IX ENCONTRO VIRTUAL DO CONPEDI

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS VI

D598

Direito, governança e novas tecnologias VI [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Jonathan Barros Vita; Patricia Eliane da Rosa Sardeto; Thiago De Mello Azevedo Guilherme – Florianópolis: CONPEDI, 2026.

Inclui bibliografia
ISBN: 978-65-5274-587-3
Modo de acesso: www.conpedi.org.br em publicações
Tema: Constituição, Processo e Justiça Social: o papel da jurisdição constitucional na efetivação de direitos
2. Direito. 3. Governança e novas tecnologias. IX Encontro Virtual do CONPEDI (2: 2026: Florianópolis, Brasil).

CDU: 34

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

IX ENCONTRO VIRTUAL DO CONPEDI

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS VI

Apresentação

O IX Encontro Virtual do CONPEDI foi realizado entre os dias 22 a 26 de junho de 2026 e teve como temática central “Constituição, processo e justiça social: o papel da jurisdição constitucional na efetivação de direitos”.

No plano das diversas atividades acadêmicas ocorridas neste encontro, destacam-se, além das palestras e oficinas, os grupos de trabalho temáticos, os quais representam um locus de interação entre pesquisadores que apresentam as suas pesquisas temáticas, seguindo-se de debates.

Especificamente, para operacionalizar tal modelo, os coordenadores dos GTs são os responsáveis pela organização dos trabalhos em blocos temáticos, dando coerência à produção e estabelecendo um fio condutor para organizar os debates em subtemas.

No caso concreto, assim aconteceu com o GT Direito, Governança e Novas Tecnologias VI, o qual ocorreu no dia 26 de junho de 2026 das 14h00 às 17h30 e foi coordenado pelos professores Jonathan Barros Vita, Thiago de Mello Azevedo Guilherme e Patricia Eliane da Rosa Sardeto.

O referido GT foi palco de profícuas discussões decorrentes dos trabalhos apresentados, os quais são publicados na presente obra, a qual foi organizada seguindo alguns blocos temáticos específicos, que compreenderam os 21 artigos submetidos ao GT, cujos temas são citados abaixo:

2. O declínio do senso-crítico na era digital: a erosão da autonomia e a superficialidade na sociedade do espetáculo.

Autor(es): Juliana Sales Pavini / Victor Matheus de Campos Leite Neves

3. Sistemas autônomos, vigilância algorítmica, cidadania e os limites do controle humano na governança contemporânea.

Autor(es): Rossana Gemeli Roncato Carloto / Marcio Renan Hamel

4. Transformações legislativas no enfrentamento da desinformação política: uma análise comparativa sobre projetos de lei propostos entre 2018 e 2026.

Autor(es):Bruna Bastos / Leticia Kirinus Danski / Isabela Quartieri da Rosa

5. Proteção integral, opacidade algorítmica e os limites do ECA Digital na governança de plataformas digitais.

Autor(es):Isabela Quartieri da Rosa / Ana Carolina Sassi / Rafael Santos de Oliveira

6. O constitucionalismo digital como limite ao poder privado das Big Techs nas relações digitais.

Autor(es):Samira Bonfim Bernardi / Roberto da Freiria Estevão

7. A possibilidade do desenvolvimento da ação comunicativa entre adolescentes na era digital.

Autor(es):Samira Bonfim Bernardi

9. Governança algorítmica no setor público, participação social e seus impactos jurídicos.

Autor(es): Amadeu dos Anjos Vidonho Junior

10. Inteligência Artificial de Alto Risco e Assurance Contínua: um estudo dogmático à luz do AI Act e do NIST AI RMF.

Autor(es):Daniel David Guimarães Freire / Karine Queiroz de Souza

11. Web agêntica, microtrabalhos e responsabilização jurídica: rastreabilidade e proteção de direitos fundamentais.

Autor(es): Sebastiana Sena Carvalho / Cibele Alexandre Uchoa / João Araújo Monteiro Neto

12. Quality Assurance em Sistemas Automatizados de Compliance e AML: limites jurídicos da confiança em decisões algorítmicas.

Autor(es): Daniel David Guimarães Freire / Karine Queiroz de Souza

13. Governança de IA Agêntica: uma análise do Framework AgentSafe e os desafios de compliance na Web Agêntica.

Autor(es): Gustavo Amaral Lima / Cibele Alexandre Uchoa / João Araújo Monteiro Neto

14. A accountability algorítmica na atividade administrativa do Poder Judiciário brasileiro.

Autor(es): Mateus Marinho Alencar / Cassius Guimaraes Chai

Bloco 3 – Inteligência Artificial, Profissões, Educação e Instituições

16. Educação jurídica em transformação: entre a formação crítica e os desafios do uso da Inteligência Artificial.

Autor(es): Denise Almeida De Andrade / Beatriz de Castro Rosa / Rafaela Mota Holanda

17. Responsabilidade civil do advogado pelos atos praticados com a Inteligência Artificial Generativa no processo judicial eletrônico brasileiro.

Autor(es): Amadeu dos Anjos Vidonho Junior

18. Sala de aula em movimento, uma experiência com o ensino médio: juventude e redes sociais, entre a liberdade de acesso e os riscos da exposição íntima.

