2 Opacidade e o problema da caixa-preta algorítmica

O segundo risco decorre diretamente do primeiro: mesmo quando um viés é identificado, nem sempre é possível explicar por que o modelo chegou a um resultado específico. Modelos de aprendizado profundo (*deep learning*) e grandes modelos de linguagem processam informação por meio de milhões (ou até bilhões) de parâmetros interconectados, de modo que a relação entre a entrada (*input*) e a saída (*output*) frequentemente não é redutível a uma explicação causal simples e compreensível por um ser humano. É o que a literatura técnica chama de "problema da caixa-preta".

A opacidade não é um detalhe técnico secundário: tem consequências jurídicas diretas sobre devido processo, direito de defesa e responsabilização civil. Se uma instituição financeira nega crédito, se um sistema de triagem elimina um candidato ou se uma seguradora recusa cobertura com base em um modelo de IA, o afetado precisa de uma explicação minimamente inteligível para poder contestar a decisão. Sem explicabilidade, o direito de revisão previsto na LGPD e a "supervisão humana significativa" exigida na versão mais recente conhecida do PL 2.338/2023, correm o risco de se tornar exercícios formais, sem efetividade prática. A pessoa designada para "revisar" a decisão pode não ter, ela própria, acesso aos critérios reais utilizados pelo modelo.

O EU AI Act[3], publicado no Jornal Oficial da União Europeia em julho de 2024 e com aplicação (*enforcement*) "fatiada" e escalonada a partir de então (cronograma que o atual Digital Omnibus[4], também europeu, propõe flexibilizar e postergar), endereça esse problema ao impor, para sistemas classificados como de alto risco, obrigações de documentação técnica, registro de *logs* e transparência mínima que permitam auditoria externa.

O modelo brasileiro de regulação (conforme a versão conhecida até o momento), atualmente em tramitação, deve seguir lógica semelhante, ao classificar sistemas por nível de risco e vincular obrigações de explicabilidade e documentação à intensidade desse risco.

No plano da governança corporativa, a resposta mais consolidada à opacidade tem sido a criação de comitês multidisciplinares/*multistakeholders* de ética em IA, com poderes que variam conforme a organização. Empresas como a Adobe estruturaram comitês com poder não apenas consultivo, mas também de suspender a implantação de tecnologia que não observe princípios de responsabilidade e transparência; já a Panasonic ado-

[2] IBM NEWSROOM BRASIL. *Banco do Brasil adota governança de IA com IBM e EY e reforça seu compromisso com transparência, ética e confiabilidade*. São Paulo, 17 jun. 2025. Disponível em: https://brasil.newsroom.ibm.com/news?item=122949. Acesso em: 30 jun. 2026 e 18 jul.2026.

[3] EU AI Act ou Regulamento sobre Inteligência Artificial (IA) é uma norma sobre o uso da inteligência artificial na União Europeia. Proposto pela Comissão Europeia em 21 de abril de 2021, tem por objetivo introduzir um quadro regulamentar e jurídico comum para a IA. O seu âmbito abrange todos os setores (exceto o militar) e todos os tipos de IA. Disponível em: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/por.

[4] COMISSÃO EUROPEIA. Proposta «Omnibus Digital» sobre o Regulamento Inteligência Artificial. Comissão Europeia, [*S. l.*], 19 nov. 2025. Disponível em: https://digital-strategy.ec.europa.eu/pt/library/digital-omnibus-ai-regulation-proposal. Acesso em: 30 jun. 2026.

tou modelo de atuação mais preventiva, concentrado na avaliação de risco dos projetos antes de sua execução. Ambos os *cases* são referenciados em texto escrito pelo brasileiro Eduardo Magrani, consultor sênior na área de TMT da CCA Law Firm[5]. No Brasil, o Centro de Ensino e Pesquisa em Inovação (CEPI) da FGV Direito SP sistematizou, a partir de pesquisa de campo com empresas, um *framework* de seis etapas para a estruturação desses comitês, da definição de responsabilidades à elaboração de relatórios de impacto algorítmico (Coelho *et al.*, 2023). Trata-se de modelo replicável, mas que depende de recursos e maturidade organizacional, que (infelizmente) nem toda empresa brasileira ainda possui.

1.3 Impactos sociais: mercado de trabalho, concentração de poder e desinformação

Os impactos sociais da IA transcendem a relação individual entre sistema e usuário. No mercado de trabalho, a automação de tarefas cognitivas, antes consideradas imunes à automação, ao contrário de tarefas manuais repetitivas, tem gerado transformações relevantes em funções de atendimento, análise de dados, redação de primeiras versões de documentos e triagem administrativa. O debate jurídico relevante aqui não é apenas trabalhista (extinção ou recolocação de postos), mas também de gestão algorítmica: sistemas que distribuem tarefas, avaliam desempenho e influenciam remuneração de trabalhadores de plataforma, com reduzida margem de contestação humana sobre os critérios aplicados.

Há também uma dimensão de concentração de poder informacional. O desenvolvimento de modelos de fronteira exige capacidade computacional, acesso a dados em larga escala e investimento que apenas um número reduzido de empresas globais consegue sustentar, o que levanta preocupações concorrenciais e de soberania digital, tema este que, no Brasil, dialoga diretamente com discussões sobre infraestrutura nacional de dados e com o próprio desenho institucional do PL 2.338/2023, que cria o Sistema Nacional de Regulação e Governança de Inteligência Artificial (SAI).

Por fim, a capacidade da IA generativa de produzir textos, imagens, áudios e vídeos sintéticos de alta verossimilhança (*deepfakes*) tem impacto direto sobre a integridade informacional, especialmente em períodos eleitorais. O Tribunal Superior Eleitoral (TSE) já editou resoluções específicas sobre o uso de IA nas eleições de 2024 e a proximidade do calendário eleitoral de 2026 tende a intensificar esse debate, o que, segundo análises recentes do setor, pode inclusive acelerar a tramitação do próprio PL 2.338/2023 na Câmara dos Deputados[6]. Oremos!

1.4 Impactos ambientais: a "pegada" material da IA

Ouso dizer que, talvez, o risco menos discutido pelos Departamentos Jurídicos e de P&PD, até recentemente, seja o ambiental. Diferentemente dos vieses e da opacidade, cujos efeitos são majoritariamente informacionais, o impacto ambiental da IA é físico e mensurável: energia elétrica, água para resfriamento de servidores ("*chillers*") e ocupação de solo para construção de *data centers*.

Um relatório do Instituto de Água, Meio Ambiente e Saúde da Organização das Nações Unidas, divulgado em junho de 2026, apresentou uma das análises mais abrangentes já realizadas sobre esses impactos. Segundo o estudo, a operação e o resfriamento da infraestrutura global de IA poderão demandar, até 2030, um volume de água equivalente ao consumo doméstico básico de aproximadamente 1,3 bilhão de pessoas, com uso total estimado em cerca de 9,3 trilhões de litros. O mesmo relatório estima que treinar um único modelo de grande porte pode consumir eletricidade em volume comparável ao consumo residencial anual de centenas de milhares de pessoas em regiões de baixa renda, além de gerar

[5] MAGRANI, Eduardo. Governação de Algoritmos e Comitê de Ética de IA. *CCA Law Firm, Insights & Media* (Newsletters), 15 dez. 2023. Disponível em: https://www.cca.law/pt/insights-and-media/newsletters/Governacao-de-Algoritmos-e-Comite-de-Etica-de-IA/9187/. Acesso em: 22 out. 2026.

[6] BARBIERI ADVOGADOS. Regulamentação da inteligência artificial no Brasil: estado atual e perspectivas. 2026. Disponível em: https://www.barbieriadvogados.com/regulamentacao-inteligencia-artificial-brasil/. Acesso em: 30 jun. 2026.

pegada territorial que, em casos individuais, chega à extensão de centenas de campos de futebol[7]. São números que devem ser lidos como estimativas de um estudo recente (e não como medição direta e consolidada) dada a diversidade de metodologias hoje empregadas para mensurar consumo de recursos por infraestrutura de IA.

Nessa mesma linha, projeções setoriais indicam que o consumo elétrico global de *data centers*, não exclusivamente de IA, mas forte e intensamente impulsionado por ela, pode ter alcançado aproximadamente 485 *terawatts*-hora em 2025, com estimativas de alta para algo entre 950 e 1.050 *terawatts*-hora até 2030, o que representaria próximo de 3% da demanda mundial de eletricidade[8]. Posicionamento setorial apresentado por sócio de uma *Big4* (*EY*) por ocasião da *COP30* apontou ainda[9] que o treinamento de modelos de IA generativa pode consumir até oito vezes mais energia do que o treinamento de modelos tradicionais de aprendizado de máquina, e que as emissões de carbono associadas ao treinamento de modelos de fronteira cresceram de forma expressiva desde os primeiros grandes modelos de linguagem lançados no início desta década, crescimento que vale certamente verificar em fonte primária, dada a diversidade de metodologias de mensuração adotadas pelas próprias empresas do segmento de tecnologia.

Do ponto de vista jurídico, esse quadro desloca o debate ambiental da IA do campo estritamente reputacional, como relatórios de ASG (Ambiental, Social e Governança) voluntários, para o campo regulatório: licenciamento ambiental de *data centers*, estudos de impacto ambiental que contemplem o ciclo de vida completo da infraestrutura digital e zoneamento de áreas sensíveis à escassez hídrica passam a ser, ou deveriam passar a ser, exigências concretas de órgãos ambientais estaduais e municipais, tema ainda incipiente no arcabouço regulatório brasileiro específico de IA, mas já identificado pela doutrina especializada como fronteira necessária de regulação[10].

1.5 Da regulação à prática: governança de IA como resposta institucional

O arcabouço regulatório brasileiro está em formação acelerada, mas ainda incompleto. O PL 2.338/2023 foi aprovado pelo Senado Federal em 10 de dezembro de 2024 e permanece, até a data deste artigo, em tramitação na Câmara dos Deputados, sob relatoria do deputado Aguinaldo Ribeiro, com votação final prevista, mas não garantida, para 2026 (afirmação reiteradamente feita em meus *posts* semanais do SentAI & AtentAI, por meio do meu perfil[11] na rede social LinkedIn). A versão até o momento conhecida do texto adota abordagem baseada em risco, inspirada no EU AI Act, classificando sistemas de IA em risco excessivo (proibido), alto risco (sujeito a obrigações materiais, como avaliação de impacto algorítmico e supervisão humana) e demais categorias de risco mais leve, além de prever sanções que podem chegar a até 2% do faturamento da empresa ou grupo econômico, limitadas a R$ 50 milhões por infração (idêntico ao "*cap*" constante na LGPD), sem abordar o detalhamento para cálculo de dosimetria de sanção.

Enquanto essa estrutura legal não se consolida, a LGPD, o MCI, *frameworks* e *guidelines* internacionais, assim como alguns documentos de entidades setoriais seguem sendo a base normativa disponível, porém insuficiente: regulam o tratamento de dados pessoais que alimentam

[7] ONU NEWS. Consumo de água por centros de dados de IA pode chegar a 9,3 trilhões de litros. *ONU News*, [*S. l.*], 3 jun. 2026.. Disponível em: https://news.un.org/pt/story/2026/06/1853321. Acesso em: 30 jun. 2026.

[8] CRISOFT. Impacto ambiental da IA: energia, água e uso consciente. *Crisoft*, Piracicaba, 25 jun. 2026. Disponível em: https://www.crisoft.com.br/noticias/impacto-ambiental-inteligencia-artificial-uso-consciente. Acesso em: 30 jun. 2026.

[9] EY. COP30: IA desafia agenda climática em relação ao consumo de energia e água. *EY*, [*S. l.*], 18 nov. 2025. Disponível em: https://www.ey.com/pt_br/newsroom/2025/11/ia-desafia-agenda-climatica-consumo-energia-agua. Acesso em: 30 jun. 2026 e 18 jul.2026.

[10] FERRARI, Vanessa Carolina Fernandes. Inteligência artificial: bits que pesam toneladas. *Consultor Jurídico*, São Paulo, 21 abr. 2026.. Disponível em: https://www.conjur.com.br/2026-abr-21/inteligencia-artificial-bits-que-pesam-toneladas/. Acesso em: 30 jun. 2026.

[11] Gustavo Godinho.. Perfil que publica os posts semanais "SentAI & AtentAI" na rede social LINKEDIN. Disponível em: https://www.linkedin.com/in/gustavogodinho/.

os modelos, mas não o funcionamento, o risco nem os impactos dos sistemas, as ferramentas e aplicações de IA propriamente ditos, independentemente de estes envolverem ou não dados pessoais.

Diante dessa lacuna, a governança corporativa de IA deixou de ser exercício de antecipação regulatória e passa a se tornar necessidade operacional imediata. Na prática observada em empresas brasileiras e internacionais, essa governança se estrutura, tipicamente, em torno de: (i) comitês multidisciplinares que reúnem jurídico, compliance, tecnologia, cibersegurança, riscos, negócios, recursos humanos, comunicação e eventuais outras áreas internas de uma empresa; (ii) inventário e classificação de sistemas de IA por nível de risco; (iii) avaliação de impacto algorítmico (AIA) prévia à implantação de sistemas de alto risco; (iv) políticas de transparência ao usuário final; (v) regras para evitar não só o *shadow IT* mas, inclusive, o *shadow AI*; (vi) protocolos de supervisão humana em decisões de alto impacto; e (vii) trilhas de auditoria documentadas.

A abordagem de "*Trusted AI*", proposta por consultorias como a KPMG, sintetiza a lógica que deveria orientar a liderança jurídica e de P&PD: o objetivo não é apenas cumprir requisitos regulatórios, mas criar condições para inovar com segurança, resiliência e responsabilidade[12]. O risco de não o fazer não se resume somente à imposição de uma sanção administrativa (muitas vezes pecuniária em especial): envolve dano reputacional, exposição a litígios, obstáculos em operações de fusões e aquisições (M&A), nas quais a ausência de programa de adequação de IA já é tratada como fator de deságio por investidores sofisticados e, em mercados regulados, pode ser considerada como risco de impacto em negociações comerciais/societárias.

Conclusão

Os três riscos examinados neste artigo: (i) viés algorítmico; (ii) opacidade; e (iii) impactos sociais e ambientais, não são hipóteses futuras a serem endereçadas apenas quando a regulação brasileira finalmente amadurecer. São riscos atuais e iminentes, muitas vezes já presentes, documentados por casos concretos e por dados que, mesmo sujeitos a atualização constante, já indicam tendência inequívoca de crescimento em escala e intensidade.

Para a advocacia empresarial e para os DPOs, CISOs e, mais atualmente, CAIOs, a lição prática é dupla. Primeiro: a ausência de lei específica em vigor no Brasil não significa ausência de risco jurídico: a LGPD, o MCI, o Código de Defesa do Consumidor (CDC) e os princípios gerais de responsabilidade civil já oferecem base suficiente para responsabilização em casos de dano decorrente de viés discriminatório ou de decisão automatizada cujo funcionamento seja comprovadamente inexplicável. Segundo: esperar a finalização da tramitação do PL 2.338/2023 para começar a estruturar governança de IA é estratégia que subestima tanto o risco reputacional quanto o comercial, ambos já presentes hoje, como demonstram os mais diversos exemplos atualmente disponíveis, entre eles os casos analisados neste texto.

A governança de IA, nesse sentido, não deve ser compreendida como um freio à inovação, mas como sua pré-condição de sustentabilidade. Empresas que estruturam comitês de ética, processos de auditoria de viés, mecanismos de explicabilidade e políticas de mensuração de impacto ambiental não apenas se protegem de sanções futuras: constroem a legitimidade social necessária para operar e escalar sistemas de IA em ambiente de escrutínio público crescente. É esse o papel que cabe, hoje, à liderança jurídica e/ou de P&PD, não apenas identificando riscos, mas transformando-os em habilitadoras estratégicas dos usos de IA que sejam, ao mesmo tempo, competitivos, éticos, inovadores, com riscos (de alguma forma) mitigados e, não menos importante, ambientalmente responsáveis.

[12] KPMG. Governança de Inteligência Artificial no Brasil. *KPMG Insights*, [*S. l.*], 19 maio 2026. Disponível em: https://kpmg.com/br/pt/insights/2026/05/governanca-inteligencia-artificial-brasil.html. Acesso em: 18 jul. 2026.

Referências

ANGWIN, Julia; LARSON, Jeff; MATTU, Surya; KIRCHNER, Lauren. Machine Bias: there's software used across the country to predict future criminals. And it's biased against blacks. *ProPublica*, [*S. l.*], 23 maio 2016. Disponível em: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing. Acesso em: 30 jun. 2026.

BARBIERI ADVOGADOS. *Regulamentação da inteligência artificial no Brasil: estado atual e perspectivas.* 2026. Disponível em: https://www.barbieriadvogados.com/regulamentacao-inteligencia-artificial-brasil/. Acesso em: 30 jun. 2026.

BRASIL. *Lei nº 12.965, de 23 de abril de 2014*. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 22 out. 2026.

BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 22 out. 2026.

BRASIL. *Projeto de Lei nº 2.338, de 2023*. Brasília, DF: Câmara dos Deputados, 2023. Aprovado pelo Senado Federal em 10 dez. 2024 e remetido à Câmara dos Deputados em 17 mar. 2025, onde tramita. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2487262. Acesso em: 22 out. 2026.

BRASIL. Projeto de Lei nº 6.237, de 2025. Institui o Sistema Nacional para Desenvolvimento, Regulação e Governança de Inteligência Artificial. Brasília, DF: Câmara dos Deputados, 2025. Apensado ao Projeto de Lei nº 2.338, de 2023. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2594000. Acesso em: 22 out. 2026.

COELHO, Alexandre Zavaglia; KLAFKE, Guilherme Forma; MAITO, Deíse Camargo; LATINI, Lucas Maldonado Diz; MARUCA, Gabriela; CHOW, Bruno Gonzaga; FEFERBAUM, Marina. *Governança da inteligência artificial em organizações: framework para Comitês de Ética em IA* – versão 1.0. São Paulo: CEPI FGV Direito SP, 2023. Disponível em: https://hdl.handle.net/10438/33736. Acesso em: 30 jun. 2026.

COMISSÃO EUROPEIA. Proposta *«Omnibus Digital» sobre o Regulamento Inteligência Artificial*. Bruxelas, 19 nov. 2025. Disponível em: https://digital-strategy.ec.europa.eu/pt/library/digital-omnibus-ai-regulation-proposal. Acesso em: 18 jul. 2026.

CONJUR. *Inteligência artificial: bits que pesam toneladas*. Consultor Jurídico, 21 abr. 2026. Disponível em: https://www.conjur.com.br/2026-abr-21/inteligencia-artificial-bits-que-pesam-toneladas/. Acesso em: 30 jun. 2026 e 18 jul.2026.

CRISOFT. Impacto ambiental da IA: energia, água e uso consciente. Crisoft Soluções Web, [*S. l.*], 25 jun. 2026. Disponível em: https://www.crisoft.com.br/noticias/impacto-ambiental-inteligencia-artificial-uso-consciente. Acesso em: 18 jul. 2026.

DASTIN, Jeffrey. Amazon scraps secret AI recruiting tool that showed bias against women. *Reuters*, São Francisco, 10 out. 2018. Disponível em: https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G. Acesso em: 18 jul. 2026.

EY BRASIL. COP30: IA desafia agenda climática em relação ao consumo de energia e água. *EY Newsroom*, [*S. l.*], 18 nov. 2025. Disponível em: https://www.ey.com/pt_br/newsroom/2025/11/ia-desafia-agenda-climatica-consumo-energia-agua. Acesso em: 18 jul. 2026.

FERRARI, Vanessa Carolina Fernandes. Inteligência artificial: bits que pesam toneladas. *Consultor Jurídico*, [*S. l.*], 21 abr. 2026. Disponível em: https://www.conjur.com.br/2026-abr-21/inteligencia-artificial-bits-que-pesam-toneladas/. Acesso em: 18 jul. 2026.

FLORES, Anthony W.; BECHTEL, Kristin; LOWENKAMP, Christopher T. False positives, false negatives, and false analyses: a rejoinder to "Machine Bias: There's software used across the country to predict future criminals and it's biased against blacks". *Federal Probation Journal*, [*S. l.*], v. 80, n. 2, p. 38-46, 2016.

