Edition: Vol. 02 | Nº. 01 | (2026)
Publication: 31/03/2026
DOI: https://doi.org/10.70579/rfd.v2i1.149

Governança de IA em ambientes automatizados: impactos na cadeia de custódia e na integridade da prova digital

Governance of AI in automated environments: impacts on the custody chain and on the integrity of digital data

Gobernanza de IA en ambientes automatizados: impactos na cadeia de custódia e na integridade da prova digital

Mario Vieira Quevedo
LEC – Legal, Ethics & Compliance
Especialista em Governança, Riscos e Compliance (GRC)
São Paulo, SP – Brasil
mariovieiraquevedo@gmail.com

RESUMO
O artigo inicia abordando o conceito de ESG (Environmental, Social, and Governance), que se refere a práticas empresariais focadas na sustentabilidade ambiental, responsabilidade social e governança corporativa. Essas práticas são essenciais para empresas que desejam alinhar seus negócios com padrões éticos e sustentáveis. Paralelamente, discute a indústria farmacêutica OTC (Over-The-Counter) no Brasil, que engloba medicamentos vendidos diretamente ao consumidor sem necessidade de prescrição médica. Esta indústria enfrenta desafios únicos relacionados à sustentabilidade e responsabilidade social, tornando a integração das práticas ESG particularmente relevante. O principal objetivo do estudo é investigar como a implementação das práticas ESG pode influenciar e melhorar a responsabilidade previdenciária na indústria farmacêutica OTC no Brasil, contribuindo para um modelo de negócios mais sustentável e eticamente responsável. A metodologia adotada é bibliográfica, baseando-se na análise de literatura existente sobre as práticas ESG, a indústria farmacêutica OTC e a legislação previdenciária brasileira. Este método permite uma compreensão abrangente do tema através do estudo de publicações acadêmicas, relatórios de indústria e documentos governamentais. Os resultados mostram que a adoção de práticas ESG pela indústria farmacêutica OTC tem um impacto positivo na responsabilidade previdenciária. Isso se reflete em uma maior transparência, ética empresarial, e responsabilidade social. A conclusão enfatiza que a integração das práticas ESG é crucial para a sustentabilidade a longo prazo das empresas no setor, influenciando positivamente a sua interação com o sistema previdenciário e contribuindo para um desenvolvimento econômico mais sustentável e ético.

Edition: Vol. 02 | Nº. 01 | (2026)
Publication: 31/03/2026
DOI: https://doi.org/10.70579/rfd.v2i1.149

Palavras-chave: ESG, indústria farmacêutica OTC, responsabilidade previdenciária.

ABSTRACT
The article begins by addressing the concept of ESG (Environmental, Social, and Governance), which refers to business practices focused on environmental sustainability, social responsibility and corporate governance. These practices are essential for companies that want to align their businesses with ethical and sustainable standards. In parallel, it discusses the OTC (Over-The-Counter) pharmaceutical industry in Brazil, which encompasses medications sold directly to the consumer without the need for a medical prescription. This industry faces unique challenges related to sustainability and social responsibility, making the integration of ESG practices particularly relevant. The main objective of the study is to investigate how the implementation of ESG practices can influence and improve safety liability in the OTC pharmaceutical industry in Brazil, contributing to a more sustainable and ethically responsible business model. The bibliographical methodology is based on an analysis of existing literature on ESG practices, the OTC pharmaceutical industry and Brazilian regulatory legislation. This method allows a broad understanding of the subject through the study of academic publications, industry reports and government documents. The results show that the adoption of ESG practices by the OTC pharmaceutical industry has a positive impact on healthcare liability. This is reflected in greater transparency, business ethics, and social responsibility. The conclusion emphasizes that the integration of ESG practices is crucial for the long-term sustainability of non-sector companies, positively influencing their interaction with the pension system and contributing to a more sustainable and ethical economic development.

Keywords: ESG, OTC pharmaceutical industry, healthcare liability.

RESUMEN
El artículo inicia abordando el concepto de ESG (Environmental, Social, and Governance), que se refiere a prácticas empresariales enfocadas en sustentabilidad ambiental, responsabilidad social y gobernanza corporativa. Estas prácticas son esenciales para empresas que desean combinar sus negocios con padrones éticos y sustentables. Paralelamente, se discute una industria farmacéutica OTC (Over-The-Counter) en Brasil, que engloba medicamentos vendidos directamente al consumidor sin necesidad de prescripción médica. Esta industria enfrenta desafíos únicos relacionados con la sustentabilidad y la responsabilidad social, tornando a la integración de las prácticas ESG particularmente relevantes. El objetivo principal del estudio es investigar cómo la implementación de prácticas ESG puede influir y mejorar la responsabilidad previdenciária de la industria farmacéutica OTC en Brasil, contribuyendo para un modelo de negocios más sustentable y éticamente responsable. Una metodología adoptada y bibliográfica, basándose en el análisis de la literatura existente sobre las prácticas ESG,

Edition: Vol. 02 | Nº. 01 | (2026)
Publication: 31/03/2026
DOI: https://doi.org/10.70579/rfd.v2i1.149

la industria farmacéutica OTC y la legislación brasileña. Este método permite una comprensión abrangente del tema a través del estudio de publicaciones académicas, relaciones industriales y documentos gubernamentales. Los resultados muestran que la adopción de prácticas ESG en la industria farmacéutica OTC tiene un impacto positivo en la responsabilidad preventiva. Esto se refleja en una mayor transparencia, ética empresarial y responsabilidad social. La conclusión enfatiza que la integración de las prácticas ESG es crucial para la sustentabilidad a largo plazo de las empresas en el sector, influyendo positivamente en su interacción con el sistema preventivo y contribuyendo para un desarrollo económico más sustentable y ético.

Palavras-chave: ESG, industria farmacéutica OTC, responsabilidade previdenciária.

1 INTRODUÇÃO

A incorporação de sistemas de inteligência artificial aos ambientes corporativos, investigativos e operacionais transformou de maneira profunda a forma como evidências digitais são produzidas, processadas e interpretadas. O que antes se restringia a documentos estáticos, registros isolados ou artefatos periciais passou a decorrer de fluxos automatizados, modelos algorítmicos, pipelines de dados e infraestruturas distribuídas que operam em alta velocidade e por meio de múltiplas camadas de dependências técnicas. Em consequência, a dinâmica probatória deixa de gravitar exclusivamente em torno do vestígio final e passa a depender, cada vez mais, das condições técnicas em que esse resultado foi gerado.