Autor(es): Dayana Claudia Tavares Barros De Castro / Aimme Beatrice de Oliveira Dutra Cordeiro / Denise Almeida De Andrade

19. Da imprescindibilidade da subjetividade humana na tessitura do processo decisório: por uma perspectiva ética na utilização da Inteligência Artificial.

Autor(es): Lanaira da Silva / Rayssa Gargano Soares

20. A reconfiguração do standard of care médico na era algorítmica: o dever de diligência tecnológica e os limites da confiança nas decisões automatizadas na saúde.

Autor(es): Sara Lupion dos Santos / Patricia Eliane da Rosa Sardeto

21. Inteligência Artificial e qualificação registral: limites dogmáticos e possibilidades de coexistência no registro de imóveis.

Esse é o contexto que permite a promoção e o incentivo da cultura jurídica no Brasil, consolidando o CONPEDI, cada vez mais, como um importante espaço para discussão e apresentação das pesquisas desenvolvidas nos ambientes acadêmicos da graduação e pós-graduação em direito.

Finalmente, desejamos uma boa leitura, deste Grupo de trabalho que reuniu diversos textos e autores de todo o Brasil para servir como resultado de pesquisas científicas realizadas no âmbito dos cursos de Pós-Graduação Stricto Sensu de nosso país.

Prof. Dr. Jonathan Barros Vita – Unimar

Prof. Dr. Thiago De Mello Azevedo Guilherme - ITE-CEUB

Profa. Dra. Patricia Eliane da Rosa Sardeto – Pontifícia Universidade Católica do Paraná – Câmpus Londrina

QUALITY ASSURANCE EM SISTEMAS AUTOMATIZADOS DE COMPLIANCE E AML: LIMITES JURÍDICOS DA CONFIANÇA EM DECISÕES ALGORÍTMICAS

QUALITY ASSURANCE IN AUTOMATED COMPLIANCE AND AML SYSTEMS: LEGAL LIMITS OF TRUST IN ALGORITHMIC DECISION-MAKING

Daniel David Guimarães Freire
Karine Queiroz de Souza

Resumo

O presente artigo analisa os limites jurídicos da utilização de sistemas de inteligência artificial em estruturas automatizadas de Compliance e prevenção à lavagem de dinheiro (AML), com especial atenção ao papel do Quality Assurance como mecanismo de governança algorítmica contínua. Parte-se da hipótese de que modelos tradicionais de supervisão e validação são insuficientes para assegurar legitimidade, accountability e controle institucional em sistemas adaptativos capazes de alterar seu desempenho ao longo do tempo. A pesquisa examina como processos automatizados de classificação de risco, monitoramento transacional e detecção de padrões suspeitos produzem tensões relevantes envolvendo opacidade algorítmica, supervisão humana, discricionariedade automatizada e proteção de direitos fundamentais. A partir de revisão bibliográfica e análise normativa, o trabalho investiga a relação entre governança de IA, auditabilidade, rastreabilidade e observabilidade algorítmica em ambientes regulatórios de alta complexidade. Sustenta-se que o Quality Assurance não pode ser compreendido apenas como mecanismo técnico de teste ou validação operacional, mas como infraestrutura jurídico-regulatória voltada à produção contínua de evidências de conformidade, monitoramento de riscos, detecção de falhas, controle institucional e revisão permanente de sistemas automatizados de decisão em ambientes de Compliance e AML.

Palavras-chave: Inteligência artificial, Compliance automatizado, Aml, Quality assurance, Governança algorítmica, Accountability

Abstract/Resumen/Résumé

fundamental rights. Through bibliographic review and normative analysis, the paper explores the relationship between AI governance, auditability, traceability, and algorithmic observability within highly complex regulatory environments. It argues that Quality Assurance should not be understood merely as a technical mechanism for testing or operational validation, but rather as a legal-regulatory infrastructure aimed at the continuous production of evidence regarding compliance, risk monitoring, failure detection, institutional oversight, and permanent review of automated decision-making systems in Compliance and AML environments.

Keywords/Palabras-claves/Mots-clés: Artificial intelligence, Automated compliance, Anti-money laundering, Quality assurance, Algorithmic governance, Accountability

1. INTRODUÇÃO

A transformação digital provocou profundas alterações na estrutura dos sistemas regulatórios contemporâneos. O avanço da inteligência artificial e das tecnologias de automação passou a influenciar diretamente a forma como empresas, instituições financeiras e órgãos reguladores executam atividades relacionadas à prevenção à lavagem de dinheiro, análise de risco e Compliance corporativo. Em um cenário marcado pela expansão do fluxo global de dados, pela digitalização das relações econômicas e pelo aumento exponencial das transações financeiras, tornou-se praticamente inviável depender exclusivamente da atuação humana tradicional para monitoramento regulatório em larga escala.

A utilização de sistemas automatizados de Compliance passou a ocupar posição estratégica dentro das estruturas de governança corporativa. Ferramentas baseadas em machine learning, mineração de dados e inteligência artificial são utilizadas para identificar operações suspeitas, detectar padrões anômalos, classificar perfis de risco e gerar alertas automatizados de possível irregularidade. Esses sistemas permitem velocidade operacional significativamente superior à análise humana convencional, além de redução de custos regulatórios e aumento da capacidade de monitoramento contínuo.