Gustavo Godinho. *Perfil que publica os posts semanais "SentAI & AtentAI" na rede social LINKEDIN*. Disponível em: https://www.linkedin.com/in/gustavogodinho/. Acesso em: 18 jul. 2026.

IBM NEWSROOM BRASIL. Banco do Brasil adota governança de IA com IBM e EY e reforça seu compromisso com transparência, ética e confiabilidade. *IBM Newsroom Brasil*, São Paulo, 17 jun. 2025. Disponível em: https://brasil.newsroom.ibm.com/news?item=122949. Acesso em: 18 jul. 2026.

KPMG. Governança de Inteligência Artificial no Brasil. *KPMG Insights*, [*S. l.*], 19 maio 2026. Disponível em: https://kpmg.com/br/pt/insights/2026/05/governanca-inteligencia-artificial-brasil.html. Acesso em: 18 jul. 2026.

MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS. PL do governo propõe sistema de governança para a inteligência artificial no país. *Agência Gou*, Brasília, 9 dez. 2025. Disponível em: https://agenciagov.ebc.com.br/noticias/202512/pl-do-governo-propoe-sistema-de-governanca-para-a-inteligencia-artificial-no-pais. Acesso em: 18 jul. 2026.

MIND GROUP. EU AI Act e PL 2338: o que muda na sua operação em 2026. *Mind Group*, Sorocaba, 29 abr. 2026. Disponível em: https://mindconsulting.com.br/2026/04/eu-ai-act-pl-2338-regulacao-ia-empresas-brasileiras-2026/. Acesso em: 18 jul. 2026.

ONU NEWS. Consumo de água por centros de dados de IA pode chegar a 9,3 trilhões de litros. *ONU News*, [*S. l.*], 3 jun. 2026. Disponível em: https://news.un.org/pt/story/2026/06/1853321. Acesso em: 18 jul. 2026.

UNIÃO EUROPEIA. *Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024*: que cria regras harmonizadas em matéria de inteligência artificial e que altera os Regulamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e as Diretivas 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (Regulamento da Inteligência Artificial). [S. l.]: Jornal Oficial da União Europeia, 12 jul. 2024. Disponível em: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/por. Acesso em: 24 jul. 2026.

Criatividade induzida por sistemas de IA:

quem é o autor e a quem pertencem os direitos?

Tatiana Machado Dunshee de Abranches

Tatiana Machado Dunshee de Abranches é gerente Jurídica Empresarial e Cível da Firjan. Mestre em Direito das Atividades Econômicas pela UERJ e pós-graduada em Direito Público pela EMERJ e em Direito Ambiental pela PUC-RJ, com graduação em Direito pela PUC-RJ.

Introdução

A criação intelectual é inata ao ser humano, pois a todo instante ele tem ideias e cria algo. Todos possuem um potencial criativo que pode resultar em bens ou criações passíveis de aproveitamento econômico. Essa é a razão da existência do direito autoral, que incide sobre as obras intelectuais protegidas, como textos de obras literárias, artísticas ou científicas; e os direitos conexos, que protegem os artistas, intérpretes, executores e produtores de fonogramas e radiodifusão. O direito do autor nasce com a exteriorização da criação intelectual, independentemente de registro, que nesse caso tem efeito declaratório.

O uso crescente da Inteligência Artificial (IA) tem levantado um debate relevante sobre autoria. Afinal, é possível reconhecer a máquina como produtora de uma obra ou seria ela apenas mais uma ferramenta tecnológica? Os sistemas de IA generativa são capazes de gerar textos, imagens, músicas e outros conteúdos, porque foram treinados com obras humanas protegidas por direito autoral. Porém, como muitas vezes não há autorização e remuneração aos criadores das obras originais, cria-se um conflito difícil de solucionar, já que esses mesmos autores, cujos trabalhos alimentaram o aprendizado da máquina, enfrentam concorrência da própria ferramenta que os consumiu e nada pagou por isso.

A revolução das IAs generativas tem gerado um impacto disruptivo sobre o conceito clássico da autoria. A questão central é determinar a quem pertencem os direitos quando um ser humano usa IA como ferramenta criativa. O resultado dessa problemática pode variar a depender do modelo de criação, isto é, quando a IA é utilizada como ferramenta; quando ela é cocriadora e quando ela atua sem intervenção humana relevante, ou seja, quando a IA age como criadora autônoma.

O debate a respeito dessa temática tem sido intenso e não se pretende com esse artigo chegar a uma resposta efetiva, tendo em vista a atual ausência de um quadro regulatório do uso da IA no Brasil. O caminho para uma regulação, tal como desenhada no Projeto de Lei nº 2.338/2023 que vem sendo discutido no Congresso Nacional, porém, é duvidoso, não só com relação à sua necessidade, como também ao tratamento dado ao tema. No entanto, a reflexão é válida e necessária, considerando o impacto gerado e que ainda gerará na sociedade. Portanto, a grande batalha atual do direito autoral brasileiro é se ele, tal como está, serve para regular o que a IA produz.

1. O conceito clássico de autoria e seus pressupostos

O artigo 11 da Lei nº 9.610/1998 (Lei de Direitos Autorais - LDA) considera autor a **pessoa física** criadora de obra literária, artística ou científica; ou seja, a lei vincula a autoria à existência de uma pessoa. Assim sendo, a premissa inequívoca do direito autoral brasileiro é a de que a autoria está necessariamente vinculada ao ser humano criador.

Ocorre que os sistemas de inteligência artificial operam por meio de algoritmos, que são treinados com grandes volumes de dados e geram conteúdo a partir de padrões, sem processo criativo ou expressão subjetiva. Logo, de antemão, reconhecer a IA como titular de direitos de autor implicaria admitir que um ente desprovido de personalidade jurídica possa figurar como sujeito de direitos, o que, por si só, contraria a legislação vigente. Nesse sentido, o autor seria sempre o humano, seja o desenvolvedor do sistema, seja o usuário que elabora os *prompts*, e a IA seria sempre a ferramenta.

Observando a evolução histórica dos direitos autorais no mundo, é importante destacar os dois principais sistemas de proteção existentes: o *copyright* e o *droit d´auteur*, sendo o segundo o sistema adotado pelo Brasil.

O sistema do *copyright* é oriundo dos países anglo-saxões e da *commom law*. Nesse sistema, a proteção recai sobre a obra, especificamente sobre a reprodução da obra, o viés econômico é preponderante e tido como um instrumento facilitador e viabilizador de sua circulação. Já o

sistema do *droit d´auteur* é oriundo do direito francês, do direito *civil law*. Nele, a proteção recai precipuamente sobre o autor. Para esse sistema, a dimensão do direito moral é preponderante, razão pela qual prepondera o conceito da dignidade da pessoa humana e das características da personalidade do autor sobre sua obra.

O direito autoral brasileiro é oriundo do sistema do *droit d´auteur* e assim o aspecto moral é algo determinante e tem raiz constitucional (artigo 5º, XXVII e XXVIII), pois garante ao autor o direito exclusivo de utilização, publicação ou reprodução de suas obras; bem como assegura a proteção às participações individuais em obras coletivas e à reprodução da imagem e voz humanas, além do direito de fiscalizar o aproveitamento econômico das obras. Dessa forma, o legislador constituinte garantiu aos autores a faculdade de oferecer ou não ao público o acesso à sua obra e, ao inserir o tema no Título II, que cuida dos direitos e garantias fundamentais, elevou esse instituto à categoria de especial proteção institucional.

A Lei de Direitos Autorais (LDA), por sua vez, apresenta uma série de dispositivos que demonstram o poder do autor ou de seus representantes de proibir ou decidir quem utilizará e como serão exploradas economicamente suas criações. A definição desse poder depende do enquadramento, da natureza jurídica atribuída ao direito autoral, pois caso se entenda que é um direito patrimonial, a lógica é puramente econômica e disponível; se é de um direito da personalidade, é intransferível e pressupõe necessariamente uma pessoa; se é *sui generis*, abre-se caminho para uma terceira via.

A natureza do direito autoral é determinante para a discussão sobre a autoria de obras criadas por meio de sistema de IA. Essa discussão não é acadêmica; ela define se a proteção pode existir sem que haja um autor humano; se os direitos são ou não transferíveis; se uma IA pode ou não ser titular, ainda que por ficção jurídica; se o investimento do desenvolvedor ou do usuário pode ser protegido mesmo na ausência de criação humana e qual será o regime de responsabilidade por eventual violação de direito autoral.

A corrente patrimonialista enquadra o direito autoral como espécie de propriedade intelectual, com natureza essencialmente econômica. O direito recai sobre a obra como bem imaterial passível de exploração, circulação e alienação. Seus defensores se apoiam no artigo 5º, XXVII, da Constituição da República, que garante ao autor o direito exclusivo de utilização, publicação ou reprodução de suas obras, e nos artigos 28 a 45 da LDA, que regulam os direitos patrimoniais como monopólio de exploração econômica.

Nessa lógica, a obra é um ativo econômico que pode ser cedido, licenciado ou transmitido *mortis causa*. O autor é relevante para concepção histórica do bem, mas o que a lei protege, na prática, é a exploração econômica do resultado. A corrente patrimonialista é a que acomoda mais facilmente a proteção de obras geradas por IA, pois, na medida em que o que importa é o investimento econômico e o resultado útil, não a subjetividade do criador, então o desenvolvedor que investiu capital e tecnologia no sistema pode ser reconhecido como titular dos direitos patrimoniais sobre as obras por ele geradas. É o modelo adotado pelo Reino Unido no "Copyright, Designs and Patents Act" de 1988, que reconhece direitos sobre *computer-generated works* e atribui autoria à pessoa responsável pelos arranjos necessários para a criação.

A corrente do direito da personalidade sustenta que o direito autoral é, em sua essência, uma expressão da personalidade do criador, o vínculo indissolúvel entre o autor e sua obra. Tem como base os direitos morais do autor, que no Brasil estão consagrados no artigo 24 da LDA, que expressa o direito de ter o nome reconhecido na obra, de manter a obra inédita, de assegurar sua integridade, de modificá-la ou retirá-la de circulação. Esses direitos são inalienáveis e irrenunciáveis, não podem ser cedidos nem transferidos, nem mesmo por contrato.

Essa corrente é a que menos acomoda qualquer proteção autoral a obras geradas por IA, pois, se o direito autoral é expressão da personalidade humana, não pode existir onde não há pessoa. Uma IA não tem honra, não tem nome; portanto, não pode ser sujeito de direitos morais, e sem direitos morais não há autoria no sentido pleno da lei. Essa é a posição dominante na doutrina brasileira contemporânea, que encontra suporte no artigo 11 da LDA, que considera autor a pessoa física criadora de obra. O problema é que essa corrente leva ao domínio público automático de tudo que a IA produz, consequência que nenhum agente do setor aceita como solução definitiva.

A corrente dominante na doutrina internacional e crescentemente adotada no Brasil é a da teoria dualista ou do direito *sui generis*, que preceitua que o direito autoral é um gênero próprio, que reúne de forma indissociável

aspectos patrimoniais e morais, sem se reduzir a nenhum deles. Não é propriedade comum, pois tem dimensão personalíssima. Não é direito da personalidade puro, pois é plenamente passível de cessão na dimensão patrimonial.

A LDA de 1998 estrutura-se a partir dessa dualidade: o artigo 22 separa expressamente os direitos morais (capítulo II) dos direitos patrimoniais (capítulo III). Os morais são perpétuos e inalienáveis; os patrimoniais têm prazo (70 anos *post mortem*) e são livremente cedíveis. O autor é o ponto de convergência dos dois feixes de direitos, e é por isso que a lei exige, na origem, uma pessoa física criadora.

A teoria dualista abre espaço para que, ao menos na dimensão patrimonial, a lei reconheça proteção a obras geradas por IA, ao atribuir os direitos de exploração ao desenvolvedor, ao operador ou ao usuário que investiu no processo criativo, sem exigir que se reconheça à IA direitos morais. É exatamente essa a solução que Luca Schirru propõe em sua obra "Direito Autoral e Inteligência Artificial: autoria e titularidade nos produtos da IA". Ele sugere um regime *sui generis* ao sistema autoral, que proteja patrimonialmente as obras geradas por IA sem romper com o pressuposto de que direitos morais pressupõem a existência de uma pessoa física.

Na doutrina e na jurisprudência brasileira, prevalece a teoria dualista, com a abertura patrimonialista nos direitos econômicos e o olhar personalista nos direitos morais. O Superior Tribunal de Justiça (STJ), nos poucos acórdãos em que enfrentou a questão, tem tratado o direito autoral como direito *sui generis*, recorrendo à lógica patrimonial para questões de cessão, licença, remuneração e à lógica personalíssima para violações de integridade da obra e direito ao crédito da autoria. Não há, contudo, decisão do STJ ou do Supremo Tribunal Federal (STF) que tenha enfrentado diretamente a questão da natureza jurídica do direito autoral em relação à IA.

Independente do entendimento que se adote, fato é que as normas de proteção ao direito autoral aplicam-se a todos os meios em que as obras são dispostas, ou seja, no meio físico e virtual, tal como descrito no artigo 7º, da Lei 9.610/1998. E, ao se garantir aos titulares do direito autoral o exercício dos atributos inerentes à propriedade, ou seja, os relacionados ao uso, gozo e disposição, também se garante um direito oponível *erga omnes*. Contudo, se prevalecer o entendimento de que os atributos da propriedade só se encontram nos bens corpóreos, na medida em que a autoria é imaterial, a proteção do direito autoral melhor se enquadra no âmbito da teoria das pessoas, na parte referente aos direitos da personalidade.

2. IA e o impacto sobre o trabalho criativo. Propriedade intelectual em crise?

Dentro da análise do impacto da IA sobre obras protegidas por direito do autor, o único fato incontroverso é que no mundo contemporâneo tudo muda de forma rápida, o que faz com que produtos, serviços ou formas de gestão de negócios fiquem obsoletos em um curto espaço de tempo. A mudança é constante e profunda. Internet, celulares, redes sociais, computação em nuvem e quântica, e várias outras inovações, vêm sendo importantes na evolução da sociedade. O conhecimento, em todas as suas formas, desempenha papel cada vez maior no progresso econômico. Em um mundo cada vez mais globalizado, a inovação tecnológica assume função de destaque no crescimento das atividades econômicas, já que novas ideias geram inovações com velocidade e com isso aumentam os padrões de concorrência. Em razão disso, diversos têm sido os esforços dos países para compreender o processo de produção e difusão do conhecimento, com o fim de estabelecer políticas públicas adequadas.

Hoje, livros, músicas, vídeos e todas as formas de expressão possuem um novo espaço, muito mais acessível: o virtual. Ocorre que o ambiente digital é um desafio e uma oportunidade para o criador de obras literárias e artísticas, pois, diante da facilidade com que se reproduz ou se comunica ao público, uma obra ultrapassa largamente a capacidade de controle do autor sobre a sua utilização. A questão fundamental reside atualmente em como remunerar de maneira condizente o criador intelectual que tem sua obra veiculada para um público incalculável.

As mesmas indagações feitas atualmente com a disseminação da IA foram feitas quando surgiu a internet. Cada novo avanço tecnológico é acompanhado de complexas questões. Naquela época indagava-se se a internet era

um território livre; se as obras disponíveis na internet estavam sujeitas ao disposto na LDA ou se eram de domínio público; se quem disponibilizava fotos, desenhos, música ou livros eletrônicos na internet renunciava a seus direitos de autor. Todos esses questionamentos estão sendo repensados com a chegada da IA.

A internet é hoje o maior reservatório de informações já conhecido. No entanto, não é uma terra de ninguém ou faroeste, tanto é assim que muitos autores utilizam a expressão "direito cibernético" para falar do direito aplicado e adaptado às novas condições do meio digital. Se a inteligência artificial é mais um meio pelo qual se criam obras, por qual motivo se debate tanto a questão autoral? Se a IA é apenas uma ferramenta utilizada pelo usuário e não possui autonomia suficiente para ser considerada autora, por que essa questão tem sido tão debatida?

A discussão tem como foco a capacidade criativa da máquina e a contribuição dos humanos em cada etapa para determinar a autoria em obras geradas por IA. Os sistemas de IA generativa obedecem a comandos humanos, os *prompts*, e assim podem ser vistos como mera ferramenta de apoio ao criador, ao agilizar o processo criativo, mas sem o substituir. Nesse ponto, há quem defenda que sobre o resultado dos comandos humanos incide a proteção legal do direito autoral. O usuário seria o verdadeiro autor, sob o argumento de que a IA é apenas uma ferramenta e que a força intelectual é do instrutor que dá os comandos certos, independentemente de quem executou fisicamente a obra.

Outra corrente defende a criação de um regime *sui generis*, tal como o dos direitos sobre os bancos de dados ou topografias de circuito integrado, em que o legislador reconheceu que havia valor econômico a ser protegido, mas que o modelo clássico de autoria não se prestava a tal fim. A solução foi criar regimes próprios, desacoplados da exigência de criatividade humana individualizável. Isso porque, se o critério for o investimento substancial, o desenvolvedor da plataforma poderia ser reconhecido como titular de um direito exclusivo sobre os *outputs* do sistema, com prazo limitado e sem os direitos morais que pressupõem pessoa. O regime protegeria o ativo econômico sem fingir que há um autor onde não há.

Nessa hipótese, seria assegurado proteção patrimonial ou direito exclusivo ao programador, à empresa responsável pela IA ou mesmo ao usuário que deu os comandos no sistema, com regras de prioridade definidas em lei, por analogia com as regras de obra por encomenda e obra coletiva da LDA, com prazos menores do que no regime autoral clássico e com a obrigatoriedade de o titular declarar que a obra foi gerada por IA.

A distinção entre os modelos de criação com IA não é meramente descritiva, ela determina quem pode reivindicar autoria, qual o grau de proteção autoral cabível e quem deve responder por eventuais violações de direitos de terceiros. Trata-se, portanto, de uma classificação que traz consequências jurídicas práticas e distintas para cada hipótese.

Nas hipóteses em que a IA atua como mera ferramenta, o humano concebe integralmente a obra, define seu conteúdo, estrutura e utiliza a IA como apoio para executar ou refinar o resultado. A IA não toma decisões criativas, ela apenas obedece, razão pela qual a consequência jurídica aqui é clara, a autoria pertence integralmente ao humano, nos termos do artigo 11 da LDA, e a proteção autoral incide sobre a obra sem qualquer ressalva. A utilização da ferramenta não altera nem fragmenta a titularidade.

O desafio é demonstrar que o humano exerceu controle criativo integral e não apenas aceitou o *output* gerado automaticamente. Essa prova tende a ser necessária quando a obra é contestada, especialmente em litígios sobre plágio ou violação de direitos de terceiros.

Nas hipóteses em que a IA é cocriadora, o humano e o sistema de IA generativa colaboram entre si; o usuário fornece *prompts*, seleciona entre múltiplos *outputs*, edita, impõe seu estilo e refina o resultado em ciclos sucessivos. O produto é uma construção híbrida, em que não é fácil separar a contribuição humana da contribuição da máquina. Esse é o modelo mais comum e o mais juridicamente complexo, pois a proteção autoral incidirá proporcionalmente à contribuição criativa humana identificável no processo. É o que já se extrai do precedente norte-americano de "Zarya of the Dawn", em que se garantiu a proteção ao texto humano e ao arranjo criativo da obra, sem proteção às imagens geradas autonomamente pelo Midjourney.

A indagação é se o papel do usuário que insere comandos é mitigado a ponto de ele não poder ser considerado autor ou, a depender do grau de originalidade, criatividade e controle exercido sobre o processo, por meio de interações sucessivas e edição humana significativa, a autoria estaria justificada. *Prompts* genéricos não configuram contribuição criativa, ou seja, quanto mais gené-

rico e passivo for o *prompt*, mais fraca é a pretensão de autoria do usuário. Se o *prompt* determina que o sistema escreva um poema sobre o inverno e o sistema o cria, não há que se falar em autoria do autor do *prompt*; mas quanto mais iterativa for a intervenção humana, com definições de estilo, estruturação, edição e organização, mais sólida é a base para o reconhecimento de autoria. Quando a IA assume a execução, o que permanece ao humano é a concepção e a curadoria; e a questão é se isso basta para configurar autoria nos termos da lei.