Para profissionais que atuam em governança, riscos e *compliance*, inteligência de fontes abertas, segurança da informação, forense digital e gestão de riscos, essa mudança representa uma inflexão relevante. A evidência digital já não pode ser compreendida apenas como objeto, mas como resultado de um processo técnico contínuo, influenciado por versionamento de modelos, parâmetros de execução, logs, integrações com APIs, atualizações sistêmicas e condições operacionais específicas do ambiente no momento da coleta ou do processamento (Faccia, 2022; Paracrypt, 2021)

Essa realidade impõe revisão dos conceitos tradicionais de integridade, autenticidade e confiabilidade da prova digital. A cadeia de custódia, historicamente estruturada para lidar com vestígios materiais ou arquivos estáticos, mostra-se

Edition: Vol. 02 | Nº. 01 | (2026)
Publication: 31/03/2026
DOI: https://doi.org/10.70579/rfd.v2i1.149

insuficiente diante de sistemas que se atualizam continuamente, operam de forma distribuída e dependem de múltiplos componentes técnicos para gerar um único resultado. Nesses contextos, preservar apenas o artefato final não basta, porque a confiabilidade probatória passa a depender também da preservação documentada do processo que o originou (Wieteska, 2020; Williams, 2021)

Além disso, a crescente complexidade dos sistemas de IA introduz riscos adicionais à produção probatória, entre os quais se destacam a opacidade algorítmica, os vieses estatísticos, a dependência de dados externos, a mutabilidade dos modelos e as vulnerabilidades cibernéticas. Tais elementos podem comprometer a integridade da prova sem necessariamente deixar marcas visíveis no resultado final, razão pela qual a confiabilidade da evidência não pode mais ser aferida apenas pelo exame do arquivo produzido, mas pelo conjunto de registros técnicos que permitam reconstruir seu percurso de geração, processamento e armazenamento.

Nesse cenário, a discussão sobre cadeia de custódia adquire nova densidade jurídica. Se, no processo penal democrático, a validade da prova depende da preservação de sua integridade e da possibilidade de controle pelas partes, então a documentação de logs, metadados, parâmetros de execução, contexto operacional e versionamento de modelos deixa de ser mera exigência técnica e passa a integrar o próprio núcleo de validade probatória. A dogmática processual penal contemporânea já reconhece que a cadeia de custódia se relaciona diretamente ao contraditório substancial, à ampla defesa e ao devido processo legal, especialmente quando a fragilidade dos vestígios compromete a possibilidade de verificação independente por parte da defesa (Lopes Jr., 2023; Badaró, 2022)

É nesse contexto que o presente estudo examina os impactos da utilização de sistemas automatizados de inteligência artificial sobre a cadeia de custódia e sobre a integridade da prova digital. Parte-se da premissa de que, em ambientes automatizados, a preservação do resultado probatório exige também a preservação rastreável das condições técnicas de sua produção. Com isso, propõe-se uma compreensão ampliada da cadeia de

Edition: Vol. 02 | Nº. 01 | (2026)
Publication: 31/03/2026
DOI: https://doi.org/10.70579/rfd.v2i1.149

custódia, aqui tratada como cadeia de custódia digital expandida, apta a responder às exigências de ambientes corporativos e investigativos de alta complexidade.

Para enfrentar esse problema, o estudo adota um framework híbrido, que articula governança de IA, engenharia de modelos, forense digital e dogmática processual penal. No eixo técnico, mobilizam-se contribuições voltadas à compreensão de pipelines algorítmicos, mutabilidade, auditoria, rastreabilidade e preservação de registros em ambientes distribuídos (Faccia, 2022; Paracrypt, 2021; Wieteska, 2020; Williams, 2021). No eixo jurídico, o estudo dialoga com a disciplina da cadeia de custódia no Código de Processo Penal, com a teoria das nulidades, com o contraditório substancial e com a integridade probatória, à luz da doutrina processual penal contemporânea (Lopes Jr., 2023; Badaró, 2022; Kologeski, 2025)

O objetivo do estudo consiste em analisar de que modo a automação e a IA impactam a cadeia de custódia e a integridade da prova digital, propondo parâmetros teóricos e práticos para uma abordagem ampliada, capaz de atender às demandas de ambientes tecnológicos marcados por mutabilidade, opacidade e alta dependência sistêmica. Busca-se, assim, contribuir para a construção de um modelo de governança probatória compatível com as exigências de um processo penal democrático, no qual a inovação tecnológica permaneça subordinada às garantias fundamentais e ao controle jurídico da prova.

2 PROVA ALGORÍTMICA E TRANSFORMAÇÕES NA PRODUÇÃO DE EVIDÊNCIAS DIGITAIS

A incorporação de sistemas de inteligência artificial em ambientes corporativos, investigativos e operacionais produziu uma inflexão relevante na forma como evidências digitais são constituídas, tratadas e interpretadas. Em contraste com o paradigma tradicional, centrado em artefatos estáticos — como arquivos, registros isolados ou capturas periciais —, a evidência passa a emergir de fluxos automatizados, compostos

Edition: Vol. 02 | Nº. 01 | (2026)
Publication: 31/03/2026
DOI: https://doi.org/10.70579/rfd.v2i1.149

por múltiplas etapas técnicas interdependentes que condicionam diretamente sua confiabilidade.

Nesse contexto, a prova algorítmica não pode ser compreendida como um objeto finalizado, mas como resultado de um processo técnico contínuo, estruturado em pipelines de dados, modelos de machine learning, integrações sistêmicas e mecanismos automatizados de decisão. Tal mudança impõe não apenas a ampliação do olhar técnico, mas também a redefinição dos critérios jurídicos de validade da prova, uma vez que o resultado apresentado depende de variáveis que ultrapassam o próprio conteúdo do artefato produzido.

Para profissionais que atuam em governança, auditoria, segurança da informação, engenharia de dados e forense digital, essa transformação implica reconhecer que a confiabilidade probatória está diretamente vinculada à capacidade de reconstruir o fluxo técnico que originou a evidência. A literatura especializada destaca que sistemas automatizados operam sob condições de variabilidade contínua, nas quais parâmetros, versões de modelos e dependências externas podem alterar significativamente o comportamento do sistema, ainda que o output final aparente consistência formal (Faccia, 2022; Paracrypt, 2021)

Essa mudança estrutural desloca o eixo da análise probatória: deixa-se de avaliar exclusivamente o resultado para incorporar o exame das condições técnicas de sua produção. Em sistemas de IA, elementos como versionamento de modelos, qualidade dos dados de entrada, parâmetros de execução, logs de processamento e contexto operacional passam a integrar o núcleo da confiabilidade da evidência, exigindo documentação sistemática e mecanismos robustos de rastreabilidade (Wieteska, 2020; Williams, 2021)

Além disso, a produção algorítmica de evidências introduz desafios que não se manifestavam com a mesma intensidade em ambientes tradicionais. A opacidade dos modelos, especialmente em arquiteturas complexas, dificulta a compreensão dos critérios de decisão; a mutabilidade dos sistemas compromete a estabilidade dos resultados ao longo do tempo; e a dependência de dados externos e integrações amplia a exposição a

Edition: Vol. 02 | Nº. 01 | (2026)
Publication: 31/03/2026
DOI: https://doi.org/10.70579/rfd.v2i1.149

riscos operacionais e inconsistências técnicas. Esses fatores tornam insuficiente qualquer abordagem que se limite à análise do artefato final, exigindo, ao contrário, uma perspectiva que considere a evidência como expressão de um ecossistema técnico dinâmico.