A expansão da automação regulatória foi incentivada também por organismos internacionais voltados ao combate à lavagem de dinheiro e financiamento do terrorismo. O Grupo de Ação Financeira Internacional (GAFI/FATF) consolidou internacionalmente a chamada abordagem baseada em risco, estimulando instituições a desenvolver mecanismos mais sofisticados de monitoramento e identificação de operações potencialmente ilícitas (FATF, 2021).

Entretanto, a crescente dependência de decisões automatizadas levanta importantes preocupações jurídicas e éticas. Embora os sistemas algorítmicos ampliem a eficiência operacional, eles também introduzem riscos relacionados à opacidade decisória, discriminação algorítmica, falsos positivos e ausência de transparência. Em diversos casos, indivíduos podem sofrer restrições financeiras, encerramento de contas, bloqueios operacionais ou classificação automática de risco sem compreender os critérios utilizados pelos sistemas automatizados.

A literatura contemporânea passou a questionar a ideia de neutralidade tecnológica. Os sistemas automatizados não operam de maneira completamente imparcial, uma vez que refletem escolhas humanas relacionadas à coleta de dados, definição de parâmetros estatísticos, objetivos

institucionais e variáveis utilizadas no treinamento dos modelos (O'NEIL, 2020). Dessa forma, decisões automatizadas podem reproduzir vieses estruturais e ampliar desigualdades já existentes.

No plano internacional, instrumentos regulatórios como o General Data Protection Regulation (GDPR) e o AI Act europeu vêm consolidando modelos de governança algorítmica voltados à transparência, supervisão humana e accountability. O debate contemporâneo sobre inteligência artificial deixou de se limitar à eficiência tecnológica e passou a envolver diretamente a preservação de direitos fundamentais em sociedades altamente digitalizadas.

O problema central deste artigo consiste em analisar quais são os limites jurídicos da confiança em sistemas automatizados de Compliance e AML, especialmente em ambientes regulatórios sensíveis. Busca-se investigar até que ponto decisões automatizadas podem substituir a atuação humana e quais mecanismos jurídicos são necessários para assegurar legitimidade, auditabilidade e proteção de direitos fundamentais. A metodologia utilizada é qualitativa, baseada em revisão bibliográfica e análise normativa nacional e internacional. O estudo divide-se em dois capítulos principais. O primeiro aborda a expansão dos sistemas automatizados de Compliance e seus impactos jurídicos na regulação contemporânea. O segundo analisa os limites jurídicos da confiança algorítmica, especialmente à luz da LGPD, da governança algorítmica e da responsabilidade decorrente de decisões automatizadas.

Ao final, apresenta-se uma reflexão acerca da necessidade de mecanismos de Quality Assurance voltados à validação, auditabilidade e confiabilidade de sistemas automatizados utilizados em ambientes regulatórios críticos.

2. SISTEMAS AUTOMATIZADOS DE COMPLIANCE NA REGULAÇÃO CONTEMPORÂNEA

O desenvolvimento tecnológico das últimas décadas alterou profundamente a forma como empresas e instituições financeiras executam atividades regulatórias relacionadas à prevenção à lavagem de dinheiro e Compliance corporativo. O crescimento exponencial do fluxo de informações financeiras, aliado à complexidade das transações digitais contemporâneas, tornou inviável a dependência exclusiva de processos humanos tradicionais para monitoramento regulatório.

A incorporação de inteligência artificial aos sistemas de Compliance decorre diretamente da necessidade de ampliação da capacidade operacional das instituições financeiras. Ferramentas

automatizadas passaram a ser utilizadas para identificar padrões suspeitos, analisar movimentações financeiras, detectar inconsistências comportamentais e classificar níveis de risco de usuários e operações.

A lógica da automação regulatória foi fortalecida internacionalmente pela consolidação da abordagem baseada em risco. O GAFI passou a estimular que instituições financeiras desenvolvessem mecanismos proporcionais aos riscos identificados, incentivando a utilização de tecnologias capazes de processar grandes volumes de dados em tempo real (FATF, 2021).

A expansão dessas tecnologias também decorre de razões econômicas e operacionais. Sistemas automatizados permitem monitoramento contínuo, geração instantânea de alertas e redução significativa de custos regulatórios. Em um ambiente marcado pela hipercomplexidade das relações econômicas digitais, a automação passou a ser compreendida como instrumento indispensável para a manutenção da eficiência regulatória.

Todavia, a ampliação da eficiência operacional não elimina os riscos jurídicos decorrentes da automatização decisória. Pelo contrário, a crescente dependência de sistemas algorítmicos introduz novos problemas relacionados à transparência, accountability e proteção de direitos fundamentais.

Os modelos baseados em inteligência artificial operam frequentemente mediante análise probabilística de padrões comportamentais. Isso significa que decisões automatizadas não são construídas sobre certezas absolutas, mas sim sobre inferências estatísticas derivadas do comportamento de usuários e transações anteriores. Nesse contexto, indivíduos podem ser classificados como suspeitos sem terem praticado qualquer ilícito, apenas por apresentarem comportamentos semelhantes aos identificados previamente pelo sistema como potencialmente problemáticos. Tal lógica probabilística cria tensão direta com princípios fundamentais do Estado Democrático de Direito, especialmente a presunção de inocência e o devido processo legal.