No modelo em que a IA figura como criadora autônoma, o humano se limita a acionar o sistema com instruções genéricas, ou até mesmo sem instrução alguma, e a IA produz a obra de forma autônoma, sem que haja escolha criativa humana identificável no *output*. É o caso dos sistemas que geram milhares de músicas automaticamente para plataformas de *streaming* ou de sistemas que produzem imagens ou textos sem curadoria humana relevante.

Nesse caso, as consequências jurídicas são as mais radicais, haja vista que sob o regime da LDA vigente, a obra simplesmente não tem autor. Não há pessoa física criadora identificada e a lei não reconhece a IA como sujeito de direitos. O resultado prático é que a obra cai automaticamente em domínio público desde sua criação, o que, do ponto de vista dos desenvolvedores das plataformas, representa uma enorme perda de valor econômico sem qualquer previsão de compensação.

É nesse modelo que a tese de Luca Schirru expressa a inadequação das normas atuais, pois o direito autoral clássico foi construído precisamente para proteger a criação humana, e quando a criação humana está ausente, o sistema simplesmente não funciona. Daí a proposta de um regime *sui generis* para esse tipo de produção, em que se reconheça proteção patrimonial ao desenvolvedor ou ao operador do sistema, sem exigir a ficção de que há autoria humana onde ela não existe.

3. O projeto de regulamentação da IA e seus gargalos

O PL 2.338/2023, conhecido como o Marco Legal da Inteligência Artificial no Brasil, é uma das propostas legislativas mais relevantes e debatidas atualmente. O projeto é amplamente inspirado no AI Act da União Europeia e baseia-se em uma abordagem baseada em risco.

O PL 2.338/2023 em si não é um projeto sobre propriedade intelectual. Ele foca mais nos riscos e na transparência. No entanto, o debate sobre IA é indissociável do direito autoral, que se divide em duas grandes questões, que são o treinamento de modelos (*input*) e as obras criadas pela IA (*outputs*).

O PL 2.338/2023, contudo, não entra a fundo no tema da titularidade, mas foca na transparência. O texto aprovado no Senado exige que conteúdos gerados por IA (como áudio, vídeo e texto) sejam claramente rotulados como tal, especialmente *deepfakes*, para evitar desinformação.

Assim sendo, o PL 2.338/2023, em seu texto original, não faz qualquer distinção entre os três modelos de criação de uma obra com sistema de IA e não atribui consequências jurídicas diferentes a cada um deles, no que tange à autoria ou à titularidade das criações. O texto aprovado pelo Senado e atualmente em tramitação na Câmara define, no artigo 4º, inciso IV, a IA generativa como um modelo destinado a gerar ou modificar significativamente, com diferentes graus de autonomia, texto, imagens, áudio, vídeo ou código de software. A referência a diferentes graus de autonomia é importante, mas não soluciona o problema, pois não a desenvolve.

O projeto impõe, no artigo 62, ao desenvolvedor de IA que utilizar conteúdo protegido no desenvolvimento de seus sistemas, o dever de informar quais conteúdos foram utilizados. Isso deve ser feito por meio de publicação de sumário em *site* de fácil acesso. Entretanto, trata-se de obrigação de transparência sobre os *inputs* do treinamento, mas não de uma regulação sobre os *outputs* criativos gerados pelo sistema.

O projeto menciona, nos seus fundamentos (artigo 2º, XVII), a proteção de direitos de autor e conexos, de direitos de propriedade intelectual e de segredo comercial e industrial. No entanto, eleva o tema à condição de valor a ser promovido, sem descer ao nível operacional de definir *como* essa proteção se realiza diante das obras geradas por IA.

O artigo 28, por sua vez, estabelece que os agentes de

inteligência artificial não serão isentos de responsabilidade por danos causados, independentemente do grau de autonomia do sistema. Essa disposição, voltada à responsabilidade civil por dano, é o único dispositivo que tangencia a questão dos graus de autonomia, mas sem vincular esse critério à autoria das obras geradas.

A omissão é significativa e tem consequências práticas imediatas. Ao não diferenciar os modelos de criação, o PL 2.338 deixa sem resposta a questão central da autoria das obras geradas por IA, ao manter o silêncio regulatório que hoje força os juízes a decidir por analogia, com instrumentos inadequados. Além disso, não cria mecanismo algum de remuneração dos criadores humanos, cujas obras foram utilizadas para treinar os modelos, exigindo apenas transparência sobre o que foi usado. Também não enfrenta a questão do domínio público automático das obras geradas, nas hipóteses em que a IA atua como criadora autônoma, o que representa um vácuo de enorme relevância econômica para a indústria criativa e para os desenvolvedores de plataformas de IA. O projeto também não responde se o usuário que emite *prompts* pode ser considerado autor da obra gerada, nem em que condições isso seria possível.

A tramitação na Câmara é a grande oportunidade de o legislador brasileiro enfrentar essas questões antes que a jurisprudência o faça de maneira improvisada. Há necessidade de distinguir expressamente os três modelos de criação, com base no critério do grau de contribuição criativa humana, e estabelecer as consequências jurídicas para cada hipótese; ir além da transparência sobre o treinamento (artigo 62) e regulamentar a questão da autorização e remuneração pelo uso de obras protegidas, mesmo que seja para estabelecer um sistema de licenciamento obrigatório com remuneração equitativa, nos moldes das licenças compulsórias da Lei de Propriedade Industrial. E, por fim, criar um mecanismo de proteção patrimonial para as obras geradas autonomamente pela IA, assegurando que o investimento dos desenvolvedores seja juridicamente amparado, sem recorrer à ficção de autoria humana inexistente.

Na ausência de norma legal específica, abre-se caminho para decisões contraditórias, como em casos de *deepfakes*, manipulação de imagem ou voz gerados por IA, que têm sido solucionadas por meio da tutela legal conferida à imagem, uso indevido de marca ou responsabilidade civil. A maioria dos tribunais tem examinado o papel do ser humano no *output* gerado pela IA, no sentido de negar a autoria ou originalidade em um *prompt*. Não há, portanto, regulação e jurisprudência consolidada no país sobre a titularidade de obras protegidas por IA. No Brasil, enquanto não há norma específica, aplica-se o artigo 11 da LDA por analogia, em que somente haverá autoria humana protegida se o resultado refletir uma criação intelectual individualizada do usuário, e não mera instrução mecânica ao sistema.

Na análise e no debate sobre o estabelecimento de diretrizes claras que reconheçam e protejam a contribuição humana no processo criativo, mesmo quando mediado por tecnologias avançadas, a necessidade de implementação de mecanismos de transparência nos dados utilizados para treinamento de IA, a possibilidade de rastreamento das obras originais e a garantia de remuneração justa para os criadores cujas obras alimentam esses sistemas devem ser o foco.

4. O paradoxo dos *inputs* e *outputs*

A grande controvérsia em torno do treinamento dos sistemas de inteligência artificial generativa não reside na questão de quem é o autor dos resultados produzidos, mas em uma etapa anterior e ainda mais fundamental: a utilização massiva de obras intelectuais protegidas como matéria-prima para o desenvolvimento dos próprios modelos. Trata-se do paradoxo dos *inputs* e *outputs*, haja vista que as plataformas de IA constroem seus sistemas a partir de obras humanas protegidas, frequentemente sem autorização e sem remuneração, e os resultados gerados por esses sistemas concorrem diretamente com os criadores das obras que lhes deram origem.

As plataformas digitais defendem que os direitos autorais devem ficar de fora da regulação da IA, sob o argumento de que sua inclusão inviabilizaria o modelo de negócio do setor. A defesa jurídica das empresas ancora-se na tese de que o treinamento constitui um uso não expressivo e de natureza estritamente tecnológica, insuscetível de configurar reprodução não autorizada nos termos da lei autoral. O raciocínio é o de que a máquina não lê, nem frui a obra como bem cultural, ela extrai padrões estatísticos de grandes volumes de dados. Não há con-

sumo criativo, mas processamento matemático. Por conseguinte, o treinamento não seria uso da obra no sentido que a legislação autoral protege, assim como digitalizar um livro para fins de indexação e busca por palavras não equivale a lê-lo ou reproduzi-lo para fruição.

Nessa linha, as plataformas sustentam que, se o uso não compete com a exploração normal da obra, nem causa prejuízo injustificado aos interesses do autor, tal critério, extraído da Regra dos Três Passos da Convenção de Berna, incorporada ao ordenamento brasileiro, é considerado lícito o uso, ainda que não esteja expressamente previsto no rol taxativo do artigo 46 da Lei nº 9.610/1998. Invocam, ainda, a doutrina norte-americana do *fair use*, que autoriza determinados usos de obras protegidas sem necessidade de autorização prévia. A analogia é a de que, assim como um escritor que lê mil livros, aprende com eles sem violar direito autoral, a IA que processa bilhões de obras estaria apenas aprendendo. A comparação, contudo, é estruturalmente falsa, pois o ser humano que lê não faz cópias digitais de cada obra, não as armazena em servidores de alta capacidade e não as utiliza como insumo para um serviço que compete, em escala industrial, com os próprios autores das obras lidas.

Além do argumento da natureza não expressiva do uso, as empresas de IA sustentam a impossibilidade técnica de mensuração e remuneração retroativa, pois, uma vez concluído o treinamento, os dados são processados, os padrões extraídos e a contribuição individual de cada obra tornam-se irrastreável no resultado. Remunerar os titulares seria, portanto, operacionalmente inviável. A esse argumento técnico sobrepõe-se um argumento de política regulatória, pois o setor privado afirma que a cobrança de direitos autorais, nos termos previstos no PL 2.338/2023, pode inviabilizar o desenvolvimento da IA no Brasil. Representantes das grandes plataformas, presentes nas audiências públicas realizadas na Câmara dos Deputados, foram explícitos ao advertir que os investimentos em treinamento de modelos, abertura de operações e infraestrutura fluirão na direção dos países que ofereçam ambientes regulatórios mais favoráveis. Trata-se do clássico argumento de competitividade, em que, se o Brasil regular com rigor, as empresas migrarão para jurisdições mais permissivas.

Por outro lado, o argumento dos criadores é estruturalmente inverso e igualmente sólido. O uso de conteúdos protegidos por direitos autorais em processos de mineração, treinamento e desenvolvimento de sistemas de IA comercializados enseja remuneração aos seus titulares, não como favor ou concessão, mas como consequência lógica do regime autoral vigente. A suposta inviabilidade técnica da remuneração desfaz-se diante de um dado concreto: o modelo de licenciamento de conteúdo já foi utilizado em centenas de acordos entre empresas de IA, editoras e veículos jornalísticos internacionais. Quando há pressão jurídica ou regulatória, as plataformas negociam e remuneram. A inviabilidade técnica é, portanto, um argumento seletivo, invocado apenas na ausência de obrigação legal.

Há ainda uma dimensão geopolítica que Ronaldo Lemos sustenta em suas obras; se os representantes eleitos não valorizarem a produção de conhecimento gerada no Brasil, não serão empresas estrangeiras que o farão. O Brasil é exportador de conteúdo cultural, jornalismo, música, literatura, audiovisual, que hoje alimenta modelos treinados em servidores norte-americanos sem qualquer retorno aos criadores brasileiros. Ao deixar os direitos autorais fora da regulação da IA, o Brasil não adota uma postura neutra, mas sim uma postura que favorece ativamente as plataformas estrangeiras, em detrimento dos criadores nacionais.

Esse tensionamento encontrou sua expressão judicial mais concreta no Brasil por meio da ação ajuizada pela Folha de São Paulo contra a OpenAI em agosto de 2025. O jornal demonstrou, com base em registros de servidores e repositórios públicos do GitHub mantidos pela própria OpenAI, que seu domínio figurava entre os mil sítios mais utilizados na composição de um dos conjuntos de treinamento dos modelos da empresa, tendo seus servidores registrado, em julho de 2025, mais de 45 mil acessos de robôs de coleta da OpenAI. O pedido mais ousado da ação, a destruição dos modelos treinados com conteúdo do jornal, amparada no artigo 106 da LDA, evidencia a seriedade jurídica da controvérsia e o potencial de impacto global de uma decisão favorável ao autor. O caso é apontado como o primeiro grande teste da Lei de Direitos Autorais brasileira diante da IA generativa, e sua instrução probatória deverá revelar os limites da tese do uso não expressivo no ordenamento pátrio.

O diagnóstico que emerge desse confronto é o de que ambos os lados têm razão em parte. As plataformas têm razão ao alertar que uma regulação excessivamente onerosa pode comprometer o desenvolvimento da IA no Brasil. Os criadores têm razão ao afirmar que foi o trabalho deles que tornou possível a IA generativa como a

conhecemos e que o enriquecimento das plataformas às suas custas, sem qualquer contrapartida, configura apropriação indevida de ativo econômico alheio.

A solução não está em eleger um vencedor, mas em construir um modelo de licenciamento obrigatório, com remuneração equitativa, como já existe em outros setores da indústria criativa, a exemplo da radiodifusão e da execução pública de obras musicais, que permita o uso sem criar ônus proibitivo para a inovação e sem deixar os criadores com as mãos vazias. Esse é o equilíbrio que o legislador brasileiro precisa encontrar e que a Câmara dos Deputados tem, ainda, a oportunidade de construir.

Conclusão

Todos os seres humanos possuem um potencial criativo que pode resultar em bens ou criações passíveis de aproveitamento econômico. Essa premissa elementar sustenta a razão de existir do direito autoral: proteger o criador e assegurar que o fruto de sua expressão intelectual seja por ele controlado e economicamente aproveitado. O uso crescente da inteligência artificial generativa, contudo, tensiona essa premissa em suas bases, ao colocar em xeque a figura do autor humano como pressuposto inafastável da proteção legal.

O presente artigo demonstrou que a questão não é apenas tecnológica, mas estruturalmente jurídica. Os sistemas de IA generativa são capazes de gerar textos, imagens e músicas porque foram treinados com obras humanas protegidas por direito autoral, frequentemente sem autorização e sem remuneração aos criadores originais. Instaura-se, assim, um paradoxo de difícil solução; os autores cujos trabalhos alimentaram o aprendizado da máquina passam a enfrentar a concorrência da própria ferramenta que os consumiu sem nada pagar por isso. Essa contradição é estrutural ao modelo de negócio das grandes plataformas de IA generativa.

A análise empreendida revelou que as consequências jurídicas desse fenômeno variam conforme o modelo de criação adotado. Quando a IA é utilizada como ferramenta pelo criador humano, a autoria permanece integralmente na esfera do usuário, e a proteção autoral incide sem ressalvas, nos termos do artigo 11 da Lei nº 9.610/1998. Quando a IA atua como cocriadora, o produto resultante é uma construção híbrida, cuja proteção será proporcional à densidade da contribuição criativa humana em cada etapa do processo, sendo este o modelo mais frequente e o mais juridicamente complexo da atualidade. E quando a IA opera como criadora autônoma, sem intervenção humana relevante, o sistema autoral vigente simplesmente não oferece resposta, pois se não há autor, a obra cai em domínio público desde sua criação, consequência que nenhum agente do setor aceita como solução definitiva.

A discussão sobre a natureza jurídica do direito autoral mostrou-se decisiva para o equacionamento do problema. A corrente patrimonialista, ao fundar a proteção no investimento econômico, acomoda com maior facilidade a tutela das obras geradas por IA, ao reconhecer o desenvolvedor como titular. A corrente personalista, ao vincular a autoria ao vínculo indissolúvel entre a obra e a personalidade do criador, opõe-se a qualquer proteção onde não haja pessoa. A teoria dualista ou *sui generis*, hoje dominante na doutrina internacional e crescentemente adotada no Brasil, oferece a síntese mais coerente ao separar os direitos morais, intransferíveis e personalíssimos, dos direitos patrimoniais, cessíveis e economicamente exploráveis. Dessa forma, ela abre caminho para que, ao menos na dimensão patrimonial, a lei reconheça proteção a obras geradas por IA, sem exigir a ficção de uma autoria humana inexistente.

É precisamente nessa abertura que repousa a proposta doutrinária de um regime *sui generis* inspirado nos modelos dos bancos de dados e das topografias de circuito integrado. Em ambos os casos, o legislador reconheceu que havia valor econômico a proteger, mas que o modelo clássico de autoria era inadequado para tanto. A solução foi criar regimes próprios, desassociados da exigência de criatividade humana individualizada, mas ancorados no critério do investimento substancial. Transposta para o campo das obras geradas por IA, essa lógica permitiria reconhecer o desenvolvedor da plataforma como titular de um direito exclusivo de natureza patrimonial sobre os *outputs* do sistema, com prazo reduzido de proteção e sem os direitos morais que pressupõem uma pessoa, protegendo o ativo econômico sem recorrer à ficção de uma autoria que não existe.

O Projeto de Lei nº 2.338/2023, aprovado pelo Senado Federal em dezembro de 2024 e em tramitação na Câmara

dos Deputados, representa avanço normativo relevante ao estruturar a regulação da IA a partir da classificação por nível de risco e ao impor obrigações de transparência sobre o uso de obras protegidas no treinamento de modelos. O artigo 62 exige que o desenvolvedor informe quais conteúdos protegidos foram utilizados; o artigo 64 mantém a responsabilidade civil mesmo quando a proibição é posterior ao treinamento; e o artigo 65 impõe o dever de remuneração aos titulares, mediante negociação coletiva ou direta.

Trata-se, porém, de um marco de transparência e responsabilidade civil, não de um marco autoral. O projeto não distingue os três modelos de criação, não atribui consequências jurídicas diferenciadas a cada hipótese, não define quem é o autor ou titular das obras geradas, e não resolve a questão central do uso de obras protegidas para treinamento sem autorização prévia. O único dispositivo que tangencia a questão dos graus de autonomia, o artigo 28, trata da responsabilidade de forma independente do grau de autonomia do sistema e, portanto, não vincula esse critério à autoria das criações.

A tramitação na Câmara dos Deputados é a derradeira oportunidade de o legislador brasileiro enfrentar essas questões antes que o Poder Judiciário o faça de maneira improvisada e casuística. Três medidas se mostram indispensáveis. Primeiro, a distinção expressa dos três modelos de criação, com base no grau de contribuição criativa humana, e a atribuição de consequências jurídicas específicas para cada hipótese. Segundo, a regulação da autorização e remuneração pelo uso de obras protegidas no treinamento de sistemas de IA, ainda que mediante sistema de licenciamento obrigatório, com remuneração equitativa, à semelhança das licenças compulsórias da Lei de Propriedade Industrial. Terceiro, a criação de um mecanismo de proteção patrimonial para obras geradas autonomamente por IA, que ampare juridicamente o investimento dos desenvolvedores sem recorrer à ficção de autoria humana inexistente.

Como bem advertiu Luca Schirru, as normas de direito autoral hoje vigentes são inadequadas para a regulação dos produtos da inteligência artificial. O direito autoral brasileiro foi construído para proteger o autor individual. A IA não cabe nesse molde. Forçá-la a caber, por analogia ou interpretação extensiva, pode ser mais prejudicial do que admitir que o molde precisa ser reformado. Ao legislador, compete agir antes que o vácuo normativo se consolide como norma de fato, favorável às plataformas estrangeiras e prejudicial aos criadores brasileiros, à indústria cultural nacional e à própria razão de existir do direito que se pretende proteger.

A despeito da discussão sobre a autoria em obras criadas em sistemas de IA, cabe atentar para a distinção existente entre ela e titularidade. O autor cria, o titular da obra detém os direitos de exploração econômica, que, no caso das IAs, ainda que a autoria seja atribuída ao humano, a titularidade pode ser objeto de negociação contratual.

Atribuir a titularidade ao desenvolvedor da IA criaria um monopólio sem precedentes sobre a cultura. Por outro lado, deixar tais obras em domínio público poderia desincentivar o investimento na criatividade incentivada pela IA. A solução pode residir na proteção do esforço investido pelo usuário, desde que este comprove uma manipulação substancial do resultado gerado."