Sob essa perspectiva, a prova algorítmica exige novos padrões de governança e validação, capazes de assegurar não apenas a integridade do resultado, mas também a verificabilidade do processo que o produziu. A literatura de governança de IA e forense digital converge no sentido de que a confiabilidade probatória depende da articulação entre rastreabilidade, reprodutibilidade, auditabilidade e segurança operacional, elementos que passam a constituir parâmetros mínimos para a aceitação de evidências produzidas em ambientes automatizados (Faccia, 2022; Wieteska, 2020).

Dessa forma, compreender as transformações na produção de evidências digitais não é apenas um exercício técnico, mas uma exigência jurídica. A redefinição da prova como processo impõe que categorias clássicas do direito probatório sejam reinterpretadas à luz das novas condições tecnológicas, abrindo espaço para a construção de modelos mais adequados à complexidade dos sistemas contemporâneos. É nesse cenário que se inserem as análises subsequentes, voltadas à compreensão dos mecanismos de produção da evidência algorítmica, das variáveis que afetam sua confiabilidade e dos riscos associados à opacidade e à assimetria informacional.

2.1 COMO SISTEMAS AUTOMATIZADOS PRODUZEM EVIDÊNCIAS

Os sistemas de inteligência artificial produzem evidências a partir de estruturas técnicas complexas, organizadas em pipelines de processamento que integram múltiplas etapas interdependentes. Diferentemente dos modelos tradicionais de produção probatória, em que o vestígio é identificado e preservado como um objeto relativamente estável, nos ambientes automatizados a evidência resulta de um encadeamento contínuo de operações que envolvem coleta, tratamento, processamento e registro de dados.

Edition: Vol. 02 | Nº. 01 | (2026)
Publication: 31/03/2026
DOI: https://doi.org/10.70579/rfd.v2i1.149

Esses pipelines, em termos operacionais, compreendem fases como a coleta automatizada de dados, o pré-processamento e normalização das informações, a inferência realizada por modelos de machine learning, a integração com serviços externos por meio de APIs, a execução de mecanismos de decisão automatizada e, por fim, a geração de logs, metadados e registros persistentes em ambientes distribuídos. Cada uma dessas etapas não apenas contribui para o resultado final, mas condiciona diretamente sua confiabilidade, na medida em que qualquer variação ao longo do fluxo pode alterar o comportamento do sistema (Floridi et al., 2018)

Nesse contexto, a evidência deixa de ser compreendida como um artefato isolado e passa a ser interpretada como expressão de um processo técnico contínuo. A literatura de forense digital demonstra que, em sistemas distribuídos, cada etapa do pipeline deixa rastros técnicos — como logs de execução, hashes, registros de chamadas de API e metadados — que constituem a base para a reconstrução do comportamento do sistema no momento da geração da evidência (Paracrypt, 2021)

Outro elemento central diz respeito à mutabilidade dos modelos de IA. Diferentemente de sistemas determinísticos clássicos, modelos de machine learning são constantemente atualizados, reconfigurados ou retreinados, o que implica que um mesmo conjunto de dados de entrada pode produzir resultados distintos ao longo do tempo. Essa variabilidade decorre de fatores como alterações nos parâmetros de execução, atualização de datasets, mudanças na arquitetura do modelo ou integração com novos componentes técnicos, configurando um cenário em que a estabilidade do resultado não pode ser presumida (Williams, 2021).

Além disso, a dependência de serviços externos e de componentes distribuídos amplia a complexidade do processo de produção da evidência. APIs, bibliotecas, serviços em nuvem e integrações com sistemas de terceiros introduzem variáveis que escapam ao controle direto da organização, podendo afetar desempenho, consistência e integridade dos resultados. A literatura especializada aponta que essas dependências constituem uma

Edition: Vol. 02 | Nº. 01 | (2026)
Publication: 31/03/2026
DOI: https://doi.org/10.70579/rfd.v2i1.149

das principais fontes de instabilidade em ambientes automatizados, exigindo mecanismos robustos de monitoramento e documentação (Wieteska, 2020)

Diante desse cenário, torna-se evidente que a produção de evidências em sistemas automatizados não pode ser analisada a partir de uma lógica linear ou estática. O resultado apresentado é sempre condicionado por um conjunto de variáveis técnicas que operam de forma simultânea e interdependente, o que exige uma abordagem metodológica capaz de capturar essa complexidade. Nesse sentido, a confiabilidade da prova algorítmica depende diretamente da capacidade de registrar, versionar e auditar cada etapa do pipeline, garantindo que o processo possa ser posteriormente reconstruído, verificado e contestado (Faccia, 2022).

Assim, a compreensão dos mecanismos de produção da evidência algorítmica constitui etapa fundamental para a redefinição dos critérios de validade probatória em ambientes automatizados. Mais do que identificar o resultado final, é necessário compreender o percurso técnico que o originou, pois é nesse percurso que se encontram os elementos determinantes para a avaliação de sua integridade, autenticidade e confiabilidade.

2.2 VARIÁVEIS TÉCNICAS QUE AFETAM A CONFIABILIDADE DA EVIDÊNCIA

A confiabilidade da evidência produzida por sistemas automatizados está diretamente condicionada a um conjunto de variáveis técnicas que atuam de forma simultânea e interdependente ao longo do pipeline de processamento. Diferentemente dos modelos tradicionais de produção probatória, nos quais a integridade pode ser aferida a partir da preservação do vestígio em si, nos ambientes baseados em inteligência artificial a validade da evidência depende da estabilidade e da rastreabilidade das condições técnicas que orientaram sua produção.

Entre essas variáveis, destaca-se inicialmente o versionamento de modelos e de componentes do sistema. Em ambientes de machine learning, modelos são frequentemente atualizados, retreinados ou substituídos, o que implica que pequenas

Edition: Vol. 02 | Nº. 01 | (2026)
Publication: 31/03/2026
DOI: https://doi.org/10.70579/rfd.v2i1.149

alterações na arquitetura, nos parâmetros ou nos dados de treinamento podem gerar resultados distintos a partir de entradas semelhantes. Essa característica compromete a reprodutibilidade da evidência quando não há controle rigoroso de versões, uma vez que a ausência de registro impede a reconstrução fiel do estado do sistema no momento da geração do resultado (Floridi et al., 2018)

Outro fator relevante refere-se à qualidade e à integridade dos dados de entrada. A evidência algorítmica é altamente sensível às características dos dados utilizados, de modo que inconsistências, ruídos, vieses ou manipulações podem afetar diretamente o output produzido. A literatura especializada ressalta que a confiabilidade de sistemas automatizados está intrinsecamente vinculada à governança dos dados, sendo indispensável garantir a origem, a integridade e a consistência das informações utilizadas no processamento (Paracrypt, 2021).