A sociedade contemporânea passa, assim, a depender de estruturas decisórias inacessíveis ao escrutínio público e à fiscalização social (PASQUALE, 2015). No setor financeiro, a opacidade algorítmica torna-se particularmente preocupante devido ao potencial impacto sobre direitos fundamentais relacionados ao acesso a serviços financeiros e à liberdade econômica. Bloqueios automáticos, encerramento de contas e restrições operacionais podem ocorrer sem explicação adequada ao usuário afetado.

Além disso, sistemas automatizados de AML frequentemente operam mediante tratamento massivo de dados pessoais. Informações financeiras, geolocalização, perfil de consumo, histórico de transações e padrões comportamentais passam a alimentar modelos automatizados de classificação de risco. A utilização intensiva desses dados gera importantes questionamentos relacionados à proteção da privacidade e à autodeterminação informativa. A proteção de dados pessoais deixou de representar apenas uma questão de sigilo individual e passou a envolver mecanismos de controle sobre processos automatizados de decisão (DONEDA, 2021).

A Lei Geral de Proteção de Dados estabeleceu princípios relevantes para limitação do tratamento automatizado de dados pessoais. O princípio da transparência exige acesso claro às informações relacionadas ao tratamento de dados, enquanto os princípios da finalidade, necessidade e não discriminação impõem limites à utilização indiscriminada de sistemas automatizados (BRASIL, 2018).

A transparência algorítmica surge, assim, como requisito indispensável para legitimidade dos sistemas automatizados. A utilização de inteligência artificial em ambientes regulatórios sensíveis exige capacidade mínima de explicação acerca dos critérios utilizados pelas decisões automatizadas.

O problema torna-se ainda mais complexo diante da crescente autonomia dos sistemas de machine learning. Em muitos casos, modelos algorítmicos passam a modificar seus próprios padrões decisórios com base na análise contínua de novos dados.

Essa realidade amplia significativamente as dificuldades relacionadas à responsabilização jurídica. Quando uma decisão automatizada produz danos indevidos, torna-se difícil identificar exatamente onde ocorreu a falha: nos dados utilizados, na programação do sistema, nos critérios estatísticos adotados ou na ausência de supervisão humana adequada.

A discussão contemporânea sobre inteligência artificial aplicada ao Compliance demonstra que a eficiência tecnológica não pode ser confundida com legitimidade jurídica. A expansão da automação regulatória exige a construção de mecanismos robustos de governança, auditabilidade e controle humano efetivo.

Dessa forma, sistemas automatizados de Compliance deixam de representar apenas ferramentas operacionais e passam a desempenhar verdadeira função decisória em ambientes regulatórios altamente sensíveis.

A expansão da automação regulatória também produz transformações relevantes na própria estrutura de exercício do poder institucional. A utilização crescente de sistemas automatizados em ambientes de Compliance e AML não representa apenas substituição tecnológica de tarefas operacionais anteriormente desempenhadas por agentes humanos, mas a consolidação de formas de governança baseadas em classificação probabilística, monitoramento contínuo e gestão antecipatória de riscos (YEUNG, 2018). Nesse contexto, decisões potencialmente restritivas deixam de depender exclusivamente da constatação concreta de ilícitos e passam a ser influenciadas por inferências estatísticas derivadas de padrões comportamentais, correlações algorítmicas e modelos preditivos. A lógica regulatória desloca-se progressivamente da investigação de fatos determinados para a identificação preventiva de perfis considerados potencialmente suspeitos, ampliando o espaço de atuação de mecanismos automatizados de vigilância financeira (ROUVROY; BERNS, 2013).

Esse deslocamento produz tensão significativa com garantias clássicas do Estado Democrático de Direito. A classificação automatizada de indivíduos a partir de padrões probabilísticos pode gerar formas indiretas de presunção de risco incompatíveis com exigências de proporcionalidade, devido processo legal e não discriminação. Em muitos casos, o indivíduo afetado não possui acesso efetivo aos critérios utilizados pelo sistema, tampouco capacidade concreta de compreender quais fatores contribuíram para determinada classificação automatizada. A opacidade algorítmica, nesse cenário, não constitui apenas dificuldade técnica, mas elemento estrutural de assimetria informacional entre instituições financeiras e usuários submetidos às decisões automatizadas (PASQUALE, 2015).

Além disso, a incorporação de inteligência artificial aos mecanismos de Compliance tende a reforçar uma racionalidade institucional orientada pela maximização da detecção de risco e pela redução de exposição regulatória das organizações. Em ambientes marcados por forte pressão regulatória e possibilidade de responsabilização institucional, sistemas automatizados podem ser calibrados de maneira excessivamente conservadora, ampliando falsos positivos e produzindo bloqueios preventivos desproporcionais. A eficiência operacional, portanto, não elimina o risco de decisões arbitrárias; em determinadas circunstâncias, pode inclusive ampliar a escala e velocidade de reprodução de erros sistêmicos (O’NEIL, 2020).

A própria ideia de neutralidade tecnológica mostra-se insuficiente para compreender esses fenômenos. Modelos algorítmicos não operam em abstração, mas refletem escolhas institucionais

relacionadas à seleção de dados, definição de variáveis relevantes, construção de métricas de risco e estabelecimento de objetivos operacionais. A automação regulatória não elimina discricionariedade; apenas desloca parte dela para estruturas técnicas frequentemente inacessíveis ao escrutínio público. Como consequência, decisões automatizadas podem adquirir aparência de objetividade estatística mesmo quando reproduzem vieses estruturais, prioridades econômicas e estratégias institucionais de gerenciamento de risco incompatíveis com parâmetros adequados de proteção de direitos fundamentais (ZUBOFF, 2021; HILDEBRANDT, 2015).