Esse trabalho buscou contribuir para o aprimoramento das discussões sobre direito autoral no contexto da inteligência artificial e demonstrou que a IA não pode ser titular de direitos perante o INPI, ao demonstrar que, no presente ordenamento jurídico brasileiro, somente pessoas naturais podem ter autoria ou coautoria de obras protegidas pelo direto autoral e a titularidade de tais obras só pode ser reivindicada por aqueles que detêm personalidade, seja ela civil ou jurídica. Mostrou-se também que no atual formato do ordenamento jurídico brasileiro, a IA é compreendida como bem jurídico, porque consiste em uma ferramenta por meio da qual uma pessoa natural pode disparar um comando para que seja criada uma obra nova.

Embora a pesquisa tenha demonstrado a titularidade das obras e natureza jurídica da IA no Brasil, algumas questões ainda merecem reflexão. Diante da probabilidade do incremento do aprendizado de máquina em um futuro próximo, deveriam legisladores, juristas e profissionais de vários setores refletir sobre um novo enquadramento de natureza jurídica para a IA? Deveria a IA ser considerada como natureza jurídica híbrida, possibilitando que ora fosse bem, ora coautora a depender da obra criada? Seria viável coautoria da IA em um software que ameaça ou lesa direito de terceiros, se ela não pode responder civil, penal e administrativamente? Por ser bem jurídico, teria a IA algum viés de foro íntimo para reivindicar o direito moral ou o direito patrimonial advindos do direito autoral? Poderia a IA ser lesada se tais direitos não lhe forem concedidos? Essas são algumas questões que ainda serão enfrentadas, e muitas outras surgirão com a

evolução da IA. Dessa forma, espera-se que as reflexões apresentadas nesta pesquisa auxiliem na construção de um arcabouço legal mais adequado para proteger os direitos criados a partir da IA.

Para evitar que o Brasil se torne um terreno fértil para a exploração desenfreada de obras geradas por IA, é imperativo que o legislador estabeleça diretrizes claras que reconheçam e protejam a contribuição humana no processo criativo, mesmo quando mediado por tecnologias avançadas. Isso inclui a implementação de mecanismos de transparência nos dados utilizados para treinamento de IA, a possibilidade de rastreamento das obras originais e a garantia de remuneração justa para os criadores cujas obras alimentam esses sistemas.

Referências

BRASIL. *Lei nº 9.610, de 19 de fevereiro de 1998*. Altera, atualiza e consolida a legislação sobre direitos autorais e dá outras providências. Brasília: Presidência da República, 1998. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9610.htm. Acesso em: 5 jul. 2026.

BRASIL. *Projeto de Lei nº 1.473, de 2023*. Obriga empresas de inteligência artificial a disponibilizarem ferramentas para que autores restrinjam o uso de seus conteúdos pelos algoritmos. Brasília: Câmara dos Deputados, 2023. Disponível em: https://www.camara.leg.br/noticias/1115343-comissao-aprova-projeto-que-obriga-empresa-de-inteligencia-artificial-a-oferecer-ferramenta-para-proteger-direito-autoral/. Acesso em: 5 jul. 2026.

BRASIL. *Projeto de Lei nº 2.338, de 2023*. Dispõe sobre o uso da inteligência artificial. Brasília: Senado Federal, 2023. Disponível em: https://www.camara.leg.br/noticias/1115343-comissao-aprova-projeto-que-obriga-empresa-de-inteligencia-artificial-a-oferecer-ferramenta-para-proteger-direito-autoral/. Acesso em: 5 jul. 2026.

IBDAUTORAL. *Inteligência Artificial e Direitos Autorais:* contribuições ao debate regulatório no Brasil. Brasília: Instituto Brasileiro de Direito Autoral, 2024.

LEMOS, Ronaldo. As três forças que regulam a IA. *Folha de S.Paulo*, São Paulo, 23 out. 2023. Disponível em: https://itsrio.org/pt/artigos/as-tres-forcas-que-regulam-a-ia/. Acesso em: 5 jul. 2026.

LEMOS, Ronaldo. Batalha da IA será travada no direito autoral. *Folha de S.Paulo,* São Paulo, 25 jun. 2023. Disponível em: https://itsrio.org/pt/artigos/batalha-da-ia-sera-travada-no-direito-autoral/. Acesso em: 5 jul. 2026.

LEMOS, Ronaldo. Inteligência artificial vai acabar com o direito autoral? *Folha de S.Paulo,* São Paulo, 24 abr. 2023. Disponível em: https://itsrio.org/pt/artigos/inteligencia-artificial-vai-acabar-com-o-direito-autoral/. Acesso em: 5 jul. 2026.

LEMOS, Ronaldo. Qual é a visão do Brasil para a inteligência artificial? *Folha de S.Paulo*, São Paulo, 2024. Disponível em: https://itsrio.org/en/artigos/what-is-brazils-vision-for-artificial-intelligence/. Acesso em: 5 jul. 2026.

MEDEIROS, Erick Felipe. Direitos autorais e inteligência artificial: a quem pertence a obra criada pela máquina? *Consultor Jurídico*, São Paulo, 5 ago. 2024. Disponível em: https://www.conjur.com.br/2024-ago-05/direitos-autorais-e-inteligencia-artificial-a-quem-pertence-a-obra-criada-pela-maquina/. Acesso em: 5 jul. 2026.

SCHIRRU, Luca. *Direito Autoral e Inteligência Artificial:* autoria e titularidade nos produtos de IA. 2020. Tese (Doutorado em Políticas Públicas, Estratégias e Desenvolvimento) — Instituto de Economia, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2020.

Quando tudo parece real:

o desafio da confiança na era da IA

Patrícia Gouvêa

Patrícia Gouvêa é advogada especializada em propriedade intelectual, proteção de dados e governança de inteligência artificial. Bacharel em Direito e pós-graduada em Direito da Propriedade Intelectual pela PUC-Rio, possui LL.M. em Propriedade Intelectual pela George Washington University (EUA) e certificação CIPM (Certified Information Privacy Manager) pela IAPP. Atua há mais de duas décadas em temas relacionados à inovação, tecnologia, privacidade e regulação digital.

Introdução

Distinguir conteúdos autênticos daqueles integralmente produzidos ou substancialmente modificados por Inteligência Artificial (IA), sobretudo a generativa, também denominados conteúdos sintéticos, tornou-se um dos principais desafios contemporâneos. Essa tecnologia já gera textos, imagens, áudios e vídeos hiper-realistas, reproduzindo vozes, características humanas, ambientes e acontecimentos com elevado grau de verossimilhança[1] e tornando menos perceptíveis os rastros da intervenção artificial[2].

A capacidade de produzir representações convincentes põe em xeque o antigo "ver para crer". Embora registros visuais e sonoros sempre tenham admitido manipulação, a IA ampliou a escala de produção, circulação e influência desses conteúdos. Surge, assim, um risco duplo: conteúdos sintéticos podem ser aceitos como autênticos, enquanto registros genuínos podem ser desacreditados como artificiais. Além de favorecer o engano, esse cenário também produz o que Chesney e Citron chamam de *liar's dividend*[3], benefício obtido por quem explora a possibilidade de manipulação audiovisual para negar a autenticidade de registros verdadeiros.

Nesse contexto, destaca-se a relevância de sinalizar conteúdos dessa natureza, prática que consiste em rotular ou aplicar marcações capazes de identificar a sua origem ou alteração significativa por IA. A necessidade e a forma da sinalização devem ser definidas pelo risco concreto de indução do público a erro, e não pelo simples uso da tecnologia.

Também é importante destacar que a transparência proporcionada pela sinalização não sana irregularidades anteriores relacionadas ao uso desses conteúdos nem substitui o respeito a outros direitos, como imagem, voz e propriedade intelectual, tampouco a obtenção de autorizações quando necessárias, embora possa futuramente auxiliar na rastreabilidade dos usos de obras protegidas.

A partir dessa premissa, este artigo examina quatro aspectos. Primeiro, os limites da detecção humana e automatizada. Em seguida, as principais formas pelas quais tais conteúdos podem enganar o público quanto à identidade, à atribuição e ao contexto. Depois, a transparência como mecanismo para evitar percepções equivocadas sobre a autenticidade e a procedência do conteúdo, com critérios para definir quando a sinalização é necessária, como deve ser calibrada e de que modo avisos ao público e marcações legíveis por máquina podem atuar de forma complementar. Por fim, os deveres de informação e transparência já previstos no ordenamento jurídico brasileiro e as perspectivas de sistematização trazidas pelo Projeto de Lei nº 2.338/2023 (PL nº 2.338/2023), principal proposta de marco regulatório da inteligência artificial atualmente em discussão no país.

[1] Estudos destacam que a IA generativa é capaz de produzir conteúdos de alta qualidade, coerentes e semanticamente ricos, cf. "Generative AI for multimodal content: a survey with applications, challenges and future directions". Artificial Intelligence Review, 2026. DOI: 10.1007/s10462-026-11525-6.

[2] AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD). *Deepfakes*. Brasília, DF: ANPD, 2026.

[3] CHESNEY, Robert; CITRON, Danielle Keats. Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. California *Law Review*, [*S. l.*], v. 107, n. 6, p. 1753-1820, 2019. DOI: https://doi.org/10.15779/Z38RV0D15J.

1. Os limites da detecção

Quando empregada para representar fatos, testemunhos ou circunstâncias como reais, a IA pode distorcer a compreensão do público e influenciar suas crenças, percepções e decisões. O risco se agrava porque nem a avaliação humana nem os sistemas automatizados oferecem método universal e infalível para identificar conteúdos gerados ou substancialmente alterados por IA.

No estudo "Fooled Twice: People Cannot Detect Deepfakes but Think They Can"[4], Köbis, Doležalová e Soraperra constataram que os participantes tiveram dificuldade para identificar *deepfakes* e superestimaram sua capacidade de reconhecer manipulações audiovisuais. Assim, se a avaliação humana é prejudicada pela dificuldade de reconhecer manipulações e pela confiança excessiva na própria percepção, a detecção automatizada enfrenta limitações de outra natureza. Como se baseia em probabilidades, está sujeita a falsos positivos e negativos e pode falhar diante de conteúdos produzidos por modelos distintos daqueles usados em seu treinamento. Além disso, a rápida evolução da IA pode tornar os métodos de detecção rapidamente obsoletos[5].

A dificuldade pode ser comparada à distinção entre diamantes naturais e aqueles desenvolvidos em laboratório. Ambos são diamantes e apresentam composição química, estrutura cristalina e aparência praticamente idênticas, de modo que a origem artificial nem sempre pode ser reconhecida a olho nu ou por instrumentos gemológicos convencionais. Em certos casos, a identificação segura exige análise laboratorial especializada, com técnicas como espectroscopia e observação de padrões de crescimento e fluorescência[6]. A resposta do setor não foi aprimorar a inspeção visual, mas criar infraestrutura de proveniência, com laudos de certificação e inscrição a laser do número do relatório na própria pedra. De forma semelhante, quanto mais verossímil o conteúdo gerado por IA, menos confiável se torna a tentativa de reconhecer sua origem apenas pela aparência, o que reforça a importância de informações de procedência e mecanismos de sinalização.

Portanto, depender apenas de análises *a posteriori* é uma estratégia reativa e insuficiente para sustentar um ambiente informacional confiável. Assim como a identificação da origem de um diamante pode exigir dados e técnicas que ultrapassam sua aparência, a identificação de conteúdos gerados ou substancialmente modificados por IA precisa ser apoiada por informações de procedência produzidas e preservadas ao longo de seu ciclo de circulação.

2. Três formas de engano do público

Como visto, o risco de engano não decorre do simples uso de IA, mas da possibilidade de a intervenção tecnológica alterar a compreensão do público sobre elementos relevantes do conteúdo. A avaliação desse risco deve considerar, de forma conjunta, o realismo da representação, a extensão da modificação, o contexto de circulação, a expectativa de autenticidade e as possíveis consequências do erro. Para orientar essa análise, este artigo examina três possíveis formas de engano: quanto à identidade, à atribuição e ao contexto.

Essa avaliação também delimita o que se entende por modificação substancial. Não basta que a IA tenha participado da cadeia de produção. A modificação é substancial quando altera elemento capaz de influenciar o juízo do destinatário sobre quem participa do conteúdo, sobre o que lhe é atribuído ou sobre a natureza do registro apresentado. Ajustes de qualidade, cor, ruído, legendagem ou acessibilidade, que não afetam esses elementos, por exemplo, não se enquadram nessa categoria.

No **engano quanto à identidade**, o público acredita estar diante de uma pessoa real, embora a figura apresentada tenha sido integralmente criada por IA. A verossimilhança de sua aparência, voz e comportamento pode ocultar sua origem artificial. O risco aumenta quando essa pessoa reivindica formação, experiência ou autoridade em determinado assunto, levando o público a confiar não apenas em alguém que não existe, mas também em credenciais e reputação igualmente inexistentes.

Essa dimensão aproxima-se do conceito de *sockpuppeting*, utilizado por Marchal e outros[7] para designar personas sintéticas apresentadas como sujeitos reais.

Imagine-se, por exemplo, uma pessoa criada integralmente por IA que, em uma rede social, apareça de jaleco e estetoscópio, em ambiente clínico, apresentando-se como médica e oferecendo orientações de saúde e bem-estar. A combinação entre aparência humana verossímil e sinais visuais de autoridade pode levar o público a acreditar que está diante de uma profissional real e habilitada, embora tanto sua identidade quanto suas credenciais sejam artificiais.

No **engano quanto à atribuição**, não há dúvida sobre a existência da pessoa retratada, mas sobre o que ela efetivamente disse, fez ou produziu. A intervenção tecnológica cria ou modifica falas, condutas, características ou atuações de modo a associá-los falsamente a uma pessoa real, podendo alterar a percepção do público sobre suas ideias, decisões ou participação no conteúdo. Robert Chesney e Danielle Keats Citron descrevem esse fenômeno como a representação de "pessoas reais dizendo e fazendo coisas que nunca disseram ou fizeram" (tradução livre)[8].

Considere-se, por exemplo, um vídeo em que uma pessoa pública ou celebridade aparenta recomendar um produto que nunca utilizou ou defender uma posição contrária às convicções que manifesta publicamente, com reprodução convincente de sua imagem e voz. Nesse cenário, a figura da pessoa retratada corresponde a um indivíduo real, mas a conduta, a declaração e o endosso que lhe são atribuídos são inteiramente artificiais.

No engano quanto ao contexto, o público interpreta de forma equivocada a natureza do material e sua relação com a realidade. Isso ocorre quando uma reconstrução, simulação ou dramatização é apresentada, ou pode ser razoavelmente percebida, como registro factual de um acontecimento real. O conteúdo representado pode até corresponder a fatos verdadeiros, mas sua apresentação leva os interlocutores a acreditar que estão diante de um registro produzido no momento ou no local do evento.

Nesse cenário, atribui-se inadvertidamente valor documental a uma representação artificial[9]. Ao examinar o uso de IA e conteúdos sintéticos em documentários, Maher[10] destaca que reencenações e reconstruções de arquivos podem introduzir realidades simuladas em narrativas comprometidas com a representação do real.

Tome-se, por exemplo, uma sequência de imagens geradas por IA que reproduza com realismo um incêndio em determinado edifício e circule nas redes sociais como se tivesse sido registrada no local durante o acontecimento. Ainda que o incidente tenha realmente ocorrido, as imagens não documentam o evento. O engano reside na falsa aparência de registro documental e no valor probatório que o público pode atribuir ao material.

As três formas de engano podem ocorrer isoladamente ou de maneira combinada. Um mesmo conteúdo, gerado ou substancialmente modificado por IA, pode apresentar uma pessoa inexistente como real, atribuir a alguém uma manifestação que nunca ocorreu ou conferir a uma simulação a aparência de registro autêntico. Esses riscos não dependem necessariamente da falsidade da mensagem. Afinal, uma figura criada por IA pode transmitir uma informação correta e, ainda assim, induzir o público a erro sobre sua identidade, da mesma forma que um fato real pode ser ilustrado por imagens sintéticas apresentadas como registros factuais do acontecimento. O que importa, portanto, é identificar se a forma de apresentação distorce a compreensão do público sobre a identidade representada, a atribuição de uma manifestação ou o contexto documental do conteúdo.

[7] MARCHAL, Nahema; XU, Rachel; ELASMAR, Rasmi; GABRIEL, Iason; GOLDBERG, Beth; ISAAC, William. Generative AI Misuse: A Taxonomy of Tactics and Insights from Real-World Data. *arXiv*, [*S. l.*], 2024. DOI: https://doi.org/10.48550/arXiv.2406.13843.

[8] CHESNEY; CITRON, 2019, p. 1753.

[9] WILSON, Dawn M. Against Imprinting: The Photographic Image as a Source of Evidence. Social Research: *An International Quarterly*, [*S. l.*], v. 89, n. 4, p. 947-969, 2022. DOI: https://doi.org/10.1353/sor.2022.0061. A autora observa que registros fotográficos exercem função probatória porque são percebidos como vestígios causalmente conectados aos eventos que retratam.

[10] MAHER, Sean. AI and Deepfakes in Contemporary Documentary: Negotiating a New Real. *In*: INTERNATIONAL CONFERENCE ON COMMUNICATION AND MEDIA STUDIES, 10., 2025, Paris. *Anais* […]. Paris: Common Ground Research Networks, 2026.

3. Transparência: quando exigir e como calibrar a sinalização

Identificadas as principais formas de engano, cabe examinar como a transparência pode contribuir para mitigá-las. Nesse exame, ela constitui um importante instrumento para reduzir a assimetria informacional sobre a origem e as alterações do conteúdo, pois fornece elementos que não podem ser inferidos apenas por sua aparência. Ao esclarecer a existência da intervenção tecnológica na produção ou modificação do conteúdo, a transparência permite avaliar com maior segurança a origem, a autenticidade e a confiabilidade da informação. A sinalização não torna o conteúdo verdadeiro, mas evita que sua forma de apresentação crie uma expectativa equivocada de autenticidade.

Essa transparência pode ocorrer em duas camadas complementares. A primeira compreende avisos perceptíveis, como rótulos, ícones padronizados, legendas ou créditos inseridos no conteúdo, que comunicam diretamente ao público destinatário que o material foi gerado ou substancialmente modificado por IA. A segunda consiste em marcações legíveis por máquina, que registram dados sobre a procedência e as alterações do conteúdo e permitem sua verificação por plataformas, autoridades e sistemas automatizados. A distinção entre elas encontra respaldo direto no artigo 50 do Regulamento (UE) 2024/1689, conhecido como Regulamento Europeu de Inteligência Artificial (AI Act)[11], e estrutura semelhante é proposta no Brasil pelo PL nº 2.338/2023, cuja disciplina será examinada adiante.

Um exemplo é o padrão C2PA (Coalition for Content Provenance and Authenticity), que incorpora ao arquivo credenciais protegidas criptograficamente sobre sua origem e alterações, permitindo a verificação automatizada da proveniência e da integridade de seu histórico. A eficácia desse padrão, contudo, depende de sua adoção interoperável e coordenada ao longo de toda a cadeia de circulação do conteúdo, com a cooperação entre produtores, desenvolvedores, dispositivos, editores e plataformas digitais para preservar, reconhecer e exibir as informações de procedência. Essa cadeia também ajuda a situar o dever de sinalizar. Em regra, quem produz o conteúdo responde pela marcação na origem; quem o publica ou divulga, pela informação apresentada ao público; e as plataformas, pela preservação e exibição dos metadados e rótulos recebidos.

Compreendidas essas duas camadas, é preciso definir quando a transparência deve ser exigida. A sinalização é necessária se a natureza sintética do conteúdo puder induzir o público a erro quanto à identidade, à atribuição ou ao contexto, sobretudo quando a intervenção alterar a percepção sobre quem participa do conteúdo, o que lhe é atribuído ou seu caráter documental. Essa avaliação deve considerar o gênero, a finalidade e o contexto de circulação, a função desempenhada pela IA, a expectativa de autenticidade e os possíveis danos.