A mutabilidade dos sistemas também se apresenta como variável crítica. Em muitos contextos, modelos operam de forma adaptativa, incorporando novos dados ou ajustando seus parâmetros em tempo real. Essa capacidade, embora aumente a eficiência operacional, introduz instabilidade na produção probatória, uma vez que o comportamento do sistema pode variar ao longo do tempo, dificultando a reprodução dos resultados e a verificação independente por terceiros (Williams, 2021).

Além disso, a dependência de ambientes distribuídos e de serviços externos amplia significativamente a complexidade do processo. A integração com APIs, serviços em nuvem, bibliotecas e infraestruturas de terceiros insere variáveis que não estão sob controle direto dos operadores do sistema, podendo influenciar tanto o desempenho quanto a consistência dos resultados. Essa dependência exige mecanismos robustos de monitoramento e registro, capazes de documentar o estado do ambiente técnico em cada etapa do processamento (Wieteska, 2020).

Outro elemento que merece destaque é a configuração dos parâmetros de execução. Sistemas automatizados operam a partir de definições técnicas específicas — como thresholds, pesos, filtros e critérios de decisão — que influenciam diretamente o

Edition: Vol. 02 | Nº. 01 | (2026)
Publication: 31/03/2026
DOI: https://doi.org/10.70579/rfd.v2i1.149

resultado final. Alterações nesses parâmetros, mesmo que sutis, podem produzir impactos significativos na saída do sistema, o que torna indispensável o registro detalhado dessas configurações para fins de auditoria e validação.

A existência e a qualidade dos logs e metadados constituem, por sua vez, um dos principais pilares da confiabilidade da evidência digital. É por meio desses registros que se torna possível reconstruir o fluxo de processamento, identificar eventuais falhas, verificar a integridade das operações e assegurar a rastreabilidade do sistema. A ausência, inconsistência ou fragilidade desses registros compromete não apenas a análise técnica, mas também a própria validade jurídica da prova.

Sob a perspectiva jurídica, essas variáveis técnicas não podem ser tratadas como elementos periféricos. Ao contrário, passam a integrar o núcleo da integridade probatória, na medida em que condicionam a possibilidade de verificação, contestação e reprodução da evidência. Em um processo orientado pelo contraditório e pela ampla defesa, a impossibilidade de reconstruir as condições técnicas de produção da prova compromete sua confiabilidade e pode ensejar questionamentos quanto à sua admissibilidade (Lopes Jr., 2023).

Dessa forma, a análise das variáveis técnicas evidencia que a confiabilidade da prova algorítmica não reside apenas no resultado apresentado, mas na transparência e na rastreabilidade do processo que o originou. A incorporação dessas variáveis ao campo jurídico impõe a necessidade de redefinir os critérios tradicionais de validade probatória, incorporando elementos técnicos como parte integrante da avaliação da integridade da evidência em ambientes automatizados.

2.3 RISCOS TÉCNICOS: OPACIDADE, VIÉS E DEPENDÊNCIAS EXTERNAS

A incorporação de sistemas de inteligência artificial na produção de evidências digitais introduz um conjunto de riscos técnicos que impactam diretamente a confiabilidade probatória. Entre esses riscos, destacam-se a opacidade algorítmica, os vieses estatísticos e a dependência de infraestruturas externas, elementos que, embora

Edition: Vol. 02 | Nº. 01 | (2026)
Publication: 31/03/2026
DOI: https://doi.org/10.70579/rfd.v2i1.149

inerentes ao funcionamento desses sistemas, desafiam os modelos tradicionais de validação da prova no campo jurídico.

A opacidade algorítmica constitui um dos principais obstáculos à compreensão e ao controle das decisões produzidas por sistemas automatizados. Em modelos complexos, especialmente aqueles baseados em aprendizado profundo, os critérios utilizados para a geração de resultados não são facilmente acessíveis ou interpretáveis, o que dificulta a explicação do processo decisório. Essa limitação compromete a transparência da prova e fragiliza a possibilidade de verificação independente, elemento essencial em um sistema processual orientado pelo contraditório (Kroll et al., 2017).

A dificuldade de explicação não se restringe a aspectos técnicos, mas alcança também implicações jurídicas relevantes. Quando a lógica interna do sistema não pode ser plenamente reconstruída, a defesa encontra obstáculos para contestar o resultado apresentado, o que pode gerar assimetrias informacionais incompatíveis com o devido processo legal. Nesse sentido, a opacidade não é apenas um problema tecnológico, mas um fator que tensiona diretamente as garantias processuais, exigindo mecanismos de explicabilidade e auditabilidade capazes de mitigar esses efeitos.

Outro risco relevante refere-se à presença de vieses nos modelos de inteligência artificial. Sistemas treinados a partir de dados históricos podem reproduzir padrões discriminatórios, distorções estatísticas ou inconsistências presentes nos datasets utilizados, afetando a imparcialidade dos resultados. A literatura aponta que tais vieses podem se manifestar de forma sutil, influenciando decisões automatizadas sem que haja evidência explícita no resultado final, o que dificulta sua identificação e correção (Raji et al., 2020).

A presença de viés algorítmico assume relevância jurídica na medida em que pode comprometer a neutralidade da prova. Em contextos investigativos ou corporativos, decisões baseadas em modelos enviesados podem produzir evidências que não refletem adequadamente a realidade dos fatos, afetando a legitimidade do processo decisório. Esse cenário exige a adoção de práticas de governança que contemplem a avaliação contínua

Edition: Vol. 02 | Nº. 01 | (2026)
Publication: 31/03/2026
DOI: https://doi.org/10.70579/rfd.v2i1.149

dos modelos, a revisão dos dados utilizados e a implementação de mecanismos de mitigação de vieses.

A dependência de infraestruturas externas constitui outro fator de risco significativo. Sistemas automatizados frequentemente operam integrados a serviços de terceiros, como plataformas em nuvem, APIs, bibliotecas e bases de dados externas, o que amplia a complexidade do ambiente técnico e introduz variáveis que escapam ao controle direto dos operadores. Alterações nesses componentes — sejam elas decorrentes de atualizações, falhas ou mudanças contratuais — podem impactar o funcionamento do sistema e, consequentemente, a produção da evidência (Wieteska, 2020).

Essa dependência compromete a estabilidade e a previsibilidade dos resultados, especialmente quando não há mecanismos adequados de registro e monitoramento das condições operacionais. Em termos probatórios, a ausência de controle sobre esses elementos dificulta a reconstrução do ambiente técnico e fragiliza a confiabilidade da evidência, uma vez que não se pode assegurar que o resultado obtido seria reproduzível em condições equivalentes.