3. LIMITES JURÍDICOS DA CONFIANÇA EM DECISÕES ALGORÍTMICAS E GOVERNANÇA REGULATÓRIA

A crescente utilização de inteligência artificial em sistemas de Compliance e AML não implica legitimidade irrestrita das decisões produzidas por modelos automatizados. Pelo contrário, a expansão dessas tecnologias intensifica a necessidade de mecanismos jurídicos capazes de limitar abusos, assegurar supervisão humana e preservar direitos fundamentais.

A confiança excessiva em sistemas automatizados pode produzir fenômeno conhecido como automation bias, no qual operadores humanos passam a aceitar conclusões algorítmicas sem questionamento crítico adequado. Em ambientes regulatórios, esse problema torna-se especialmente grave devido ao potencial impacto das decisões automatizadas sobre indivíduos e organizações.

A utilização massiva de dados comportamentais para previsão e classificação de indivíduos cria estruturas de monitoramento permanente capazes de ampliar práticas de vigilância social (ZUBOFF, 2021). Em ambientes financeiros, essa lógica pode resultar em exclusões automatizadas, classificação discriminatória de risco e restrições indevidas ao acesso a serviços essenciais.

Nesse contexto, a proteção de direitos fundamentais torna-se elemento central da discussão sobre governança algorítmica. A dignidade da pessoa humana, o devido processo legal, a proporcionalidade e a proteção de dados pessoais funcionam como limites constitucionais à autonomia decisória dos sistemas automatizados.

O artigo 20 da LGPD representa importante mecanismo de contenção da automação irrestrita. O direito à revisão de decisões automatizadas demonstra preocupação legislativa com a necessidade de preservação da supervisão humana sobre processos decisórios relevantes.

A proteção de dados pessoais não se limita à tutela da privacidade tradicional, mas envolve também controle sobre estruturas automatizadas capazes de impactar diretamente a esfera jurídica dos indivíduos (DONEDA, 2021).

A transparência algorítmica assume papel central nesse cenário. A legitimidade jurídica das decisões automatizadas depende da possibilidade de compreensão mínima acerca dos critérios utilizados pelos sistemas.

Não se trata necessariamente de exigir divulgação integral de códigos-fonte ou segredos comerciais, mas sim de assegurar capacidade mínima de explicação e auditabilidade. Sem transparência adequada, indivíduos afetados por decisões automatizadas tornam-se incapazes de exercer contraditório efetivo ou questionar eventuais erros sistêmicos.

A ausência de explicabilidade transforma os algoritmos em estruturas opacas de poder decisório. O fenômeno da "caixa-preta" algorítmica produz assimetria informacional significativa entre instituições e indivíduos afetados pelas decisões automatizadas (PASQUALE, 2015).

O avanço regulatório europeu demonstra preocupação crescente com esses riscos. O GDPR estabeleceu mecanismos voltados à proteção contra profiling abusivo e decisões exclusivamente automatizadas, enquanto o AI Act passou a classificar determinados sistemas de inteligência artificial como aplicações de alto risco.

Os sistemas utilizados em ambientes financeiros e regulatórios tendem a ser enquadrados como aplicações de alto risco devido ao potencial impacto sobre direitos fundamentais e acesso a serviços essenciais.

O AI Act europeu estabelece requisitos específicos relacionados à supervisão humana, gestão de riscos, qualidade dos dados utilizados, documentação técnica e monitoramento contínuo dos sistemas automatizados (EUROPEAN UNION, 2021).

Esses elementos demonstram que a governança algorítmica vem se consolidando internacionalmente como requisito indispensável para utilização legítima da inteligência artificial.

Outro aspecto relevante refere-se à responsabilidade civil decorrente de decisões automatizadas equivocadas. A utilização de inteligência artificial não elimina a responsabilidade das instituições que implementam esses sistemas.

Instituições financeiras continuam juridicamente responsáveis pelos impactos decorrentes de bloqueios indevidos, classificações discriminatórias e danos causados por falhas algorítmicas. A complexidade tecnológica não pode servir como mecanismo de exclusão de responsabilidade.

Entretanto, a responsabilização torna-se mais complexa diante da dificuldade de identificação precisa da causalidade em modelos baseados em machine learning. Em muitos casos, nem mesmo os desenvolvedores conseguem explicar integralmente o processo decisório realizado pelo algoritmo.

Essa dificuldade reforça a necessidade de mecanismos robustos de auditoria, rastreabilidade e governança contínua dos sistemas automatizados.

Além disso, cresce internacionalmente a preocupação com auditorias independentes voltadas à identificação de vieses estatísticos, inconsistências operacionais e falhas de treinamento dos sistemas.

Nesse cenário, o debate sobre Quality Assurance passa a adquirir relevância jurídica crescente. Embora tradicionalmente associado à área tecnológica, o conceito de Quality Assurance assume dimensão regulatória quando aplicado a sistemas automatizados utilizados em ambientes de alta sensibilidade.

Dessa forma, o futuro da inteligência artificial aplicada ao Compliance e AML dependerá cada vez mais da construção de modelos interdisciplinares capazes de integrar Direito, governança algorítmica, auditoria regulatória e mecanismos permanentes de validação tecnológica.