Conteúdos jornalísticos, documentais, eleitorais ou de orientação especializada tendem a exigir maior transparência, enquanto obras evidentemente ficcionais, satíricas ou de entretenimento e ajustes meramente técnicos ou assistenciais podem admitir soluções menos intrusivas, desde que não haja risco relevante de confusão. Essa calibragem preserva a liberdade de expressão criativa ao evitar exigências desproporcionais em contextos que não criem expectativa relevante de autenticidade.

Uma vez reconhecida essa necessidade, a forma, o momento e o destaque da sinalização devem ser proporcionais ao risco. Quanto maiores o realismo, a aparência de autoridade e o potencial de dano, mais claros, imediatos e persistentes devem ser os avisos, que podem ser

[11] UNIÃO EUROPEIA. Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024, que estabelece regras harmonizadas em matéria de inteligência artificial (Regulamento da Inteligência Artificial). Jornal Oficial da União Europeia, 12 jul. 2024. Disponível em: https://eur-lex.europa.eu/eli/reg/2024/1689/oj.

combinados com marcações legíveis por máquina. Em situações de menor risco, créditos ou outras soluções discretas podem ser suficientes. A calibragem também deve considerar limites práticos, pois o excesso de alertas pode gerar fadiga e reduzir sua eficácia, enquanto agentes mal-intencionados podem omitir deliberadamente a sinalização[12].

4. Fundamentos jurídicos e perspectivas regulatórias no Brasil

Definidos os critérios para exigir e calibrar a sinalização, cabe examinar como eles se projetam no ordenamento brasileiro. Embora o país ainda não disponha de uma lei geral sobre a sinalização de conteúdos sintéticos, já existem fundamentos jurídicos para a transparência.

Deveres já previstos nas relações de consumo, na publicidade, no tratamento de dados pessoais e no processo eleitoral oferecem fundamentos distintos, mas convergentes, para informar o público quando a intervenção da IA puder afetar sua compreensão ou suas decisões. O PL nº 2.338/2023 procura sistematizar essa proteção ao incluir a identificação de conteúdos sintéticos entre as normas gerais de governança responsável da IA. A análise dessas normas, contudo, exige distinguir a força jurídica e o alcance de cada uma delas, pois, embora convirjam no objetivo de proteger a percepção do público, pertencem a diferentes âmbitos normativos, que abrangem regras vinculantes e específicas, propostas legislativas e diretrizes de autorregulação.

Nas relações de consumo, o Código de Defesa do Consumidor (Lei nº 8.078/1990 — CDC)[13] assegura informação adequada e clara sobre os produtos e serviços oferecidos e veda a publicidade enganosa tanto por ação quanto por omissão. Se a natureza sintética for relevante para compreender a mensagem ou formar o juízo do destinatário, ocultá-la pode suprimir informação essencial e comprometer a autonomia de escolha do consumidor.

Essa preocupação com o engano no mercado de consumo ganha contornos práticos no campo da autorregulação publicitária. Conselho Nacional Autorregulamentação Publicitária (CONAR), no "Guia de Marketing e Publicidade por Influenciadores Digitais"[14], já prevê a identificação do uso de IA em conteúdos comerciais. Essa orientação submete influenciadores humanos e virtuais aos mesmos princípios éticos de transparência, exigindo que a natureza simulada da mensagem seja evidente para o público.

Se na publicidade comercial a clareza protege o mercado, na esfera eleitoral, a Resolução TSE nº 23.610/2019, com as alterações introduzidas pela Resolução TSE nº 23.732/2024[15], aplicável à propaganda e ao ambiente de campanha, estabelece regras estritas de sinalização para conteúdos fabricados ou manipulados por tecnologias digitais, inclusive IA, limitando usos capazes de afetar a integridade do processo eleitoral. A identificação deve ser explícita, destacada e acessível quando a propaganda utilizar conteúdo sintético multimídia criado ou significativamente alterado por IA.

Além disso, quando a geração, a personalização ou a distribuição desses conteúdos envolver tratamento de dados pessoais, a Lei Geral de Proteção de Dados Pes-

[12] WITTENBERG, Chloe; EPSTEIN, Ziv; PÉLOQUIN-SKULSKI, Gabrielle; BERINSKY, Adam J.; RAND, David G. Labeling AI-generated media online. *PNAS Nexus*, [*S. l.*], v. 4, n. 6, pgaf170, 2025. DOI: https://doi.org/10.1093/pnasnexus/pgaf170. Em dois experimentos pré-registrados, os autores verificaram que todos os rótulos testados reduziram significativamente a crença nas alegações apresentadas, embora a simples indicação de que o conteúdo foi gerado por IA tenha produzido efeito limitado sobre a intenção declarada de interação.

[13] BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Código de Defesa do Consumidor. Arts. 6º, III; 31; e 37, §§ 1º e 3º.

[14] CONSELHO NACIONAL DE AUTORREGULAMENTAÇÃO PUBLICITÁRIA (CONAR). Guia de Marketing e Publicidade por Influenciadores Digitais. Atualização de 2026. Disponível em: https://www.conar.org.br/noticias/guia-de-marketing-e-publicidade-por-influenciadores-digitais.

[15] BRASIL. Tribunal Superior Eleitoral. *Resolução nº 23.610, de 18 de dezembro de 2019*. Dispõe sobre propaganda eleitoral, utilização e geração do horário gratuito e condutas ilícitas em campanha eleitoral. Brasília, DF: TSE, 2019. Alterada pela Resolução nº 23.732, de 27 de fevereiro de 2024. Disponível em: https://www.tse.jus.br/legislacao/compilada/res/2019/resolucao-no-23-610-de-18-de-dezembro-de-2019. Acesso em: 26 out. 2026.

soais (Lei nº 13.709/2018 — LGPD)[16] pode oferecer fundamento adicional para a transparência sobre esse tratamento. Esse dever não se confunde com a sinalização geral de todo conteúdo produzido por IA e depende da incidência da LGPD no caso concreto, da natureza do tratamento realizado e das informações necessárias ao exercício dos direitos do titular.

Diante desse cenário de regras setoriais e esparsas, ganha relevância a tentativa de sistematização proposta pelo artigo 19 do PL nº 2.338/2023, ainda em tramitação no Congresso Nacional. O dispositivo prevê que conteúdos sintéticos sejam identificados por mecanismos capazes de permitir a verificação de sua autenticidade, proveniência, modificações ou transmissão, considerados o estado da arte e o contexto de uso. Em linha com a estrutura anteriormente examinada no artigo 50 do AI Act, a regra traduz, no plano legislativo brasileiro, duas camadas complementares de transparência: a identificação técnica, voltada à rastreabilidade, deve conviver com os avisos dirigidos ao público. Ao mesmo tempo, o projeto estimula padrões interoperáveis e admite soluções menos intrusivas, como créditos ou metadados, para obras artísticas, culturais e de entretenimento quando não houver risco relevante de indução a erro. O AI Act adota solução convergente ao prever regime atenuado para conteúdo evidentemente artístico, criativo ou satírico.

Sob essa perspectiva, o PL nº 2.338/2023 procura articular, em uma disciplina geral de governança de IA, mecanismos de transparência que hoje se encontram esparsos em nosso ordenamento. Como ainda está em tramitação, suas disposições não se confundem com as obrigações legais e regulatórias já exigíveis. Sua principal contribuição reside em consolidar de forma sistêmica a identificação técnica, o dever de informar e a flexibilidade contextual sob uma abordagem estritamente proporcional ao risco.

Conclusão

Em uma era em que a IA desafia a premissa de que podemos simplesmente acreditar no que vemos ou ouvimos, a aparência realista do conteúdo já não basta para sustentar a confiança no ambiente digital. Como demonstrado, a crescente verossimilhança desses materiais e os limites da percepção humana e da detecção automatizada tornam insuficientes as estratégias meramente reativas de identificação de manipulações que podem enganar o público.

Este artigo propõe uma abordagem de transparência calibrada. As categorias de engano quanto à identidade, à atribuição e ao contexto oferecem um critério analítico e não exaustivo para identificar situações em que a intervenção da IA pode distorcer a compreensão do destinatário. A necessidade de sinalização deve ser orientada por esse risco concreto, e não pelo mero uso da tecnologia.

Embora os deveres de informação e clareza estejam previstos de forma esparsa no ordenamento jurídico brasileiro, eles oferecem fundamentos sólidos para exigir a sinalização quando a ausência de aviso puder induzir o público a erro. Nesse contexto, o PL nº 2.338/2023 não constitui um ponto de partida, mas um avanço na organização e sistematização desses deveres no âmbito de uma governança de IA mais ampla e coerente, que articule a rastreabilidade técnica com a informação clara ao público.

Em última análise, o desafio está em promover a inovação tecnológica e preservar a liberdade de expressão e a liberdade criativa, assegurando, ao mesmo tempo, proteção contra o engano por meio de uma transparência proporcional ao risco e adequada ao contexto. Quando houver possibilidade relevante de confusão, avisos perceptíveis devem informar diretamente o público, enquanto marcações legíveis por máquina podem apoiar a verificação da procedência e das alterações do conteúdo. Em contextos evidentemente criativos ou ficcionais, soluções menos intrusivas podem ser suficientes. A confiança no ambiente digital passa, assim, a não mais se apoiar apenas na aparência estética ou na impressão de realismo, mas em informações que permitam compreender a natureza, a origem e o histórico do conteúdo.

[16] BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial da União: Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 18 jul. 2026.

Inteligência Artificial:

transparência, explicabilidade e
opacidade algorítmica

Diogo Luís Manganelli de Oliveira

Diogo Luís Manganelli de Oliveira, doutorando em Direito Civil pela Universidade do Estado do Rio de Janeiro (UERJ), graduado e mestre em Direito e Inovação pela Universidade Federal de Juiz de Fora (UFJF), Data Protection Officer na Lenovo Tecnologia, fellow da IAPP e certificado em CIPP-E, CIPM e CDPO/BR, DPO certificado ECPC-B pela Maastricht University, colunista da FenalawLab, autor, palestrante e instrutor de cursos e treinamentos, pesquisador no Legal Fronts Institute.

Introdução

O tratamento de dados pessoais não é novidade na sociedade tecnológica, mas a forma pela qual vêm sendo utilizados em larga escala como insumo econômico potencializou os riscos oriundos da sua manipulação em um nível jamais visto, especialmente pelo fato de que as relações humanas, tanto profissionais, quanto pessoais estão cada vez mais integradas ao "ecossistema digital"[1]. Trata-se do que Manuel Castells denominou como sociedade em rede[2].

Entre as inúmeras formas de tecnologias mais comumente utilizadas, para fins da presente análise, destacam-se aquelas que possuem, como ponto de partida, a utilização de Inteligência Artificial (IA) como seu cerne. Para Andriei Gutierrez[3], o que é atualmente denominado como IA, na verdade, seria composto de diferentes tipos de tecnologias, abarcando desde algoritmos de análise de dados ou *analytics*, até sistemas que se desenvolvem de maneira parcial ou integralmente autônoma por meio de *machine learning* ou até mesmo *deep learning*[4]. Intuitivamente, este tipo de algoritmo é capaz de aprender a partir de experiências, positivas e negativas, incluindo generalizações criadas por padrões estatísticos adotados[5].

Eduardo Tomasevicius[6], por sua vez, traz a definição de Elaine Rich, na década de 1980, de que inteligência artificial pode ser definida como a capacidade de fazer com que os computadores realizem tarefas nas quais, atualmente, os seres humanos ainda são melhores e capazes. Trata-se de uma série de rotinas lógicas que, quando aplicadas aos computadores, lhes permitem dispensar a necessidade de supervisão humana para a tomada de decisão e interpretação de mensagens analógicas.

Embora o conceito de IA não seja necessariamente novo, remontando à década de 1950, após um longo hiato, tal forma de tecnologia vivencia hoje o seu apogeu de desenvolvimento[7].

A retomada do entusiasmo com relação ao desenvolvimento de IA, portanto, está diretamente relacionada com quatro fatores: (i) existência de métodos estatísticos e probabilísticos mais sofisticados; (ii) aumento exponencial do número de dados disponíveis; (iii) a acessibilidade a um poder computacional a baixo custo; e (iv) a cons-

[1] ZANATTA, Rafael; VALENTE, Jonas; MENDONÇA, Júlia. Entre o abusivo e o excessivo: novos contornos jurídicos para o tratamento de dados pessoais de crianças e adolescentes na LGPD. *In*: LATERÇA, Priscilla Silva; FERNANDES, Elora; TEFFÉ, Chiara Spadaccini de; BRANCO, Sérgio (coord.). *Privacidade e proteção de dados de crianças e adolescentes*. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio de Janeiro; Obliq, 2021. p. 396-426. E-book. Disponível em: https://itsrio.org/wp-content/uploads/2021/10/Privacidade-e-Protecao-de-Dados-de-Crian%C3%A7as-e-Adolescentes-ITS.pdf. Acesso em: 25 out. 2026.

[2] CASTELLS, Manuel. *A Sociedade em Rede*: A Era da Informação: economia, sociedade e cultura. Volume 1. Tradução de Roneide Venancio Majer. 8. ed. São Paulo: Paz e Terra, 2005.

[3] GUTIERREZ, Andriei. É possível confiar em um sistema de Inteligência Artificial? Práticas em torno da melhoria da sua confiança, segurança e evidências de accountability. *In*: FRAZÃO, Ana; MULHOLLAND, Caitlin (coord.). *Inteligência artificial e direito*: ética, regulação e responsabilidade. 2. ed. rev., atual. e ampl. São Paulo: Thomson Reuters Brasil, 2020. p. 81-94.

[4] De uma maneira bem simples, podemos classificar os sistemas de *machine* em dois subgrupos. Aqueles que são supervisionados dos não supervisionados. O aprendizado de máquina supervisionado é aquele no qual os critérios de correlação inicial são parametrizados ou ensinados pelos seres humanos. Já os não supervisionados conseguem dispensar essa calibragem inicial por seres humanos, o que acontece por meio do desenvolvimento de novas tecnologias, como as redes neurais ou o *deep learning*, que são capazes de criar padrões de correlações próprios, alheios ao raciocínio humano (Gutierrez, 2020).

[5] BOSTROM, Nick. *Superinteligência*: Caminhos, perigos e estratégias para um novo mundo. Rio de Janeiro. DarkSide, 2014.

[6] TOMASEVICIUS FILHO, Eduardo. Inteligência artificial e direitos da personalidade: uma contradição em termos? *Revista da Faculdade de Direito* da Universidade de São Paulo, [S. l.], v. 113, p. 133-149, 2018. DOI: https://doi.org/10.11606/issn.2318-8235.v113i0p133-149.

[7] GUTIERREZ, *op. cit.*, p. 81-94.

tante adequação de ambientes às novas tecnologias[8]. Em especial, para o presente trabalho, destaca-se que a disponibilidade massiva de dados é um catalisador para tecnologias de IA, principalmente aquelas utilizadas em criações impactadas pelos direitos de propriedade intelectual.

Utilizada para as mais diversas finalidades, as aplicações da IA, contudo, necessitam de maior atenção. Em razão do seu ainda não totalmente compreendido modo de tomada de decisão, especialmente naqueles formatos de tecnologia em que há *deep learning*, como também diante do seu potencial impacto discriminatório aos cidadãos ante as decisões automatizadas, além de violações a direitos de propriedade intelectual e autoral por técnicas de *scraping* e outras raspagem de dados[9], fato é que a IA tem despertado a atenção de toda a sociedade global.

Tal qual os benefícios trazidos pelas aplicações baseadas em IA serão cruciais para o desenvolvimento da sociedade humana nas próximas décadas, suas implicações também serão severas, afetando os direitos fundamentais e a democracia. Embora os algoritmos, a princípio, sejam imparciais, na sua construção são treinados a partir de dados já existentes. Logo, traduzem as informações inseridas como realidade, havendo o risco de reproduzirem aspectos indesejados de injustiça e discriminação de nossa sociedade em suas decisões[10].

Nesse cotejo, Frank Pasquale menciona umas das principais questões que norteiam e norteará as futuras compreensões sobre regulação e tomada de decisões no contexto de soluções de IA, especialmente na seara do conhecimento, ou no que chamou de "*knowledge problem*". Basicamente, define que a sociedade se encontra em uma era na qual o conhecimento sobre os mecanismos que impactam suas vidas é desconhecido, embora seus efeitos sejam visíveis. Aqui, conglomerados empresariais tecnológicos, financeiros e inúmeros outros setores, deliberadamente ou não, escondem seus métodos de ação do restante da sociedade de maneira proposital, seguindo a lógica já consagrada do "conhecimento é poder". Processo esse previsto e defendido pelo modelo normativo nacional, como se compreende do art. 20, §1°, da Lei n° 13.709 – Lei Geral de Proteção de Dados (LGPD) que condiciona o direito a revisão das decisões automatizadas à barreira do segredo comercial e industrial[11].

Petitgrand e Regis[12] destacam que, nesse contexto, os desafios de se traduzir os princípios éticos para as normas reguladoras relacionadas às aplicações da IA são evidentes após a compreensão do seu potencial de ampliação das injustiças existentes, o que se dá pela falta de transparência acerca do funcionamento de seus algoritmos, além de sua distribuição global, motivo pelo qual a compreensão da maneira pela qual a sua tomada de decisão ocorre torna-se fundamental.

[8] CATH, Corinne; WACHTER, Sandra; MITTELSTADT, Brent; TADDEO, Mariarosaria; FLORIDI, Luciano. Artificial Intelligence and the 'Good Society': the US, EU, and UK approach. *Science and Engineering Ethics*, [*S. l.*], v. 24, n. 2, p. 505-528, 2018. DOI: https://doi.org/10.1007/s11948-017-9901-7.

[9] Conhecida como *data scraping* ou "raspagem de dados", a técnica consiste na extração de forma automatizada de dados pessoais em páginas da internet e em bases de dados públicos com o objetivo de reutilização de tais dados para outras finalidades (LEAL, 2021).

[10] MORLEY, Jessica; FLORIDI, Luciano. The Limits of Empowerment: How to Reframe the Role of mHealth Tools in the Healthcare Ecosystem. *Science and Engineering Ethics*, [*S. l.*], v. 26, n. 3, p. 1159-1183, 2020. DOI: https://doi.org/10.1007/s11948-019-00115-1.

[11] BRASIL. Lei n. 13.709/2018. Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade. § 1° O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial.

[12] PETITGRAND, Cécile; RÉGIS, Catherine. Principes éthiques et encadrement juridique de l'intelligence artificielle en santé: exemple de la Déclaration de Montréal pour un développement responsable de l'intelligence artificielle. *Journal de Droit de la Santé et de l'Assurance Maladie,* [*S. l.*], n. 22, p. 101-105, 2019. DOI: https://doi.org/10.3917/jdsam.191.0101.

Diante do atual cenário de incertezas relacionadas aos potenciais impactos negativos produzidos ou reforçados pela IA, Ugo Pagallo[13] pondera que tais atribuições às máquinas podem lhes conferir a "autonomia" necessária para que, eventualmente, tenham a capacidade de agir de maneira diversa daquela inicialmente planejada, gerando discussões relativas às suas implicações éticas.

Nesse sentido, destaca-se inicialmente a Conferência de Asilomar, em 2017, que definiu uma série de 23 princípios para o desenvolvimento benéfico de tecnologias de IA[14]. Igualmente, a Declaração de Montreal para o Desenvolvimento Responsável da Inteligência Artificial[15] definiu, em 2018, uma série de 10 princípios para a sua aplicação ética e em sintonia com os princípios fundamentais dos indivíduos. Por sua vez, a Organização para Cooperação e Desenvolvimento Econômico (OCDE) também publicou, em 2019, orientações referentes a aspectos a serem observados para o desenvolvimento ético e responsável dos sistemas de IA[16].

Na mesma esteira também caminhou a Organização das Nações Unidas (ONU), que, em 2021, teceu um acordo internacional em mais 193 nações referente a princípios éticos para o desenvolvimento de tecnologias fundamentadas na aplicação de técnicas de IA[17]. Especificamente na Europa, a Comissão Europeia publicou a sua proposta de regulamentação da IA aplicando conceitos como "subsidiariedade" e "proporcionalidade" das intervenções estatais nas atividades privadas. Já o Parlamento Europeu publicou estudo no qual ressaltou dilemas éticos e morais do uso de IA, inclusive sobre a perspectiva de vieses[18].