Além disso, esses riscos não atuam de forma isolada, mas frequentemente se combinam, potencializando seus efeitos. Um sistema opaco, treinado com dados enviesados e dependente de múltiplos serviços externos, tende a produzir resultados cuja confiabilidade é difícil de aferir, exigindo níveis elevados de controle e supervisão. Nesse contexto, a governança de IA assume papel central, na medida em que deve estruturar mecanismos capazes de reduzir a incerteza e assegurar padrões mínimos de transparência, rastreabilidade e responsabilidade.

Sob a perspectiva jurídica, a existência desses riscos impõe a necessidade de revisão dos critérios de admissibilidade e valoração da prova digital. A simples apresentação de um resultado produzido por sistema automatizado não pode ser considerada suficiente para atestar sua confiabilidade, sendo indispensável a demonstração das condições técnicas de sua produção e a possibilidade de sua verificação independente. A doutrina processual contemporânea já reconhece que a fragilidade dos

Edition: Vol. 02 | Nº. 01 | (2026)
Publication: 31/03/2026
DOI: https://doi.org/10.70579/rfd.v2i1.149

vestígios compromete sua validade probatória, especialmente quando impede o exercício pleno do contraditório (Lopes Jr., 2023).

Dessa forma, os riscos técnicos associados à inteligência artificial evidenciam que a prova algorítmica não pode ser analisada de maneira dissociada de seu contexto de produção. A confiabilidade da evidência depende da capacidade de identificar, compreender e mitigar esses riscos, o que exige a integração entre conhecimento técnico e jurídico. A superação desses desafios não implica rejeitar o uso de tecnologias automatizadas, mas condicioná-lo à observância de padrões rigorosos de governança e controle, compatíveis com as exigências de um processo orientado pela proteção de direitos fundamentais.

2.4 CADEIA DE CUSTÓDIA DIGITAL E DESAFIOS JURÍDICOS

A cadeia de custódia, tradicionalmente compreendida como o conjunto de procedimentos destinados a garantir a integridade, autenticidade e rastreabilidade dos vestígios probatórios, assume novos contornos diante da incorporação de sistemas automatizados e de inteligência artificial nos processos de produção de evidências digitais. No modelo clássico, sua função está associada à preservação de objetos materiais ou arquivos estáticos, cuja integridade pode ser assegurada por meio de técnicas de armazenamento, lacre, registro e documentação sequencial das etapas de manuseio.

Entretanto, em ambientes digitais contemporâneos, especialmente aqueles baseados em arquiteturas distribuídas e sistemas automatizados, essa concepção revela-se insuficiente. A evidência não se apresenta mais como um elemento isolado, mas como resultado de um processo técnico contínuo, dependente de múltiplas variáveis que atuam de forma simultânea e interdependente. Nesse contexto, a cadeia de custódia não pode se limitar à preservação do artefato final, devendo abranger também as condições técnicas que possibilitaram sua produção.

A doutrina processual penal contemporânea reconhece que a cadeia de custódia está diretamente vinculada à garantia do contraditório e da ampla defesa, na medida em

Edition: Vol. 02 | Nº. 01 | (2026)
Publication: 31/03/2026
DOI: https://doi.org/10.70579/rfd.v2i1.149

que assegura às partes a possibilidade de verificar a integridade do vestígio e contestar sua validade. A ruptura ou fragilidade dessa cadeia compromete a confiabilidade da prova, podendo ensejar sua desconsideração no âmbito processual (Lopes Jr., 2023; Badaró, 2022).

No entanto, quando se trata de evidências produzidas por sistemas de inteligência artificial, a noção de integridade precisa ser ampliada. Não se trata apenas de assegurar que o arquivo final não tenha sido adulterado, mas de garantir que o processo técnico que o originou seja rastreável, auditável e passível de reconstrução. Isso inclui a documentação de logs, metadados, parâmetros de execução, versões de modelos, dependências sistêmicas e condições operacionais do ambiente no momento da geração da evidência.

Essa ampliação conceitual conduz à ideia de uma cadeia de custódia digital expandida, na qual a integridade probatória passa a depender da preservação de um conjunto mais amplo de informações técnicas. A literatura de governança de sistemas digitais indica que, em ambientes complexos, a confiabilidade não está apenas no resultado, mas na capacidade de demonstrar como esse resultado foi produzido (Louis-Charles, 2024).

Além disso, a dinâmica dos sistemas automatizados introduz desafios adicionais à preservação da cadeia de custódia. A mutabilidade dos modelos, a atualização constante de sistemas, a dependência de serviços externos e a opacidade dos algoritmos dificultam a manutenção de um registro estável e completo do processo de produção da evidência. Esses fatores ampliam o risco de lacunas na documentação, o que pode comprometer a possibilidade de verificação independente e, consequentemente, a validade da prova.

Sob a perspectiva jurídica, essas limitações impõem a necessidade de revisão dos critérios tradicionais de admissibilidade probatória. A simples apresentação de um resultado produzido por sistema automatizado não é suficiente para assegurar sua confiabilidade, sendo indispensável a demonstração das condições técnicas que permitam

Edition: Vol. 02 | Nº. 01 | (2026)
Publication: 31/03/2026
DOI: https://doi.org/10.70579/rfd.v2i1.149

sua verificação. A ausência desses elementos pode configurar fragilidade na cadeia de custódia, afetando diretamente a força probatória do material apresentado.

A relação entre cadeia de custódia e nulidades processuais torna-se, nesse cenário, ainda mais relevante. A doutrina aponta que falhas na preservação da integridade da prova podem comprometer o devido processo legal, especialmente quando impedem o exercício pleno do contraditório (Badaró, 2022). Em ambientes automatizados, essas falhas podem não decorrer de manipulação intencional, mas de limitações técnicas ou ausência de governança adequada, o que exige uma abordagem mais sofisticada por parte do Direito.

Outro aspecto relevante refere-se à necessidade de integração entre diferentes áreas do conhecimento. A análise da cadeia de custódia digital exige não apenas domínio jurídico, mas também compreensão técnica dos sistemas envolvidos, o que impõe desafios à atuação de operadores do Direito. A construção de parâmetros adequados de validação probatória depende, portanto, da articulação entre saberes jurídicos e tecnológicos, permitindo uma avaliação mais precisa das condições de produção da evidência.

Dessa forma, a cadeia de custódia digital não pode ser tratada como mera extensão dos modelos tradicionais, mas como uma categoria em transformação, que exige atualização conceitual e normativa. A incorporação de tecnologias automatizadas demanda a construção de novos parâmetros de integridade probatória, capazes de assegurar que a inovação tecnológica não comprometa as garantias fundamentais que estruturam o processo penal democrático.