4. QUALITY ASSURANCE COMO MECANISMO DE CONFIABILIDADE E GOVERNANÇA EM SISTEMAS AUTOMATIZADOS DE COMPLIANCE

A análise dos limites jurídicos da confiança em decisões automatizadas evidencia que a legitimidade desses sistemas não pode ser presumida a partir de sua eficiência tecnológica. Como demonstrado, elementos como transparência, explicabilidade, auditabilidade e supervisão humana constituem requisitos indispensáveis para a validade jurídica da automação decisória em ambientes regulatórios sensíveis.

Nesse contexto, tais requisitos deixam de representar apenas diretrizes normativas abstratas e passam a demandar mecanismos concretos de implementação. É precisamente nesse ponto que o Quality Assurance assume papel estruturante. A garantia de confiabilidade de sistemas automatizados não decorre exclusivamente de seu desempenho estatístico, mas da existência de processos contínuos de validação, monitoramento e controle capazes de assegurar aderência a parâmetros técnicos e jurídicos ao longo de todo o ciclo de vida do sistema (NIST, 2023; ISO/IEC 42001, 2023).

Dessa forma, Quality Assurance deixa de configurar função meramente operacional e passa a integrar a própria infraestrutura de governança algorítmica. Para compreender essa mudança de função, é necessário observar, inicialmente, os limites dos modelos tradicionais de teste quando aplicados a sistemas baseados em inteligência artificial.

Os modelos clássicos de teste de software foram concebidos para sistemas determinísticos, nos quais o comportamento esperado pode ser previamente definido com elevado grau de previsibilidade. Nesse paradigma, a validação consiste na verificação da conformidade entre entradas e saídas com base em regras explícitas.

Entretanto, essa abordagem mostra-se insuficiente diante de sistemas baseados em inteligência artificial. Modelos de machine learning operam por inferência estatística e dependem diretamente dos dados utilizados em seu treinamento, o que torna seu comportamento dinâmico e parcialmente imprevisível (FELDERER; RAMLER, 2021).

A ISO/IEC 25059 reconhece essa distinção ao estabelecer que a qualidade de sistemas de IA deve incorporar atributos como robustez, explicabilidade, rastreabilidade e consistência decisória (ISO/IEC 25059, 2023). Nesse contexto, testar deixa de significar apenas validar código e passa a envolver a análise crítica do comportamento do modelo, da qualidade dos dados e da estabilidade das inferências produzidas (ZHANG et al., 2022).

Em ambientes de Compliance e AML, essa limitação assume relevância jurídica direta. A utilização de modelos probabilísticos pode gerar classificações indevidas de risco, evidenciando que a insuficiência dos modelos tradicionais de teste não representa apenas um problema técnico, mas um fator de risco regulatório.

Diante dessa insuficiência, a confiabilidade de sistemas automatizados passa a depender da implementação de mecanismos estruturados de validação e auditabilidade.

A validação não pode ser compreendida como etapa pontual, restrita ao momento de desenvolvimento. Em sistemas baseados em inteligência artificial, a confiabilidade deve ser continuamente verificada ao longo de todo o ciclo de vida operacional (NIST, 2023; ISO/IEC 42001, 2023).

A ISO/IEC 42001 e o NIST AI Risk Management Framework estabelecem que sistemas de IA devem ser submetidos a monitoramento contínuo, avaliação de desempenho e gestão permanente de riscos (ISO/IEC 42001, 2023; NIST, 2023). Nesse cenário, Quality Assurance

assume função central na identificação de falhas sistêmicas, degradação de desempenho e vieses não previstos.

A auditabilidade algorítmica constitui elemento essencial desse processo. A capacidade de reconstruir decisões, compreender critérios utilizados e rastrear o comportamento do sistema permite não apenas a identificação de falhas, mas também a atribuição de responsabilidade institucional (PASQUALE, 2015).

Sem mecanismos adequados de validação e auditabilidade, a automação decisória torna-se opaca e juridicamente vulnerável. Essa vulnerabilidade se intensifica quando se considera que a confiabilidade do sistema não depende apenas do modelo utilizado, mas também dos dados que sustentam suas inferências.

A confiabilidade de sistemas baseados em inteligência artificial não decorre exclusivamente da estrutura do modelo, mas da qualidade e integridade dos dados que o alimentam.

Em sistemas de Compliance e AML, inconsistências, vieses ou lacunas nos dados utilizados podem influenciar diretamente os resultados produzidos, gerando classificações indevidas de risco e decisões potencialmente discriminatórias.

O NIST AI RMF reconhece que os riscos associados à inteligência artificial possuem natureza sociotécnica, podendo emergir tanto do modelo quanto dos dados e do contexto de uso (NIST, 2023).

Nesse cenário, mecanismos de governança de dados tornam-se indispensáveis.

A rastreabilidade e o data provenance, entendido como o registro da origem, do histórico e das transformações dos dados ao longo do tempo, permitem identificar a procedência das informações, acompanhar alterações ao longo do tempo e compreender quais informações influenciaram determinada decisão automatizada. Esses elementos são essenciais para viabilizar auditorias efetivas e garantir accountability.