Como visto, o uso de tecnologias de IA pode produzir consequências parciais ou totalmente imprevisíveis, de modo que a única solução disponível seja desativar o próprio sistema[19]. Da mesma forma, também podem tomar decisões baseadas em critérios enviesados que reforçam aspectos tradicionalmente discriminatórios. Entre tais vieses, Friedman e Nissenbaum[20] definem que podem surgir: (a) de valores sociais já existentes, intrínsecos às próprias instituições sociais contemporâneas; (b) restrições técnicas no desenvolvimento da tecnologia; e (c) novos aspectos em um cenário de utilização.

Importante esclarecer que vieses constituem uma dimensão específica do processo de tomada de decisão. Já a discriminação está presente nos efeitos dessa decisão, decorrente de um prejuízo ou dano desproporcional gerado a partir da conclusão algorítmica. Logo, decisões enviesadas têm o potencial de gerar efeitos discriminatórios negativos[21].

[13] PAGALLO, Ugo. *The Law of Robots:* Crimes, Contracts and Torts. Berlim: Springer Science & Business Media, 2013. Disponível em: https://link.springer.com/content/pdf/bfm%3A978-94-007-6564-1%2F1.pdf. Acesso em: 13 maio 2026.

[14] Disponível em: https://futureoflife.org/bai-2017/. Acesso em: 11 maio 2026.

[15] Disponível em: https://www.sbmac.org.br/wp-content/uploads/2021/02/Português-UdeM_Decl-IA-Resp_LA-Declaration_vf.pdf. Acesso em 11 maio 2026.

[16] Princípios estabelecidos pela OCDE para sistemas de IA confiáveis e seguros: 1) inclusão, bem-estar e crescimento sustentável; 2) valores e justiça antropocêntricos; 3) transparência e explicabilidade; 4) segurança e robustez; e 5) prestação de contas (*accountability*). Disponível em: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449. Acesso em: 11 maio 2026.

[17] Disponível em: https://brasil.un.org/pt-br/160484-193-paises-adotam-o-primeiro-acordo-global-sobre-etica-da-inteligencia-artificial. Acesso em: 11 maio 2026.

[18] UNIÃO EUROPEIA. Parlamento Europeu. *The ethics of artificial intelligence*: issues and initiatives. Bruxelas: Parlamento Europeu, 2020. DOI: https://doi.org/10.2861/6644. Disponível em: https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2020)634452. Acesso em: 12 jun. 2024.

[19] MAGRANI, Eduardo; SILVA, Priscila; VIOLA, Rafael. Novas perspectivas sobre ética e responsabilidade de inteligência artificial. *In:* FRAZÃO, Ana; MULHOLLAND, Caitlin (coord.). *Inteligência artificial e direito*: ética, regulação e responsabilidade. 2. ed. rev., atual. e ampl. São Paulo: Thomson Reuters Brasil, 2020. p. 111-141.

[20] FRIEDMAN, Batya; NISSENBAUM, Helen. Bias in computer systems. *ACM Transactions on Information Systems*, New York, v. 14, n. 3, p. 330-347, 1996. DOI: https://doi.org/10.1145/230538.230561.

[21] MITTELSTADT, Brent Daniel; ALLO, Patrick; TADDEO, Mariarosaria; WACHTER, Sandra; FLORIDI, Luciano. The ethics of algorithms: mapping the debate. *Big Data & Society*, [*S. l.*], v. 3, n. 2, p. 1-21, 2016. DOI: https://doi.org/10.1177/2053951716679679. Acesso em: 13 maio 2026.

Nesse cotejo, urge-se a discussão e ampliação do debate acerca das possíveis consequências da utilização de tecnologias de inteligência artificial, em especial sob o prisma da responsabilidade, transparência e explicabilidade. Assim, o presente trabalho debruça-se sobre a maneira pela qual as informações sobre o modelo de funcionamento da IA e seus impactos podem ser compartilhadas com a sociedade, em especial como titulares de dados e reguladores, de modo a viabilizar o exercício dos direitos aplicáveis e a salvaguarda dos valores constitucionais.

1. Estado da arte e regulamentações em IA

Embora seus impactos ainda não sejam totalmente compreendidos, a IA já se encontra inevitável e exponencialmente presente nas relações sociais, potencializada tanto pela demasiada oferta de dados pessoais quanto pelos avanços tecnológicos. Nesse sentido, a compreensão da IA, juntamente com as legislações de proteção de dados pessoais, é crucial para a manutenção da proteção dos direitos fundamentais dos indivíduos, em especial autodeterminação informativa e até mesmo personalidade.

Especialmente em relação ao Brasil, embora hoje o país conte com a LGPD[22], o que a princípio poderia ensejar a garantia dos direitos e das liberdades dos indivíduos com relação ao tratamento de seus dados pessoais por tecnologias que utilizam decisões automatizadas como seu principal cerne, ainda existe um longo e complexo caminho a ser criado do ponto de vista da regulamentação e do *enforcement*.

Seja pela promulgação e vigência da LGPD, da criação da Agência Nacional de Proteção de Dados (ANPD) ou também pela incipiente compreensão da população brasileira acerca de conceitos como privacidade, proteção de dados pessoais, inteligência artificial e, principalmente, transparência, há desafios para o pleno exercício do fundamento da "autodeterminação informativa"[23].

Especificamente com relação à IA, embora tanto o Regulamento Geral de Proteção de Dados (RGPD) europeu quanto a LGPD já possuam meios de combate à potencial discriminação efetuada em virtude da tomada de decisões automatizadas, tais previsões ainda carecem de aplicações práticas mais incisivas. Enquanto no RGPD há a vedação de um titular ser objeto de decisão automatizada caso manifeste sua vontade, como visto, o artigo 20 da LGPD proporciona ao titular a possibilidade de solicitar a revisão da decisão. Para Ana Frazão[24], tal direito representaria uma espécie de devido processo legal para a salvaguarda dos indivíduos com relação ao que chama de a "tirania dos julgamentos automatizados". Assim, a autora propõe ao controlador o ônus da prova sobre a legitimidade da atividade baseada em tratamento automatizado.

Porém, no ordenamento brasileiro não há definição de que a revisão deva ser necessariamente realizada por um ser humano, o que gera incertezas[25]. Igualmente preocupante é a previsão inserida no parágrafo primeiro do

[22] BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 13 maio 2026.

[23] A autodeterminação informativa é, inclusive, um dos fundamentos da disciplina da proteção de dados de acordo com a LGPD. Concebido como um direito fundamental, na esteira do direito geral de personalidade, o direito à autodeterminação informativa proporciona ao individuo o controle sobre suas informações (DONEDA, 2019, p. 169).

[24] MULHOLLAND, Caitlin Sampaio; FRAJHOF, Isabella Zalcberg. Inteligência Artificial e a Lei Geral de Proteção de Dados Pessoais: breves anotações sobre o direito à explicação perante a tomada de decisões por meio de machine learning. *In*: FRAZÃO, Ana; MULHOLLAND, Caitlin (coord.). *Inteligência artificial e direito*: ética, regulação e responsabilidade. 2. ed. rev., atual. e ampl. São Paulo: Thomson Reuters Brasil, 2020. p. 267-289.

mesmo dispositivo, que condiciona o fornecimento dos critérios aplicadas ao segredo comercial e industrial. Tal proteção poderá afastar os critérios de transparência que são caros para a compreensão acerca do funcionamento de tais tecnologias e, portanto, reforçar práticas discriminatórias.

Como explica Frazão[26], a legitimidade das decisões está intrinsecamente relacionada com a existência de meios de controle para assegurar autonomia da pessoa, ausência de viés discriminatório, bem como erros técnicos que vão de encontro aos interesses do titular. Seja pela impossibilidade de compreensão dos complexos processos de *machine learning, deep learning*, seja pelo segredo industrial, o comprometimento da transparência e explicabilidade desses sistemas certamente afeta a confiabilidade da IA.

A necessidade de conhecimento sobre os *inputs* de dados junto aos algoritmos, bem como sobre a metodologia empregada, é crucial para o desenvolvimento e a aplicação de tais ferramentas, ainda que protegidas pelo sigilo comercial. O mesmo vale para os critérios de treinamento do modelo, incluindo questões importantes como qualidade e higienização da base de dados utilizada[27].

Por isso, Caitlin Mulholland e Isabella Z. Frajhof[28] reafirmam que a possibilidade de afetação dos resultados das decisões oriundas dessas tecnologias tem intensificado os debates sobre sua transparência e *accountability*, especialmente naqueles algoritmos em que não é possível averiguar seus processos internos para a tomada de decisão.

Ainda sobre autonomia, a ausência de meios para se compreender os modos e critérios levados em consideração para a tomada de decisões pode conduzir à "ditadura dos algoritmos"[29]. A ausência de clareza dos critérios adotados aproxima-se da metáfora da *black box* apontada por Pasquale[30], que intensifica a assimetria informacional e, consequentemente, prejudica o exercício da autonomia.

Destacam-se as discussões referentes ao desenvolvimento de um marco regulatório para o desenvolvimento de IA no Brasil, entre as quais se faz referência à Comissão de Juristas (CJSUBIA) que, reiteradamente, tem aprofundado os debates junto ao Senado Federal sobre a aplicação de tais tecnologias, vinculadas ao Projeto de Lei nº 21/2020.[31] [32]

Cabe esclarecer que critérios de transparência relacionados à manifestação de autonomia do indivíduo devem

[25] Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade. [...] § 1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial. (BRASIL, 2018).

[26] FRAZÃO, Ana. Apresentação da obra. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord.). *Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro*. São Paulo: Revista dos Tribunais, 2019.

[27] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*: elementos da formação da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

[28] MULHOLLAND; FRAJHOF, 2020, p. 267-289.

[29] RODOTÀ, Stefano. *Il mondo nella rete*: quali i diritti, quali i vincoli. Roma; Bari: Laterza, 2014. Disponível em: https://www.laterza.it/scheda-libro/?isbn=9788858111659. Acesso em: 14 maio 2026.

[30] PASQUALE, 2015.

[31] Disponível em: https://www12.senado.leg.br/noticias/materias/2022/05/16/comissao-de-juristas-da-inteligencia-artificial-faz-balanco-de-audiencias-publicas. Acesso em: 12 jun. 2024.

[32] BRASIL. Câmara dos Deputados. *Projeto de Lei nº 21, de 2020*. Estabelece fundamentos, princípios e diretrizes para o desenvolvimento e a aplicação da inteligência artificial no Brasil; e dá outras providências. Autoria: Deputado Federal Eduardo Bismarck (PDT/CE). Apresentação: 4 fev. 2020. Brasília, DF: Câmara dos Deputados, 2020. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2236340. Acesso em: 13 maio 2026.

estar diretamente relacionados à autodeterminação informativa, preceito basilar insculpido no artigo 3° da LGPD[33]. Isso significa que, também nas aplicações de IA e na demonstração dos critérios de tomada de decisão, devem ser considerados aspectos de privacidade e proteção de dados pessoais do titular[34].

É certo que os progressos tecnológicos têm um significativo impacto na construção do direito à privacidade[35], que desde 1988 encontra-se insculpido no texto da Constituição Federal[36].

Como esclarece Pietro Perlingieri[37], o direito deve promover mudanças na sociedade, não podendo sucumbir aos fatos e estar apenas vinculado a aspectos econômico-sociais,, mas também deve ser constituidor da realidade na qual se vislumbra. Nesse sentido, Stefano Rodotà[38] relembra que a tecnologia salvou o direito civil assim como a ética salvou a filosofia, no sentido de que as inovações tecnológicas demandam novas exigências de regulação ao serem introduzidas, desafiando o tecido social. Todavia, lembra que nem tudo que é tecnicamente possível será, consequentemente, desejável, ético ou necessário.

Cabe ressaltar, nesse ínterim, que o direito à proteção de dados pessoais foi elevado a status de direito fundamental por meio da promulgação e vigência da Emenda Constitucional n° 115[39], o que reforça a necessidade de que haja a adaptação necessária do direito privado de modo a acomodar suas determinações nas relações sociais.

Pode-se dizer que a LGPD tenha dado passos fundamentais para o amadurecimento e a garantia dos direitos fundamentais dos cidadãos com relação à utilização dos seus dados pessoais, especialmente no que diz respeito ao direito à revisão de decisões automatizadas em aplicações de IA. Todavia, por si só, a legislação não será capaz de delimitar todos os aspectos necessários para a regulação do tema e da garantia, inclusive, do seu próprio fundamento da autodeterminação informativa e do princípio da não discriminação, especialmente no contexto da propriedade intelectual, que tensiona o debate ético até suas últimas esferas[40].

Igualmente, também se vislumbra que o Projeto de Lei n° 21/2020[41], que visa estabelecer definições para as aplicações de IA no Brasil (Marco da Inteligência Artificial), embora esteja sendo construído ao exemplo da abordagem de risco trazida pelo seu par europeu, também terá substanciais dificuldades na efetivação de valores como transparência à sociedade.

[33] BRASIL. Lei n. 13.709/2018. Art. 2° A disciplina da proteção de dados pessoais tem como fundamentos: II - a autodeterminação informativa.

[34] MULHOLLAND, Caitlin. O direito de não saber como decorrência do direito à intimidade. *Civilistica.com*, Rio de Janeiro, ano 1, n. 1, 2012. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/27. Acesso em: 13 maio 2026.

[35] KONDER, Carlos Nelson. Privacidade e corpo: convergências possíveis. *Pensar* - Revista de Ciências Jurídicas, [S. l.], v. 18, n. 2, p. 354-400, out. 2013. DOI: https://doi.org/10.5020/23172150.2012.354-400.

[36] BRASIL. [Constituição (1988)]. *Constituição da República Federativa do Brasil de 1988*. Brasília, DF: Presidência da República, [2026]. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 10 maio 2026.

[37] PERLINGIERI, Pietro. Normas constitucionais nas relações privadas. *Civilistica.com*, Rio de Janeiro, ano 8, n. 1, p. 1-9, 2019. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/407. Acesso em: 13 maio 2026.

[38] RODOTÀ, Stefano. Entrevista à RTDC. *Revista Trimestral de Direito Civil,* Rio de Janeiro, v. 3, n. 11, p. 225-308, jul./set. 2002. Entrevista concedida a Danilo Doneda. Disponível em: https://doneda.net/portfolio/entrevista-com-stefano-rodota/. Acesso em: 13 maio 2026.

[39] BRASIL. *Emenda Constitucional n° 115, de 10 de fevereiro de 2022*. Altera a Constituição Federal para incluir proteção de dados pessoais entre os direitos fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Brasília, DF: Presidência da República, 2022. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em 15 mai. 2026.

[40] Art. 6° As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: [...] IX. não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; (BRASIL, 20218).

[41] BRASIL. Câmara dos Deputados. *Projeto de Lei n° 21, de 2020*. Estabelece fundamentos, princípios e diretrizes para o desenvolvimento e a aplicação da inteligência artificial no Brasil; e dá outras providências. Brasília, DF: Câmara dos Deputados, 2020. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2236340. Acesso em: 13 maio 2026.

Gustavo Tepedino[42] acrescenta que a personalidade humana deve ser encarada como o valor máximo do ordenamento e, portanto, é capaz de sujeitar novas atividades tecnológicas ou econômicas ao seu crivo, exatamente como se vislumbra na presente pesquisa. As soluções de IA não devem sujeitar a sociedade ao tratamento massivo de dados pessoais protegidos por direitos de propriedade intelectual e direitos de autor apenas em nome do advento da tecnologia, devendo esse tratamento ser precedido de amplas considerações referentes aos seus impactos e extensões. O mesmo também deve prevalecer para a criação de bancos de dados unificados de tais tipos de informação, que são um catalisador do desenvolvimento da IA a partir de obras passíveis de debate sobre registro em tema de propriedade intelectual valendo-se de obras já devidamente protegidas.

Igualmente, também é necessária a compreensão de se, diante do tratamento de dados pessoais por meio de ferramentas de probabilidade algorítmica e modelos de aprendizado de máquina para tomada de decisão, controladores não estariam negando a fruição do direito fundamental à proteção de dados pessoais. Portanto, definições relacionadas ao dever do controlador de disponibilizar informações aos titulares sobre a tomada de decisão do algoritmo influrienciarão não apenas a compreensão do titular, mas também o exercício de seu direito fundamental[43].

2. Transparência, explicabilidade e opacidade algorítmica

As reflexões ora propostas serão necessárias no sentido de que, conforme destaca Pietro Perlingieri[44], o respeito à Constituição não se resume apenas à observância de procedimentos infraconstitucionais, mas ao atendimento aos valores presentes no próprio ordenamento. Em especial, destaca-se a dignidade da pessoa humana.

O desenvolvimento de princípios éticos como um fio condutor necessário do progresso da IA, fundamental para que a tecnologia alcance o bem comum, contudo, não afasta seus desafios. Isso porque não é exato o grau de utilização adequado da IA na sociedade, sendo possível que a sua aplicação excessiva represente riscos aos indivíduos envolvidos pelas próprias características de opacidade da IA. Por outro lado, a sua subutilização também pode trazer consequências negativas, arrefecendo avanços e possivelmente benefícios decorrentes da sua aplicação[45]. Para isso, a IA deve caminhar paralelamente aos direitos fundamentais.

A proteção de dados e os demais direitos, como os direitos de propriedade intelectual, devem ser entendidos e traduzidos com expressões de liberdade e dignidade dos indivíduos, não tolerando a utilização de informações para que sejam reduzidos a meros objetos de vigilância constante por meio da violação de seus direitos. Caso seja essa a conclusão a ser obtida a partir da utilização em larga escala da IA, isso seria incompatível com a própria natureza da proteção de dados enquanto direito fundamental[46].

[42] TEPEDINO, Gustavo. A tutela da personalidade no ordenamento civil-constitucional brasileiro. *In*: TEPEDINO, Gustavo. *Temas de Direito Civil*. 3. ed. Rio de Janeiro: Renovar, 2004. p. 23-58.

[43] MULHOLLAND; FRAJHOF, 2020.

[44] PERLINGIERI, Pietro. *Perfis do direito civil*. Tradução de: Maria Cristina de Cicco. 3. ed., rev. e ampl. – Rio de Janeiro: Renovar, 2022.

[45] FLORIDI, Luciano; COWLS, Josh; BELTRAMETTI, Monica; CHATILA, Raja; CHAZERAND, Patrice; DIGNUM, Virginia; LUETGE, Christoph; MADELIN, Robert; PAGALLO, Ugo; ROSSI, Francesca; SCHAFER, Burkhard; VALCKE, Peggy; VAYENA, Effy. AI4People: an ethical framework for a good AI society: opportunities, risks, principles, and recommendations. Minds and *Machines*, [*S. l.*], v. 28, n. 4, p. 689-707, 2018. DOI: 10.1007/s11023-018-9482-5.

[46] RODOTÀ, 2002.

Sobre as dificuldades de definições de tais valores com relação ao que, até o presente momento, já foi desenvolvido nacional e internacionalmente, um ponto crucial é o fato de não serem construções naturais, mas sim impostas de maneira *top-down* com pretensão de universalidade. Isso faz com que tenham conteúdo genérico e abstrato, distanciando-se dos desafios práticos enfrentados. Se a construção de normas principiológicas favorece o próprio desenvolvimento tecnológico, também pode contribuir negativamente para a figura da regulação em IA denominada como *ethics-washign*[47]. Nesse ínterim, um dos principais desafios dessa construção seria não apenas definir os princípios adequados ao tema da regulação da IA, mas também o momento em que devem ser implementados[48].

Inserida no viés das construções éticas de soluções de IA, mas também já abarcada pelas legislações e regulamentações mencionadas sobre privacidade e proteção de dados pessoais, urge o aprofundamento do debate sobre a opacidade algorítmica outrora mencionada que, por sua vez, rege a construção de novas tecnologias baseadas em IA. Para Pasquale[49], a destruição das *boxes* de *Big Data* não é uma tarefa simples, ainda que os seus métodos para a tomada de decisão fossem voluntariamente expostos de maneira pública. Isso porque trata-se de algoritmos compostos de fórmulas extremamente complexas, em várias camadas de tomada de decisão diversas (redes neurais), sendo necessário um alto nível de conhecimento na seara técnica tecnológica, de engenharia e ciências afins para compreendê-los. Como se não bastasse, a figura de direito privado do privilégio ao segredo comercial e industrial, inclusive mencionada na própria LGPD, é um impeditivo a mais para que sejam efetivamente disponibilizados.