2.5 CADEIA DE CUSTÓDIA COMO GARANTIA DO CONTRADITÓRIO

A cadeia de custódia, no âmbito do processo penal, não se limita a um conjunto de procedimentos técnicos voltados à preservação de vestígios, mas constitui uma garantia essencial à efetivação do contraditório e da ampla defesa. Sua função ultrapassa a dimensão operacional, assumindo natureza jurídico-processual, na medida em que

Edition: Vol. 02 | Nº. 01 | (2026)
Publication: 31/03/2026
DOI: https://doi.org/10.70579/rfd.v2i1.149

assegura às partes a possibilidade de conhecer, verificar e contestar os elementos probatórios produzidos ao longo da persecução penal.

Sob essa perspectiva, a integridade da prova não pode ser compreendida apenas como ausência de adulteração material, mas como condição de verificabilidade. A cadeia de custódia, ao documentar o percurso do vestígio desde sua coleta até sua apresentação em juízo, permite que a defesa examine a regularidade dos procedimentos adotados, identifique eventuais falhas e questione a confiabilidade do material probatório. Trata-se, portanto, de instrumento que viabiliza o contraditório substancial, entendido como efetiva possibilidade de participação e influência das partes na formação da decisão judicial (Lopes Jr., 2023).

A doutrina processual penal contemporânea tem destacado que o contraditório não se esgota na mera ciência dos atos processuais, exigindo condições concretas para a contestação da prova. Nesse contexto, a fragilidade ou ruptura da cadeia de custódia compromete não apenas a integridade do vestígio, mas a própria legitimidade do processo, uma vez que impede a verificação independente dos elementos que fundamentam a acusação (Badaró, 2022).

Em ambientes digitais e automatizados, essa relação entre cadeia de custódia e contraditório assume contornos ainda mais complexos. A produção da evidência passa a depender de sistemas técnicos que operam com elevado grau de opacidade, mutabilidade e dependência de variáveis externas, o que dificulta a compreensão do processo que levou ao resultado apresentado. Nesses casos, a simples disponibilização do artefato final — como um relatório, um score ou um registro digital — não é suficiente para assegurar o exercício pleno do contraditório.

A efetivação do contraditório em provas algorítmicas exige, portanto, acesso às condições técnicas de produção da evidência. Isso inclui a disponibilização de logs, metadados, parâmetros de execução, versões de modelos e demais elementos que permitam reconstruir o funcionamento do sistema no momento da geração do resultado.

Edition: Vol. 02 | Nº. 01 | (2026)
Publication: 31/03/2026
DOI: https://doi.org/10.70579/rfd.v2i1.149

Sem esses dados, a defesa fica impossibilitada de avaliar a regularidade do processo, identificar possíveis falhas e questionar a validade da prova.

Essa exigência revela que a cadeia de custódia, em sua dimensão contemporânea, deve incorporar elementos técnicos que tradicionalmente não integravam o campo jurídico. A rastreabilidade sistêmica passa a ser condição para o exercício do contraditório, deslocando o foco da análise do objeto final para o processo que o originou. A ausência de documentação adequada não apenas compromete a integridade probatória, mas inviabiliza o controle jurídico da evidência.

Além disso, a opacidade dos sistemas de inteligência artificial pode gerar assimetrias informacionais entre acusação e defesa. Enquanto a parte que detém o controle sobre o sistema possui acesso privilegiado às informações técnicas, a defesa pode encontrar barreiras significativas para compreender e contestar o resultado apresentado. Esse desequilíbrio contraria os princípios estruturantes do processo penal democrático, exigindo a adoção de mecanismos que garantam transparência e acesso equitativo às informações relevantes.

A jurisprudência e a doutrina têm avançado no reconhecimento de que a ausência de condições para o exercício do contraditório pode comprometer a admissibilidade da prova. Em se tratando de evidências produzidas por sistemas automatizados, essa discussão ganha relevância adicional, uma vez que a impossibilidade de reconstrução do processo técnico pode impedir a verificação de sua confiabilidade. Assim, a cadeia de custódia deve ser compreendida como elemento central na avaliação da validade probatória, especialmente em contextos tecnológicos complexos.

Dessa forma, a relação entre cadeia de custódia e contraditório evidencia a necessidade de uma abordagem ampliada da integridade da prova digital. Não se trata apenas de preservar o vestígio, mas de assegurar que seu processo de produção seja transparente, rastreável e acessível às partes. A incorporação de tecnologias automatizadas impõe, portanto, a construção de novos parâmetros jurídicos, capazes de

Edition: Vol. 02 | Nº. 01 | (2026)
Publication: 31/03/2026
DOI: https://doi.org/10.70579/rfd.v2i1.149

garantir que a inovação não comprometa os direitos fundamentais que estruturam o processo penal.

2.6 NULIDADES, INTEGRIDADE E VALIDADE DA PROVA DIGITAL

A discussão acerca das nulidades processuais assume especial relevância no contexto da prova digital produzida por sistemas automatizados, na medida em que a integridade da evidência passa a depender de fatores técnicos que extrapolam os modelos tradicionais de preservação probatória. No processo penal, a validade da prova está diretamente vinculada à observância de garantias fundamentais, entre as quais se destacam o contraditório, a ampla defesa e o devido processo legal. A violação dessas garantias, especialmente quando compromete a possibilidade de verificação da prova, pode ensejar sua nulidade.

A doutrina processual penal estabelece que a nulidade decorre da inobservância de formas essenciais à garantia dos direitos das partes, não se tratando de mero formalismo, mas de instrumento de proteção contra arbitrariedades e falhas que comprometam a legitimidade do processo (Badaró, 2022). Nesse sentido, a integridade da prova não pode ser dissociada da regularidade dos procedimentos que conduziram à sua produção, sendo a cadeia de custódia elemento central para a aferição dessa regularidade.

No contexto da prova digital, a noção de integridade adquire dimensão ampliada. Não basta assegurar que o arquivo final não sofreu alterações; é necessário demonstrar que o processo técnico que o originou ocorreu de forma confiável, documentada e passível de reconstrução. A ausência de registros que permitam verificar as condições de produção da evidência compromete sua confiabilidade e pode configurar vício capaz de afetar sua validade jurídica.

Essa problemática torna-se ainda mais complexa quando a evidência é produzida por sistemas de inteligência artificial. A opacidade dos modelos, a mutabilidade dos

Edition: Vol. 02 | Nº. 01 | (2026)
Publication: 31/03/2026
DOI: https://doi.org/10.70579/rfd.v2i1.149

sistemas e a dependência de múltiplas variáveis técnicas dificultam a reconstrução do processo que levou ao resultado apresentado. Quando não há documentação adequada — como logs, metadados, parâmetros de execução e registros de versionamento —, a defesa fica impossibilitada de exercer controle efetivo sobre a prova, o que pode caracterizar violação ao contraditório substancial (Lopes Jr., 2023).

A ausência de rastreabilidade técnica, nesse cenário, não constitui mera irregularidade, mas pode configurar nulidade probatória, especialmente quando impede a verificação independente da evidência. A doutrina reconhece que a impossibilidade de reprodução ou contestação da prova compromete sua legitimidade, uma vez que impede a atuação efetiva da defesa e fragiliza o processo decisório (Badaró, 2022).