A ausência de governança de dados compromete diretamente a capacidade de investigação de falhas e, consequentemente, a legitimidade do sistema. Além disso, mesmo quando dados e modelos são inicialmente validados, a natureza dinâmica dos sistemas de inteligência artificial exige acompanhamento permanente de seu comportamento ao longo do tempo.

Sistemas baseados em inteligência artificial são intrinsecamente dinâmicos e sujeitos à degradação de desempenho ao longo do tempo, em razão de mudanças nos padrões de dados e no contexto operacional (LU et al., 2019; GAMA et al., 2014).

Nesse contexto, a validação inicial do sistema não é suficiente para garantir sua confiabilidade contínua. A manutenção da qualidade depende da implementação de mecanismos permanentes de monitoramento e revalidação.

A observabilidade algorítmica permite acompanhar métricas de desempenho, detectar anomalias e identificar fenômenos como data drift, isto é, a mudança nos padrões dos dados de entrada, e model drift, isto é, a degradação do desempenho do modelo ao longo do tempo. Esses mecanismos são fundamentais para evitar que o sistema passe a produzir resultados inconsistentes sem detecção institucional.

Em ambientes regulatórios sensíveis, a ausência de monitoramento contínuo transforma falhas técnicas em riscos jurídicos concretos, ampliando a probabilidade de decisões indevidas com impacto sobre direitos fundamentais. Por essa razão, o Quality Assurance não atua apenas como instrumento de verificação técnica, mas também como mecanismo preventivo diante dos danos que podem decorrer da automação decisória.

Nesse sentido, a atuação do Quality Assurance deve ser compreendida como processo contínuo de gestão da confiabilidade, e não como etapa final de validação. Em sistemas automatizados de Compliance e AML, a qualidade precisa ser acompanhada desde a concepção do modelo até sua operação em ambiente real, considerando mudanças nos dados, no contexto regulatório e nos padrões de comportamento analisados. Essa perspectiva aproxima QA de uma lógica permanente de governança, na qual validar, monitorar, registrar evidências e revisar resultados tornam-se práticas indispensáveis para a manutenção da confiabilidade ao longo do ciclo de vida do sistema (NIST, 2023; ISO/IEC 42001, 2023).

A utilização de sistemas automatizados em processos de Compliance e AML introduz riscos concretos de produção de danos decorrentes de falhas algorítmicas.

Classificações indevidas, falsos positivos e bloqueios automáticos podem impactar diretamente a esfera jurídica dos indivíduos, restringindo o acesso a serviços financeiros e comprometendo a liberdade econômica.

Nesse cenário, Quality Assurance assume função preventiva. A implementação de processos estruturados de validação permite identificar inconsistências antes que se convertam em danos efetivos.

A ISO/IEC 23894 reforça essa perspectiva ao estabelecer diretrizes para gestão contínua de riscos em sistemas de IA (ISO/IEC 23894, 2023). Dessa forma, QA integra-se diretamente à governança de riscos, atuando como mecanismo de antecipação e mitigação de falhas.

A ausência de maturidade em QA, nesse contexto, não representa apenas deficiência técnica, mas um déficit de governança institucional. Essa dimensão institucional também exige que a confiabilidade seja analisada para além do desempenho técnico, incorporando critérios de explicabilidade, supervisão humana e aceitabilidade jurídica das decisões automatizadas.

Além disso, a avaliação da qualidade em sistemas automatizados de Compliance e AML deve considerar a proporcionalidade entre desempenho técnico e impacto jurídico das decisões produzidas. Um sistema pode apresentar métricas gerais satisfatórias e, ainda assim, gerar efeitos desproporcionais quando seus erros recaem sobre indivíduos ou grupos específicos. Por isso, a aceitabilidade de uma solução automatizada não deve ser medida apenas por acurácia, precisão ou redução de custos operacionais, mas também pela capacidade institucional de identificar falhas, justificar decisões, corrigir resultados indevidos e prevenir danos recorrentes (ISO/IEC 23894, 2023; NIST, 2023).

A confiabilidade técnica de sistemas automatizados não é suficiente, por si só, para legitimar decisões em ambientes regulatórios sensíveis.

A explicabilidade algorítmica constitui requisito fundamental para possibilitar revisão crítica, exercício do contraditório e contestação de decisões automatizadas. Sem capacidade mínima de compreensão do processo decisório, indivíduos afetados tornam-se incapazes de questionar eventuais erros (PASQUALE, 2015).

A supervisão humana, por sua vez, deve ser efetiva, e não meramente formal. A revisão de decisões automatizadas exige agentes capazes de compreender os limites e riscos do sistema, evitando a ocorrência de automation bias, caracterizado pela tendência de confiar excessivamente nas recomendações ou decisões produzidas por sistemas automatizados, sem revisão crítica (NIST, 2023; DOTAN et al., 2024).

Além disso, a aceitabilidade de sistemas automatizados não pode ser definida exclusivamente por métricas técnicas de desempenho. Mesmo níveis reduzidos de erro podem ser juridicamente inaceitáveis quando produzem impactos desproporcionais sobre direitos fundamentais (BARRETT et al., 2022).

Dessa forma, Quality Assurance assume papel de mediação entre eficiência tecnológica e legitimidade jurídica, contribuindo para a definição de critérios concretos de aceitabilidade em decisões automatizadas críticas.