Para a manutenção da referida opacidade, Pasquale[50] afirma que existem três estratégias centrais para que seja mantida alheia ao conhecimento público: a primeira diz respeito ao chamado "segredo real", ou seja, a existência de uma barreira entre conteúdos escondidos de maneira proposital e o acesso controlado a eles. Pode ser exemplificada pela ação cotidiana de se inserir *login* e senha para o controle de acesso a endereços de *e-mail* particulares. Já a segunda camada seria chamada de "segredo legal", que está relacionada com a existência de obrigações legais voltadas à manutenção de sigilo sobre determinadas informações, especificamente neste caso sobre a forma de funcionamento e/ou como se dá a tomada de decisões pelos algoritmos. Finalmente, a terceira estratégia é denominada "ofuscação", envolvendo situações em que há tentativas deliberadas de redução de danos quando a privacidade é comprometida. Nesse contexto, Frank Pasquale[51] salienta que tais estratégias produzem como resultado a opacidade, termo que o autor caracteriza como referente a uma "incompreensibilidade remediável".

Ainda de acordo com o autor[52], uma das grandes questões da opacidade algorítmica está relacionada ao que foi denominado por ele como *one-way mirror*. Basicamente, enquanto os grandes conglomerados empresariais possuem vastas bases de dados sobre os seus usuários, os conhecendo nos mínimos detalhes e utilizando essas informações para otimizar seus resultados; estes, por sua vez, possuem pouco ou nenhum conhecimento sobre como seus dados são utilizados e para quais finalidades, inclusive nas suas eventuais relações com o poder público.

Logo, não apenas organizações privadas e grandes conglomerados empresariais estão de posse de uma vasta extensão de dados pessoais para suas finalidades comerciais, como também o próprio Estado, cada vez mais,

[47] Em termos de regulação de IA, *Ethics-washing* representaria a adoção de princípios vagos com uma substituição para regras que tratariam maior proteção aos direitos e liberdades individuais e coletivas dos indivíduos (Maranhão; Florêncio; Almada, 2021).

[48] MARANHÃO, Juliano Souza de Albuquerque; FLORÊNCIO, Juliana Abrusio; ALMADA, Marco. Inteligência artificial aplicada ao direito e o direito da inteligência artificial. Suprema: Revista de Estudos Constitucionais, Brasília, v. 1, n. 1, p. 154-180, jan./jun. 2021. DOI: 10.53798/suprema.2021.v1.n1.a20.

[49] PASQUALE, Frank. The Black Box Society: The Secret Algorithms That Control Money and Information. Cambridge: Harvard University Press, 2015.

[50] PASQUALE, 2025, p. 6.

[51] PASQUALE, 2015, p. 7.

[52] PASQUALE, 2025, p. 7.

tem utilizados tais informações para atividades de vigilância e inteligência, inclusive com a formação de perfis prévios dos cidadãos[53].

Cathy O'Neil[54] pontua que o grande problema da opacidade algorítmica é justamente a falta de compreensão, por parte dos indivíduos afetados, acerca do funcionamento das tecnologias tomadoras de decisão, tornando impossível que se manifestem de maneira objetiva em oposição aos resultados externalizados.

Nos Estados Unidos, um caso que ficou mundialmente conhecido se deu em razão da utilização, por parte de seu sistema judiciário estadual, do software Correctional Offender Management Profiling for Alternative Sanctions (COMPAS). Basicamente, a partir da utilização do algoritmo contido na solução tecnológica, era possível prever o índice de reincidência que determinado indivíduo teria em três categorias (baixo, médio e alto). Com isso, decisões sobre aspectos criminais relativos à fiança e até mesmo sentenças poderiam ser afetadas pelo seu resultado sem que, para tanto, houvesse qualquer compreensão acerca dos critérios utilizados pela solução para efetivar tais resultados, principalmente no que se refere ao próprio acusado. Na prática, o que se percebe são critérios financeiros e étnicos tendo pesos importantes nas pontuações atribuídas, revelando aspectos potencialmente racistas em sua construção[55].

Sobre a utilização em larga escala da IA também no Brasil, seja na esfera pública ou privada, que sujeita os seus cidadãos aos resultados de decisões tomadas em contextos de parcial ou absoluta opacidade, é crucial compreender o papel que a LGPD terá na garantia dos direitos dos titulares em relação às tecnologias de IA embarcadas, em especial sob o viés do direito de revisão das decisões automatizadas estabelecido no artigo 20, diretamente relacionado ao princípio da não discriminação[56].

Stefano Rodotà determina, nesse contexto, que o direito à proteção dos dados pessoais, ora positivado na Constituição, está diretamente relacionado com a proteção da personalidade do indivíduo e não de sua propriedade. Dessa maneira, certas categorias de dados pessoais não devem ser utilizadas para fins negociais e, também, para repressão estatal[57].

Retomando o previsto não apenas pela LGPD, mas também o que está inserido na atual proposta de regulamentação de IA em desenvolvimento no país, nos moldes do que também acontece no contexto europeu com o AI ACT, a transparência torna-se peça fundamental para que haja, por parte dos titulares submetidos a decisões automatizadas inseridas no contexto de tecnologias de IA, a mínima compreensão sobre os critérios levados em consideração. Trata-se, na realidade, da expansão do conceito da "autodeterminação informativa".

O combate à discriminação ilícita produzida no contexto das decisões provenientes de sistemas de IA, ou discriminação algorítmica, afigura-se essencial para a prevalência e ênfase na transparência. Sobre a discriminação possivelmente produzida por meio da IA, Acemoglu salienta que esse é um dos principais riscos derivados de tal tecnologia. Ao fazê-lo, pode a IA levar à promoção e permanência de características indesejadas da própria sociedade, identificadas por meio das bases de dados nas quais a tecnologia foi treinada. Sobre os vieses, Requião e Costa salientam que as discriminações podem ocorrer basicamente de duas formas: (i) quando os algoritmos refletem os preconceitos humanos de maneira proposital,

[53] PASQUALE, 2015, p. 7.

[54] O'NEIL, Cathy. *Weapons of math destruction*: how big data increases inequality and threatens democracy. New York: Crown Publishers, 2016.

[55] SYMON, Maybin. Sistema de Algoritmo que determina pena de condenados cria polêmica nos Estados Unidos. *BBC Brasil*, 31 de outubro de 2016. Disponível em: https://www.bbc.com/portuguese/brasil-37677421. Acesso: em 22 maio 2026.

[56] MULHOLLAND; FRAJHOF, 2020, p. 267-289.

[57] RODOTÀ, 2002.

ou seja, são desenvolvidos desta maneira; ou (ii) quando entram em contato com bases de dados contaminadas por vieses específicos, muitas vezes invisíveis aos olhos dos programadores, em sua fase de treinamento.

Por isso, Acemoglu[58] traz a noção da inclusão do princípio da precaução em complementação à própria transparência, ou seja, fazendo com que os agentes de tratamento não apenas sejam capazes de explicar adequadamente quais os critérios levados em consideração para a tomada de uma determinada decisão pela IA, mas que também reflitam e sejam responsáveis pelas reflexões acerca das consequências potencialmente geradas a partir de suas construções[59].

Diante desse cenário, é importante que medidas sejam aplicadas para mitigar os potenciais efeitos nocivos que podem ser originados pelas tecnologias de IA aos indivíduos. Especialmente em relação à opacidade algorítmica ora tratada, uma das principais ferramentas que certamente pode ser útil para essa questão é a velha e conhecida figura da transparência.

Prevista no ordenamento jurídico brasileiro, a transparência sempre foi utilizada como instrumento reitor do direito naquelas situações em que há severa discrepância entre as partes envolvidas, exatamente o caso das relações de consumo. Para isso, o Código de Defesa do Consumidor (CDC)[60] já prevê, como direito básico dos consumidores, informações adequadas e claras sobre os produtos e serviços adquiridos[61]. A LGPD também trouxe em seu rol de princípios a consagração do princípio da transparência ao determinar que os agentes de tratamento devam fornecer informações claras, precisas e facilmente acessíveis sobre as atividades de tratamento de dados pessoais que sejam realizadas[62]. Igualmente, em consagração ao fundamento da autodeterminação informativa, estabelece como direito dos titulares a possibilidade de requerer, junto ao controlador, o acesso a todas as suas informações[63].

E por que a transparência é tão necessária para a mitigação de riscos oriundos de tais tecnologias? Para responder a tal questionamento, antes devem ser analisadas duas facetas desse instituto. O primeiro objetivo da transparência seria justamente o de dar ciência ao indivíduo que interage diretamente com a IA, de modo a ajustar as suas expectativas. Já o segundo está relacionado à forma de tomada de decisão utilizada pela IA e às consequências que podem ser produzidas em relação aos efeitos gerados ao indivíduo submetido aos seus resultados. Nesse ínterim, a transparência se caracteriza como um contraposto à produção de impactos negativos na vida dos indivíduos, oriundos de algoritmos

[58] FRAZÃO, Ana. Discriminação algorítmica: algumas conclusões. *JOTA*, [*S. l.*], 22 set. 2021. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/discriminacao-algoritmica-como-lidar-com-as-incertezas-22092021. Acesso em: 22 maio 2026.

[59] *These considerations then suggest a "precautionary regulatory principle" – ex ante regulation slowing down the use of IA technologies, especially in domains where redressing the costs of AI become politically and socially more difficult after large0scale implementation. AI technologies impacting political discourse and democratic politics may be prime candidates for the application of such a precautionary regulatory principle* (Acemoglu ***apud*** Frazão, 2021, p. 6).

[60] BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências.

[61] Art. 6º São direitos básicos do consumidor: [...]

III - a informação adequada e clara sobre os diferentes produtos e serviços, com especificação correta de quantidade, características, composição, qualidade, tributos incidentes e preço, bem como sobre os riscos que apresentem. (Brasil, 1990).

[62] Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: [...]

VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial; (Brasil, 2018).

[63] Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:

I - confirmação da existência de tratamento;

II - acesso aos dados; [...] (Brasil, 2018).

opacos, devolvendo, portanto, ao titular, a possibilidade de compreender os critérios utilizados para as tomadas de decisão[64]. Trata-se, na bem da realidade, do exercício da autonomia da vontade do indivíduo para garantia de seus valores fundamentais.

Para Maranhão[65], um desdobramento ético da transparência residiria na confiança gerada pelo sistema de IA em relação à sua interação com humanos. Isso quer dizer que, ao se delegar indiscriminadamente aspectos da vida cotidiana à IA sem a devida compreensão clara acerca dos efeitos de suas decisões, delega-se ao mesmo tempo a construção ética e moral da sociedade, o que deve ser acompanhado de uma compreensão profunda sobre os critérios embarcados e utilizados por essas tecnologias.

Conforme já demonstrado, a LGPD tratou o tema da transparência em alguns dispositivos. Todavia, para efeitos do presente trabalho, a sua principal previsão está positivada no § 1º do artigo 20, que determina que os agentes de tratamento, ao se valerem de decisões automatizadas, quando solicitados, devem disponibilizar aos titulares informações sobre os critérios utilizados para a obtenção do resultado, respeitado o segredo comercial e industrial[66].

Embora críticas possam ser feitas em relação à limitação do dispositivo em prol da figura do segredo comercial e industrial, fato é que a transparência, por si só, dada a complexidade dos sistemas de IA, especialmente aqueles desenvolvidos em formato de *machine learning* ou *deep learning*, não se demonstra capaz de trazer o equilíbrio à relação existente entre as partes. Isso porque os titulares, em sua grande maioria, ainda que disponham dos algoritmos utilizados para a tomada de decisão que diz respeito a si, não terão capacidade técnica e/ou conhecimento para identificar potenciais vieses, falhas etc. Logo, a opacidade dos sistemas de IA e o seu alto nível técnico fazem com que a transparência, nesse contexto, seja na realidade consagrada em uma explicação. Explicação essa que, pautada por aspectos éticos, deve ser traduzida em linguagem simples e acessível, destinada à população leiga[67].

Na realidade, para a utilização de algoritmos, a transparência pura e simples não é muito mais eficaz do que a própria opacidade, uma vez que tudo o que não é compreensível continua, aos olhos de seu interlocutor, sendo obscuro[68]. Todavia, isso por si só não é novidade, já que na seara tecnológica os aspectos técnicos sempre foram ocultos da maioria de seus usuários. O ineditismo, agora, encontra-se nos efeitos que tal opacidade gera nos direitos dos indivíduos.

No contexto europeu, Medon[69] menciona o considerando número 71 do RGPD que traz referência ao termo da explicação em complementação à própria transparência. Lá, a explicação serviria para minorar o problema da falta de conhecimento dos indivíduos sobre o tratamento e também acerca das decisões automatizadas, com os eventuais danos sofridos.

Diante dos desafios na explicação das decisões geradas por soluções de IA sobre seus critérios, ganha força a fi-

---

[64] MARANHÃO; FLORÊNCIO; ALMADA, 2021, p. 138-139.

[65] MARANHÃO; FLORÊNCIO; ALMADA, 2021, p. 138-139.

[66] Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade § 1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial. (BRASIL, 2018).

[67] MARANHÃO; FLORÊNCIO; ALMADA, 2021, p. 140-141.

[68] PASQUALE, 2015.

[69] MEDON, Filipe. *Inteligência Artificial e Responsabilidade Civil*: Autonomia, Riscos e Solidariedade. Salvador: JusPodivm, 2020.

gura *explainable AI* ou frequentemente mencionada como *XAI* por meio da propositura de procedimentos padronizados para a tradução dos modelos de autoaprendizagem. Embora os resultados obtidos até o momento sejam positivos, um desafio ainda resiste especialmente em relação aos algoritmos de aprendizado profundo: embora tenham desenvolvido e construído as redes deste tipo de tecnologia e as treinado sob determinados critérios e bases de dados, na grande maioria das oportunidades as relações são tão complexas na evolução da IA que as organizações sequer são capazes de conhecer e esmiuçar os padrões desenvolvidos para o resultado. Dessa forma, duas possibilidades surgem: (i) a explicação seria relacionada ao próprio desconhecimento, o que não atende aos usuários afetados; ou (ii) a IA deve ser desenvolvida de modo a ser capaz de traduzir os seus aspectos ao conhecimento humano, o que a limitaria. Ou seja, o entrave da evolução das tecnologias de aprendizado profundo está mais relacionado à dificuldade humana de compreender os procedimentos realizados do que, propriamente, a ausência de vontade na disponibilização das informações sobre ele[70].

Para Elena Esposito[71], o objetivo da *XAI* não é a transparência *per se*, mas sim a explicação, sendo estes conceitos diversos. Assim, a sua função não seria a de revelar os procedimentos das máquinas, mas sim fazer com que elas próprias forneçam explicações que sejam realmente informativas aos seus usuários, inclusive levando-se em consideração as diferenças entre os próprios interlocutores em relação aos seus contextos sociais, econômicos, etários, culturais, linguísticos etc.

Maranhão[72] salienta que a maior parte do ferramental de explicação desenvolvido até então tem como objetivo principal o fornecimento de informações ao usuário sobre os critérios pelos quais determinada decisão foi tomada, o que é diferente de tentar simplesmente convencê-lo de que a decisão foi correta. O ponto principal, portanto, é que a compreensão do processo e dos critérios para a tomada de decisão gere maior confiança na IA e possa permitir a correção de falhas e vieses.

Uma das técnicas empregadas para trabalhar a figura da explicação é a da sensibilidade. Busca-se, por meio dela, a resposta ao seguinte questionamento: a decisão deste modelo é mais sensível a quais itens? Logo, a lista dos itens respondidos, por si só, funciona como uma "explicação" disponibilizada. Duas outras técnicas possivelmente empregadas para a explicação também podem ser identificadas. A primeira é constituída a partir de uma estratégia decomposicional, ou seja, procura focar-se em um tipo de modelo e decompô-lo. Assim, a explicação seria gerada a partir de um modelo particular em relação à sua estrutura. Como exemplo, cita-se que a decisão de uma rede profunda pode ser explicada neste método com a descrição de quais neurônios e quais interações levaram uma rede a determinado resultado. Já a segunda técnica é constituída por uma estratégia agnóstica, partindo exatamente do princípio oposto: o interpretador não deve examinar o interior do modelo explicado, mas sim compreender a sua entrada, representada pelos dados, e a sua saída, composta das decisões. Nesse caso, como interpretador tem-se um modelo de IA mais "simples" do que o primeiro, ou seja, sendo ele próprio um modelo interpretável, sendo esta a explicação *per se*. Nesse contexto, merece atenção a diferenciação entre explicações locais e globais. Enquanto as primeiras são focadas em decisões particulares relativas a determinados indivíduos, as segundas tentam capturar o comportamento de todo o modelo explicado, sendo úteis

[70] ESPOSITO, Elena. *Artificial communication*: how algorithms produce social intelligence. MIT Press, 2022. Disponível em: https://direct.mit.edu/books/book/5338/Artificial-CommunicationHow-Algorithms-Produce. Acesso em: 27 maio 2026.

[71] ESPOSITO, *op. cit.*, p. 7.

[72] MARANHÃO; FLORÊNCIO; ALMADA, 2021, p. 144-145.

para contextos amplos de compreensão e auditorias. Nesse ponto, vale mencionar que a estratégia agnóstica já mencionada, ao observar especificamente entrada e saída, tipicamente gerará interpretadores locais e não globais[73].

Ainda para Maranhão[74], tais estratégias de explicação levam em consideração um interlocutor com conhecimento técnico, não sendo suficientes para os demais leigos. Para isso, salienta outras três concepções que podem ser úteis nesse desafio: a primeira, denominada simutabilidade, determina que a explicação de uma decisão deve permitir que um ser humano, diante das entradas e dos parâmetros de configuração, possa reproduzir em tempo razoável os passos que levaram o sistema de IA àquela decisão. Embora tenha a sua concepção na ciência computacional, por sua vez pode ser de difícil aplicação na seara jurídica. A segunda, denominada de contrastiva, traz a necessidade de que a decisão seja comparada com outras alternativas plausíveis, demonstrando por que elas não foram seguidas e, consequentemente, o motivo pelo qual o resultado foi o demonstrado. Nesse caso, o usuário afetado poderia ajustar sua conduta de modo a produzir os resultados desejados ciente dos critérios utilizados. Mais uma vez, contudo, pontua o autor que em relação ao domínio jurídico não é plausível que o ônus de adequação do comportamento recaia sobre o titular leigo sendo que, por vezes, o ajuste sequer é possível.

As duas primeiras etapas relacionadas à explicação direcionada ao funcionamento do modelo e à forma de compreensão entre os *inputs* e *outputs* estão mais relacionadas com as estratégias de modelos de análise de sensibilidade ou decomposicionais, já analisadas. Por sua vez, os modelos agnósticos se sobreporiam à relação de *inputs* e *outputs* com base em um formato mais simples de explicação, sequer trazendo informações sobre o método de funcionamento do sistema inicial.

Nesse cenário, pontua Maranhão[75], uma terceira concepção da explicação seria a contestabilidade, ou seja, uma explicação deve fornecer insumo para que o usuário possa avaliar as consequências de uma decisão e, caso queira, obtenha as informações necessárias para contestá-la por vias judiciais. Portanto, para que essa contestação seja efetivamente possível, deve especificar a lógica que levou à decisão sob análise, permitindo a identificação dos atores humanos que contribuíram para a produção do resultado. Esse formato traz vantagem, para o autor, em relação aos demais, já que não pressupõe o aprofundamento do funcionamento do sistema, mas apenas a compreensão sobre o resultado gerado. Assim, tal concepção se encaixa perfeitamente na definição do modelo agnóstico, oferecendo uma alternativa inteligível de justificação do *input*. Se dá, portanto, em relação ao modelo explicativo que se dirige à contestação para eventual invalidação do resultado.