Além disso, a distinção entre nulidades absolutas e relativas ganha novos contornos em ambientes automatizados. Em situações nas quais a falha técnica compromete estruturalmente a possibilidade de controle da prova — como na ausência de registros essenciais para sua verificação —, tende-se a reconhecer a existência de nulidade absoluta, por afetar diretamente garantias fundamentais. Por outro lado, falhas que não inviabilizam a verificação da evidência podem ser tratadas como nulidades relativas, desde que demonstrado prejuízo à parte interessada.

Outro aspecto relevante refere-se à necessidade de redefinição dos critérios de valoração da prova digital. Em sistemas tradicionais, a análise probatória pode se concentrar no conteúdo do vestígio; entretanto, em ambientes automatizados, a confiabilidade do resultado depende da avaliação do processo técnico que o originou. Isso exige que o julgador considere não apenas o produto final, mas também as condições de sua produção, incorporando elementos técnicos à análise jurídica.

A literatura contemporânea aponta que a validade da prova digital está diretamente relacionada à sua auditabilidade e reprodutibilidade. A ausência desses elementos compromete a confiança no resultado e dificulta a formação de um juízo seguro sobre os fatos, especialmente quando a evidência exerce papel central na fundamentação

Edition: Vol. 02 | Nº. 01 | (2026)
Publication: 31/03/2026
DOI: https://doi.org/10.70579/rfd.v2i1.149

da decisão judicial. Nesse sentido, a integridade probatória passa a ser entendida como atributo que envolve tanto o resultado quanto o processo de sua produção.

A análise das nulidades no contexto da prova digital evidencia a necessidade de atualização da dogmática processual penal. A incorporação de tecnologias automatizadas impõe desafios que não podem ser enfrentados com categorias concebidas para realidades técnicas distintas. A construção de parâmetros adequados de validade probatória exige a integração entre conhecimento jurídico e técnico, permitindo que o Direito responda de forma eficaz às transformações decorrentes da digitalização e da automação.

Desta forma, a discussão sobre nulidades reforça a centralidade da cadeia de custódia digital como instrumento de garantia. Sua função não se limita à preservação formal da prova, mas abrange a asseguração das condições necessárias para sua verificação, contestação e valoração. Em um processo penal comprometido com a proteção de direitos fundamentais, a admissibilidade da prova digital deve estar condicionada à demonstração de sua integridade em sentido amplo, o que inclui a transparência e a rastreabilidade de todo o processo que levou à sua produção.

2.7 GOVERNANÇA DE IA E NOVOS PARÂMETROS DE CONTROLE PROBATÓRIO

A incorporação de sistemas de inteligência artificial na produção de evidências digitais exige a construção de novos parâmetros de controle probatório, capazes de responder às limitações dos modelos tradicionais de validação da prova. Nesse cenário, a governança de IA emerge como elemento central, não apenas como instrumento de gestão tecnológica, mas como mecanismo normativo voltado à garantia de integridade, transparência e responsabilidade na produção de evidências.

A governança de sistemas automatizados pressupõe a adoção de estruturas organizacionais e técnicas que assegurem o controle sobre todo o ciclo de vida dos sistemas, desde sua concepção até sua operação. No contexto probatório, isso implica a implementação de mecanismos capazes de documentar, monitorar e auditar os processos

Edition: Vol. 02 | Nº. 01 | (2026)
Publication: 31/03/2026
DOI: https://doi.org/10.70579/rfd.v2i1.149

que resultam na geração da evidência digital. A literatura especializada destaca que a confiabilidade de sistemas baseados em IA depende diretamente da capacidade de rastrear suas operações e de compreender as condições em que os resultados são produzidos (Kroll et al., 2017; Raji et al., 2020).

Entre os elementos centrais dessa governança, destaca-se a rastreabilidade sistêmica, entendida como a capacidade de reconstruir o percurso técnico da evidência desde sua origem até sua apresentação em juízo. Isso envolve a preservação de logs, metadados, parâmetros de execução, versões de modelos e registros de interação com sistemas externos, formando um conjunto de informações que permite verificar a integridade do processo de produção da prova.

A auditabilidade constitui outro pilar essencial. Sistemas utilizados para fins probatórios devem ser passíveis de auditoria independente, permitindo que terceiros — incluindo a defesa — possam examinar seu funcionamento e avaliar a confiabilidade dos resultados apresentados. A ausência de auditabilidade compromete a transparência do sistema e dificulta o exercício do contraditório, especialmente em contextos marcados por opacidade algorítmica.

A reprodutibilidade, por sua vez, assume papel fundamental na validação da prova digital. A possibilidade de reproduzir o resultado a partir das mesmas condições técnicas constitui um critério relevante para aferir a confiabilidade da evidência. Em sistemas automatizados, isso exige controle rigoroso de versões, documentação de parâmetros e preservação do ambiente técnico, evitando que alterações posteriores comprometam a verificação do resultado.

Além desses elementos, a governança de IA deve incorporar mecanismos de accountability, assegurando a identificação de responsáveis pelos sistemas e pelos resultados produzidos. A fragmentação da cadeia decisória em ambientes automatizados não pode resultar em diluição de responsabilidades, sendo necessário estabelecer estruturas claras de atribuição e controle, compatíveis com as exigências do ordenamento jurídico (Binenbojm, 2019).

Edition: Vol. 02 | Nº. 01 | (2026)
Publication: 31/03/2026
DOI: https://doi.org/10.70579/rfd.v2i1.149

Outro aspecto relevante refere-se à necessidade de integração entre governança técnica e controle jurídico. A implementação de mecanismos de rastreabilidade e auditabilidade deve estar alinhada aos princípios do devido processo legal, do contraditório e da ampla defesa, garantindo que a inovação tecnológica não comprometa direitos fundamentais. Nesse sentido, a governança de IA não pode ser concebida apenas como prática organizacional, mas como elemento integrante do sistema de garantias processuais.

A construção de novos parâmetros de controle probatório exige, portanto, uma abordagem interdisciplinar, capaz de articular conhecimentos técnicos e jurídicos. A prova digital produzida por sistemas automatizados demanda critérios de validação que considerem tanto o resultado quanto o processo de sua produção, incorporando elementos como transparência, rastreabilidade, auditabilidade e responsabilidade.

Nesse contexto, a noção de cadeia de custódia digital expandida ganha centralidade, funcionando como eixo estruturante de um modelo de governança probatória adequado aos ambientes automatizados. Ao incorporar dimensões técnicas ao conceito tradicional de cadeia de custódia, torna-se possível assegurar níveis mais elevados de confiabilidade e controle sobre a produção da evidência.