5. CONCLUSÃO

Ao longo deste artigo, demonstrou-se que a expansão dos sistemas automatizados de Compliance e AML decorre de uma necessidade concreta de eficiência regulatória, sobretudo diante do volume massivo de dados, da complexidade das transações financeiras e da exigência de monitoramento contínuo. No entanto, também ficou evidenciado que a adoção de inteligência artificial nesses contextos não pode ser tratada como sinônimo de legitimidade, uma vez que a automatização decisória introduz riscos relevantes de opacidade, discriminação, falsos positivos e restrição indevida de direitos fundamentais.

A análise desenvolvida permitiu concluir que a confiança em decisões algorítmicas encontra limites jurídicos claros. Em ambientes regulatórios sensíveis, não basta que o sistema apresente desempenho satisfatório ou ganhos operacionais; é indispensável que existam transparência, explicabilidade, auditabilidade, rastreabilidade e supervisão humana efetiva. Esses elementos são fundamentais para preservar a legitimidade jurídica da automação, garantir possibilidade de revisão das decisões e assegurar compatibilidade com a LGPD, com a governança algorítmica e com a proteção de direitos fundamentais.

Nesse cenário, o Quality Assurance assume papel central e deixa de ser apenas uma prática técnica restrita ao desenvolvimento de software. Em sistemas baseados em inteligência artificial, a confiabilidade depende de validação contínua, monitoramento permanente, governança de dados, revalidação periódica e mecanismos capazes de detectar desvios de comportamento, degradação de desempenho, vieses e falhas sistêmicas ao longo de todo o ciclo de vida da solução. Assim, o QA passa a integrar a própria infraestrutura de governança algorítmica e a funcionar como instrumento de prevenção de danos e mitigação de riscos regulatórios.

Conclui-se, portanto, que a utilização de sistemas automatizados em Compliance e AML somente pode ser juridicamente aceitável quando acompanhada de controles robustos de qualidade, supervisão humana substancial e mecanismos eficazes de responsabilização. A eficiência tecnológica, por si só, não legitima decisões automatizadas em contextos de alto impacto. O desafio contemporâneo está em compatibilizar inovação, segurança regulatória e tutela de direitos,

reconhecendo que a automação pode ampliar a capacidade institucional de prevenção e controle, mas jamais substituir integralmente os parâmetros jurídicos que sustentam a validade das decisões em um Estado Democrático de Direito.

REFERÊNCIAS BIBLIOGRÁFICAS

BARRETT, Anthony M. et al. Actionable Guidance for High-Consequence AI Risk Management: Towards Standards Addressing AI Catastrophic Risks. arXiv preprint, 2022. Disponível em: https://arxiv.org/abs/2206.08966

BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2021.

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

DONEDA, Danilo. Da privacidade à proteção de dados pessoais: fundamentos da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Thomson Reuters Brasil, 2021.

DOTAN, Ravit et al. Evolving AI Risk Management: A Maturity Model based on the NIST AI Risk Management Framework. arXiv preprint, 2024. Disponível em: https://arxiv.org/abs/2401.15229

EUROPEAN UNION. Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Brussels: European Commission, 2021.

EUROPEAN UNION. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation – GDPR). Official Journal of the European Union, Brussels, 2016.

FATF. Financial Action Task Force. Guidance on Digital Identity. Paris: FATF/OECD, 2020.

FATF. Financial Action Task Force. International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. Paris: FATF/OECD, 2021.

FELDERER, Michael; RAMLER, Rudolf. The role of software testing in AI quality assurance. In: Quality of Information and Communications Technology (QUATIC). IEEE, 2021.

GAMA, João et al. A Survey on Concept Drift Adaptation. ACM Computing Surveys, v. 46, n. 4, 2014.

ISO/IEC 23894:2023. Artificial intelligence — Guidance on risk management. Geneva: International Organization for Standardization, 2023.

ISO/IEC 25059:2023. Software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Quality model for AI systems. Geneva: International Organization for Standardization, 2023. Disponível em: https://www.iso.org/standard/80655.html

ISO/IEC 42001:2023. Information technology — Artificial intelligence — Management system. Geneva: International Organization for Standardization, 2023. Disponível em: https://www.iso.org/standard/81230.html

LU, Jie et al. Learning under Concept Drift: A Review. IEEE Transactions on Knowledge and Data Engineering, v. 31, n. 12, 2019.

NIST. Artificial Intelligence Risk Management Framework (AI RMF 1.0). Gaithersburg: National Institute of Standards and Technology, 2023. Disponível em: https://nvlpubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf

O'NEIL, Cathy. Algoritmos de destruição em massa: como o big data aumenta a desigualdade e ameaça a democracia. Tradução de Rafael Abraham. Santo André: Rua do Sabão, 2020.

PASQUALE, Frank. The Black Box Society: the secret algorithms that control money and information. Cambridge: Harvard University Press, 2015.

RODOTÀ, Stefano. A vida na sociedade da vigilância: a privacidade hoje. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

SARLET, Ingo Wolfgang. A eficácia dos direitos fundamentais. 13. ed. Porto Alegre: Livraria do Advogado, 2021.

ZHANG, Jian et al. Machine Learning Testing: Survey, Landscapes and Horizons. IEEE Transactions on Software Engineering, v. 48, n. 1, 2022.

ZUBOFF, Shoshana. A era do capitalismo de vigilância. Tradução de George Schlesinger. Rio de Janeiro: Intrínseca, 2021.