Conclusão

Que as tecnologias desenvolvidas e constituídas em torno de ferramentas que utilizam técnicas de *machine learning* e *deep learning* no contexto da IA já estão inseridas no dia a dia da sociedade não restam dúvidas. Todavia, os desafios para o presente e o futuro se inserem no contexto dos efeitos que poderão advir de tais construções, positivos e negativos, especialmente no que se refere aos aspectos éticos que lhes são tangentes. Isso porque, ao delegar cada vez mais partes da vida humana às máquinas, delega-se também aspectos morais e sociais que os seres humanos sequer foram capazes de resolver. Com efeito, tem-se hodiernamente uma sociedade desigual, com questões delicadas a serem superadas. Assim, transferir tais responsabilidades à tecnologia sem a devida compreensão de seus impactos pode ser um catalisador de tais injustiças.

[73] MARANHÃO; FLORÊNCIO; ALMADA, 2021, p. 144-145.

[74] MARANHÃO; FLORÊNCIO; ALMADA, 2021, p. 145-146.

[75] MARANHÃO; FLORÊNCIO; ALMADA, 2021, p. 150.

Ao serem treinadas nas bases de dados atualmente disponíveis, as tecnologias de IA, caso não tenham um acompanhamento técnico de suas decisões próximo, levando-se em consideração a problemática ética e moral mencionada, pode não apenas trabalhar no sentido de manter o *status quo* vigente, como também reforçá-lo. Isso porque, sob o prisma da segurança, assertividade e imparcialidade que ainda hoje ronda as tecnologias existentes, as decisões advindas dessas ferramentas podem ser consideradas como verdades absolutas. Tudo isso pautado na opacidade e escuridão com que tais decisões são tomadas, revestidas de múltiplas camadas e possibilidades de tomada de decisão, bem como sem uma cadeia de responsabilidade clara acerca dos agentes envolvidos na disponibilização da ferramenta.

Nesse contexto, o trabalho debateu a questão das consequências possivelmente nefastas da opacidade algorítmica na tradução dos valores sociais diante de suas decisões. Para tanto, aprofundou-se nas definições realçadas por Pasquale sobre a *black-box* e os potenciais resultados que ela pode gerar sobre os humanos de maneira geral, tencionados a um novo contexto cada vez mais complexo de atendimento aos requisitos de transparência e explicabilidade já existentes.

Ciente das complexidades trazidas pelo novo contexto tecnológico, em um diálogo doutrinário e de comparação internacional, o trabalho buscou compreender as origens que estabelecem as bases dos direitos atuais sobre transparência e, a partir desse ponto, enfatizar as futuras possibilidades de ajustá-los ao presente cenário a partir de interpretações que seguem, especialmente, o marco teórico do direito civil-constitucional, efetivando os valores constitucionais em ordenamentos legais ordinários, como a lei de propriedade intelectual brasileira e futuras normativas referentes à regulamentação da IA no país.

Assim, conclui-se que sistemas que contam com a participação de IA em seu processo de desenvolvimento devem ser acompanhados de um processo decisório igualmente transparente. Dadas as limitações técnicas afetas a tal previsão, potencializada por processos de *machine learning*, *deep learning* e redes neurais, vislumbra-se que o alcance de tal direito deve se valer de todas as ferramentas disponíveis, sejam elas previsões legais, revisão humana, auxílio da própria tecnologia para pormenorizar os dados levados em consideração em uma determinada decisão e, inclusive, responsabilidades específicas sobre os agentes envolvidos na cadeia de utilização da IA, a saber implantadores e fornecedores. Embora não se vislumbre uma única solução, o presente trabalho aponta, na realidade, para uma miríade de alternativas que apenas em conjunto podem ser capazes de efetivar propriamente o direito à explicabilidade e, consequentemente, à transparência. Cumpre reiterar que os direitos constitucionais da dignidade da pessoa humana, efetivados aqui pela autonomia da vontade do indivíduo, somente poderão ser observados caso o sujeito seja capaz de compreender como a tecnologia impacta ou restringe seus direitos e liberdades, bem como refutá-la especificamente.

Referências

BAIÃO, Kelly Sampaio; GONÇALVES, Kalline Carvalho. A garantia da privacidade na sociedade tecnológica: um imperativo à concretização do princípio da dignidade da pessoa humana. *Civilistica.com*, Rio de Janeiro, ano 3, n. 2, p. 1-24, jul./dez. 2014. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/151. Acesso em: 15 jun. 2024.

BARBOSA, Mafalda Miranda. Nas fronteiras de um admirável mundo novo? O problema da personificação de entes dotados de inteligência artificial. *In*: BARBOSA, Mafalda Miranda; BRAGA NETTO, Felipe; SILVA, Michael César; FALEIROS JÚNIOR, José Luiz de Moura (coord.). *Direito digital e inteligência artificial*: diálogos entre Brasil e Europa. Indaiatuba, SP: Editora Foco, 2021. p. 97-112.

BLASIMME, Alessandro; VAYENA, Effy. The ethics of AI in biomedical research, patient care, and public health. *In*: DUBBER, Markus D.; PASQUALE, Frank; DAS, Sunit (ed.). *The Oxford handbook of ethics of AI*. New York: Oxford University Press, 2020. p. 703-718. DOI: https://doi.org/10.1093/oxfordhb/9780190067397.013.45.

BOSTROM, Nick. *Superinteligência:* Caminhos, perigos e estratégias para um novo mundo. Rio de Janeiro. DarkSide, 2014.

BRASIL. [Constituição (1988)]. *Constituição da República Federativa do Brasil de 1988*. Brasília, DF: Presidência da República, [2026]. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 10 maio 2026.

BRASIL. *Emenda Constitucional nº 115*, de 10 de fevereiro de 2022. Altera a Constituição Federal para incluir proteção de dados pessoais entre os direitos fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Brasília, DF: Presidência da República, 2022. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em 15 jun 2024.

BRASIL. *Lei nº 9.609, de 19 de fevereiro de 1998*. Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências. Brasília, DF: Presidência da República, 1998. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9609.htm. Acesso em: 26 jun. 2024.

BRASIL. *Lei nº 9.610, de 19 de fevereiro de 1998*. Altera, atualiza e consolida a legislação sobre direitos autorais e dá outras providências. Brasília, DF: Presidência da República, 1998. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9610.htm. Acesso em: 26 jun. 2024

BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 13 jun. 2024.

BRASIL. *Projeto de Lei nº 21, de 2020*. Estabelece os fundamentos, princípios e diretrizes para o desenvolvimento e aplicação da inteligência artificial no Brasil. Brasília, DF: Câmara dos Deputados, 2020. Disponível em: https://www.camara.leg.br/propostas-legislativas/2236340. Acesso em: 13 jun 2024.

BURR, Christopher; TADDEO, Mariarosaria; FLORIDI, Luciano. The ethics of digital well-being: a thematic review. *Science and Engineering Ethics*, [*S. l.*], v. 26, n. 4, p. 2313-2343, 2020. DOI: https://doi.org/10.1007/s11948-020-00175-8.

CATH, Corinne; WACHTER, Sandra; MITTELSTADT, Brent; TADDEO, Mariarosaria; FLORIDI, Luciano. Artificial Intelligence and the 'Good Society': the US, EU, and UK approach. *Science and Engineering Ethics*, [*S. l.*], v. 24, n. 2, p. 505-528, 2018. DOI: https://doi.org/10.1007/s11948-017-9901-7. Disponível em: https://pubmed.ncbi.nlm.nih.gov/28353045/. Acesso em: 12 maio 2026.

CHINELLATO, Silmara Juny de Abreu. A denominada personalidade eletrônica, inteligência artificial e direito do autor: autoria na obra musical. *In*: CHINELLATO, Silmara J. de A. (coord.); TOMASEVICIUS FILHO, Eduardo (org.). *Inteligência artificial*: visões interdisciplinares e internacionais. São Paulo: Almedina, 2023.

DONEDA, Danilo; ALMEIDA, Virgílio A. F. O que é a governança de algoritmos? *Revista poliTICs*, [*S. l.*], out. 2016. Disponível em: https://politics.org.br/edicoes/o-que-e-governanca-de-algoritmos. Acesso em: 22 maio 2026.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*: elementos da formação da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

FRAZÃO, Ana. Apresentação da obra. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord.). *Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro*. São Paulo: Revista dos Tribunais, 2019.

FRAZÃO, Ana. Discriminação algorítmica: algumas conclusões. *JOTA*, [*S. l.*], 29 set. 2021. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/discriminacao-algoritmica-como-lidar-com-as-incertezas-22092021. Acesso em: 22 maio 2026.

FLORIDI, Luciano; COWLS, Josh; BELTRAMETTI, Monica; CHATILA, Raja; CHAZERAND, Patrice; DIGNUM, Virginia; LUETGE, Christoph; MADELIN, Robert; PAGALLO, Ugo; ROSSI, Francesca; SCHAFER, Burkhard; VALCKE, Peggy; VAYENA, Effy. AI4People --an ethical framework for a good AI society: opportunities, risks, principles, and recommendations. Minds and *Machines*, [*S. l.*], v. 28, n. 4, p. 689-707, 2018. DOI: https://doi.org/10.1007/s11023-018-9482-5.

FLORIDI, Luciano; TADDEO, Mariarosaria. What is data ethics? Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering *Sciences*, [*S. l.*], v. 374, n. 2083, p. 20160360, 2016. DOI: https://doi.org/10.1098/rsta.2016.0360. Disponível em: https://royalsocietypublishing.org/doi/full/10.1098/rsta.2016.0360. Acesso em: 12 maio 2026.

FRIEDMAN, Batya; NISSENBAUM, Helen. Bias in computer systems. *ACM Transactions on* Information Systems, New York, v. 14, n. 3, p. 330-347, jul. 1996. DOI: https://doi.org/10.1145/230538.230561.

GUTIERREZ, Andriei. É possível confiar em um sistema de inteligência artificial? Práticas em torno da melhoria da sua confiança, segurança e evidências de accountability. In: FRAZÃO, Ana; MULHOLLAND, Caitlin (coord.). *Inteligência artificial e direito*: ética, regulação e responsabilidade. 2. ed. rev., atual. e ampl. São Paulo: Thomson Reuters Brasil, 2020. p. 81-94.

KONDER, Carlos Nelson. Privacidade e corpo: convergências possíveis. *Pensar* - Revista de Ciências Jurídicas, [*S. l.*], v. 18, n. 2, p. 354-400, 2013. DOI: https://doi.org/10.5020/23172150.2012.354-400. Acesso em: 13 mai. 2026.

LEAL, Martha. Data scraping e responsabilidade do controlador. *Consultor Jurídico*, [*S. l.*], 10 jul. 2021. Disponível em: https://www.conjur.com.br/2021-jul-10/martha-leal-data-scraping-responsabilidade-controlador/. Acesso em: 26 jun. 2024.

MAGRANI, Eduardo; SILVA, Priscila; VIOLA, Rafael. Novas perspectivas sobre ética e responsabilidade de inteligência artificial. *In*: FRAZÃO, Ana; MULHOLLAND, Caitlin (coord.). *Inteligência artificial e direito*: ética, regulação e responsabilidade. 2. ed. rev., atual. e ampl. São Paulo: Thomson Reuters Brasil, 2020. p. 111-143.

MARANHÃO, Juliano; COZMAN, Fábio Gagliardi; ALMADA, Marco. Concepções de explicação e do direito à explicação de decisões automatizadas. *In*: VAINZOF, Rony; GUTIERREZ, Andriei (coord.). *Inteligência artificial: sociedade, economia e Estado*. São Paulo: Thomson Reuters Brasil, 2021. p. 137-154.

MARANHÃO, Juliano Souza de Albuquerque; FLORÊNCIO, Juliana Abrusio; ALMADA, Marco. Inteligência artificial aplicada ao direito e o direito da inteligência artificial. *Suprema*: Revista de Estudos Constitucionais, Brasília, v. 1, n. 1, p. 154-180, jan./jun. 2021. DOI: https://doi.org/10.53798/suprema.2021.v1.n1.a20.

MEDON, Filipe. *Inteligência Artificial e Responsabilidade Civil:* Autonomia, Riscos e Solidariedade. Salvador: JusPodivm, 2020.

MITTELSTADT, Brent Daniel; ALLO, Patrick; TADDEO, Mariarosaria; WACHTER, Sandra; FLORIDI, Luciano. The ethics of algorithms: mapping the debate. *Big Data & Society*, [S. l.], v. 3, n. 2, p. 1-21, 2016. DOI: https://doi.org/10.1177/2053951716679679.

MITTELSTADT, Brent Daniel; FLORIDI, Luciano. The ethics of big data: current and foreseeable issues in biomedical contexts. *In*: MITTELSTADT, Brent Daniel; FLORIDI, Luciano (ed.). *The ethics of biomedical big data*. Cham: Springer, 2016. (Law, Governance and Technology Series, v. 29). p. 445-480. DOI: https://doi.org/10.1007/978-3-319-33525-4_19.

MORLEY, Jessica; FLORIDI, Luciano. The limits of empowerment: how to reframe the role of mHealth tools in the healthcare ecosystem. *Science and Engineering Ethics*, [*S. l.*], v. 26, n. 3, p. 1159-1183, 2020. DOI: https://doi.org/10.1007/s11948-019-00115-1.

MULHOLLAND, Caitlin. O direito de não saber como decorrência do direito à intimidade. *Civilistica.com*, Rio de Janeiro, ano 1, n. 1, 2012. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/27. Acesso em: 26 out. 2026.

MULHOLLAND, Caitlin Sampaio; FRAJHOF, Isabella Zalcberg. Inteligência artificial e a Lei Geral de Proteção de Dados Pessoais: breves anotações sobre o direito à explicação perante a tomada de decisões por meio de machine learning. *In*: FRAZÃO, Ana; MULHOLLAND, Caitlin (coord.). *Inteligência artificial e direito*: ética, regulação e responsabilidade. 2. ed. rev., atual. e ampl. São Paulo: Thomson Reuters Brasil, 2020. p. 267-289.

O'NEIL, Cathy. *Weapons of math destruction***:** how big data increase inequality and threatens democracy. New York: Crown Publishers, 2016.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD). *Recommendation of the Council on Artificial Intelligence*. Paris: OECD, 2019. Disponível em: http://bit.ly/2Zbn9pT. Acesso em: 14 jun. 2024.

PAGALLO, Ugo. *The Law of Robots:* Crimes, Contracts and Torts. Berlim: Springer Science & Business Media, 2013. Disponível em: https://link.springer.com/content/pdf/bfm%3A978-94-007-6564-1%2F1.pdf. Acesso em: 13 jun. 2024.

PASQUALE, Frank. *The Black Box Society:* The Secret Algorithms That Control Money and Information. Cambridge: Harvard University Press, 2015.

PERLINGIERI, Pietro. Normas constitucionais nas relações privadas. *Civilistica.com*, Rio de Janeiro, ano 8, n. 1, p. 1-9, 2019. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/407. Acesso em: 13 jun. 2024.

PERLINGIERI, Pietro. *Perfis do direito civil.* Tradução de: Maria Cristina de Cicco. 3. ed., rev. e ampl. Rio de Janeiro: Renovar, 2002.

PERLINGIERI, Pietro. La dottrina del diritto civile nella legalità costituzionale. *Rassegna di diritto civile*, [*S. l.*], v. 28, n. 2, p. 497-510, 2007.

PETITGAND, Cécile; RÉGIS, Catherine. Principes éthiques et encadrement juridique de l'intelligence artificielle en santé: exemple de la Déclaration de Montréal pour un développement responsable de l'intelligence artificielle. *Journal de Droit de la Santé et de l'Assurance Maladie*, [*S. l.*], n. 22, p. 101-105, 2019.

POLIDO, Fabrício Bertini Pasquot. Novas perspectivas para regulação da inteligência artificial: diálogos entre as políticas domésticas e os processos legais transnacionais. *In*: FRAZÃO, Ana; MULHOLLAND, Caitlin (coord.). *Inteligência artificial e direito*: ética, regulação e responsabilidade. 2. ed. rev., atual. e ampl. São Paulo: Thomson Reuters Brasil, 2020. p. 175-204.

REQUIÃO, Maurício; COSTA, Diego Carneiro. Discriminação algorítmica: ações afirmativas como estratégia de combate. *Civilistica.com*, Rio de Janeiro, ano 11, n. 3, p. 1-24, 2022. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/804. Acesso em: 22 jun. 2024.

RODOTÀ, Stefano. Entrevista à RTDC. *Revista Trimestral de Direito Civil*, Rio de Janeiro, v. 3, n. 11, p. 225-308, jul./set. 2002. Entrevista concedida a Danilo Doneda. Disponível em: https://doneda.net/2017/06/23/entrevista-com-stefano-rodota/. Acesso em: 13 maio 2026.

RODOTÀ, Stefano. *Il mondo nella rete*: quali i diritti, quali i vincoli. Roma; Bari: Laterza, 2014. Disponível em: https://www.laterza.it/scheda-libro/?isbn=9788858111659. Acesso em: 14 maio 2026.

SCHUMPETER, Josef Alois. *Capitalismo, socialismo e democracia.* New York, NY: Harper and Row, 1942.

SYMON, Maybin. Sistema de Algoritmo que determina pena de condenados cria polêmica nos Estados Unidos. *BBC Brasil*, 31 de outubro de 2016. Disponível em: https://www.bbc.com/portuguese/brasil-37677421. Acesso em 22 mai. 2026.

TEFFÉ, Chiara Antonia Spadaccini de; CHEDIEK, Juliana da Silva Ribeiro Gomes. A aplicação da metodologia do direito civil constitucional na realidade jurídica brasileira: os exemplos do direito de não saber e das famílias simultâneas. *In*: SCHREIBER, Anderson; KONDER, Carlos Nelson (coord.). *Direito civil constitucional*. São Paulo: Atlas, 2016. p. 189-221.

TEPEDINO, Gustavo. A tutela da personalidade no ordenamento civil-constitucional brasileiro. *In*: TEPEDINO, Gustavo. *Temas de direito civil*. 3. ed. Rio de Janeiro: Renovar, 2004. p. 23-58.

TERRA, Aline de Miranda Valverde. Liberdade do intérprete na metodologia civil constitucional. *In*: SCHREIBER, Anderson; KONDER, Carlos Nelson (coord.). *Direito civil constitucional*. São Paulo: Atlas, 2016. p. 47-70.

TOMASEVICIUS FILHO, Eduardo. Inteligência artificial e direitos da personalidade: uma contradição em termos? *Revista da Faculdade de Direito d*a Universidade de São Paulo, São Paulo, v. 113, p. 133-149, jan./dez. 2018. DOI: https://doi.org/10.11606/issn.2318-8235.v113i0p133-149.

UNIÃO EUROPEIA. Comissão Europeia. Grupo de Peritos de Alto Nível sobre Inteligência Artificial. *Orientações éticas para uma IA de confiança*. Bruxelas: Comissão Europeia, 2019. Disponível em: https://op.europa.eu/pt/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1. Acesso em: 13 jun. 2024.

UNIÃO EUROPEIA. Parlamento Europeu. *The ethics of artificial intelligence*: issues and initiatives. Bruxelas: Parlamento Europeu, 2020. DOI: https://doi.org/10.2861/6644.

UNIÃO EUROPEIA. *Parlamento Europeu e Conselho da União Europeia. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016*, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Bruxelas: Parlamento Europeu e Conselho da União Europeia, 2016. Disponível em: https://eur-lex.europa.eu/eli/reg/2016/679/oj. Acesso em: 8 jun. 2024.

UNIVERSITÉ DE MONTRÉAL. *Déclaration de Montréal pour un développement responsable de l'intelligence artificielle*. Montréal: Université de Montréal, 2018. Disponível em: https://www.montrealdeclaration-responsibleai.com/. Acesso em: 11 jun. 2024.

UNITED STATES PATENT AND TRADEMARK OFFICE. *Inventorship guidance for AI-assisted inventions*. Federal Register, v. 89, p. 10043, 13 fev. 2024. Disponível em: https://www.federalregister.gov/documents/2024/02/13/2024-02623/inventorship-guidance-for-ai-assisted-inventions.

Firjan
SENAI
SESI
IEL
CIRJ