Por fim, a consolidação desses parâmetros representa não apenas uma resposta aos desafios tecnológicos, mas uma condição para a preservação da legitimidade do processo penal em um contexto de crescente digitalização. A utilização de sistemas de inteligência artificial não deve implicar flexibilização das garantias fundamentais, mas, ao contrário, exigir o fortalecimento dos mecanismos de controle, de modo a assegurar que a prova produzida seja confiável, verificável e juridicamente válida.

3 METODOLOGIA

A presente pesquisa caracteriza-se como um estudo de natureza qualitativa, com abordagem teórico-bibliográfica, voltado à análise crítica das transformações decorrentes

Edition: Vol. 02 | Nº. 01 | (2026)
Publication: 31/03/2026
DOI: https://doi.org/10.70579/rfd.v2i1.149

da incorporação de sistemas de inteligência artificial na produção de evidências digitais e seus impactos sobre a cadeia de custódia e a integridade probatória.

O percurso metodológico fundamenta-se na revisão e interpretação de literatura especializada, abrangendo produções acadêmicas nacionais e internacionais nas áreas de governança de inteligência artificial, forense digital, engenharia de dados e direito processual penal. A escolha por essa abordagem decorre da natureza do objeto investigado, que demanda articulação entre campos distintos do conhecimento, exigindo análise interdisciplinar capaz de integrar dimensões técnicas e jurídicas.

No eixo técnico, foram examinadas contribuições relacionadas ao funcionamento de sistemas automatizados, pipelines de dados, mutabilidade de modelos, rastreabilidade, auditabilidade e gestão de registros digitais, com o objetivo de compreender os mecanismos que estruturam a produção de evidências em ambientes automatizados. Essa análise permite identificar as variáveis técnicas que condicionam a confiabilidade da prova algorítmica e os riscos associados à sua utilização.

No eixo jurídico, a pesquisa dialoga com a doutrina processual penal contemporânea, especialmente no que se refere à cadeia de custódia, à teoria das nulidades, ao contraditório substancial e à integridade da prova. A análise jurídica busca examinar de que forma os conceitos tradicionais do direito probatório se comportam diante das transformações tecnológicas, bem como identificar lacunas e tensões decorrentes da aplicação desses institutos em contextos automatizados.

A estratégia metodológica adotada baseia-se na análise interpretativa e crítica das fontes selecionadas, com ênfase na identificação de convergências e divergências entre os referenciais técnicos e jurídicos. Não se trata, portanto, de uma pesquisa empírica, mas de um estudo analítico que busca construir uma compreensão ampliada do fenômeno investigado, a partir da articulação entre diferentes perspectivas teóricas.

Além disso, o estudo adota um framework analítico híbrido, estruturado em três eixos principais: (i) a análise da produção da evidência algorítmica e das variáveis técnicas que afetam sua confiabilidade; (ii) a reinterpretação da cadeia de custódia à luz

Edition: Vol. 02 | Nº. 01 | (2026)
Publication: 31/03/2026
DOI: https://doi.org/10.70579/rfd.v2i1.149

dos ambientes automatizados; e (iii) a proposição de parâmetros de governança e controle probatório compatíveis com as exigências do processo penal contemporâneo.

Por fim, a pesquisa assume caráter exploratório e explicativo, na medida em que busca não apenas descrever as transformações em curso, mas também compreender suas implicações jurídicas e propor caminhos teóricos para sua adequada regulação. A metodologia adotada, portanto, permite uma abordagem aprofundada e integrada do problema, contribuindo para o avanço das discussões sobre prova digital, inteligência artificial e garantias processuais.

4 RESULTADOS E DISCUSSÕES

A análise desenvolvida ao longo do estudo evidencia que a incorporação de sistemas de inteligência artificial na produção de evidências digitais promove uma transformação estrutural na forma como a prova é concebida, produzida e validada no âmbito jurídico. Os resultados apontam que a evidência algorítmica não pode mais ser compreendida como um artefato estático, mas como resultado de um processo técnico dinâmico, composto por múltiplas etapas interdependentes que condicionam diretamente sua confiabilidade.

Nesse sentido, verifica-se que a tradicional centralidade do vestígio final perde relevância diante da necessidade de compreensão do fluxo técnico que o originou. A análise dos referenciais técnicos demonstra que elementos como versionamento de modelos, qualidade dos dados de entrada, parâmetros de execução e registros de processamento constituem fatores determinantes para a integridade da evidência (Faccia, 2022; Paracrypt, 2021). Esse deslocamento implica uma redefinição do próprio conceito de prova, que passa a ser entendida como processo, e não apenas como produto.

No campo jurídico, os resultados indicam que essa transformação impacta diretamente a teoria da prova e os critérios de sua validade. A cadeia de custódia, concebida originalmente para assegurar a integridade de vestígios materiais ou digitais

Edition: Vol. 02 | Nº. 01 | (2026)
Publication: 31/03/2026
DOI: https://doi.org/10.70579/rfd.v2i1.149

estáticos, revela-se insuficiente diante da complexidade dos sistemas automatizados. A necessidade de incorporar elementos como logs, metadados, parâmetros e registros de versionamento evidencia a emergência de uma abordagem ampliada, aqui compreendida como cadeia de custódia digital expandida.

A discussão evidencia ainda que a confiabilidade da prova algorítmica está diretamente relacionada à possibilidade de sua verificação independente. A ausência de rastreabilidade e de documentação adequada compromete o exercício do contraditório, na medida em que impede a reconstrução do processo técnico que originou a evidência. Conforme aponta a doutrina processual penal, a impossibilidade de contestação efetiva da prova fragiliza sua validade e pode ensejar sua desconsideração (Lopes Jr., 2023; Badaró, 2022).

Outro resultado relevante refere-se à identificação dos principais riscos técnicos associados à produção de evidências por sistemas automatizados. A opacidade algorítmica, os vieses estatísticos, a mutabilidade dos modelos e a dependência de infraestruturas externas foram identificados como fatores que comprometem a previsibilidade e a confiabilidade dos resultados. Esses riscos, embora inerentes ao funcionamento dos sistemas, assumem relevância jurídica na medida em que podem afetar a integridade da prova sem deixar indícios visíveis no artefato final (Kroll et al., 2017; Raji et al., 2020).

A análise integrada entre técnica e direito evidencia que esses riscos não podem ser tratados como meras limitações operacionais, mas devem ser incorporados aos critérios de avaliação da prova. A confiabilidade probatória passa a depender da capacidade de identificar, documentar e mitigar essas variáveis, exigindo uma abordagem mais sofisticada por parte dos operadores do Direito.

No que se refere à teoria das nulidades, os resultados indicam que falhas na rastreabilidade e na documentação do processo técnico podem configurar vícios relevantes, especialmente quando comprometem o exercício do contraditório. A ausência de elementos que permitam a verificação independente da evidência pode ser interpretada

Edition: Vol. 02 | Nº. 01 | (2026)
Publication: 31/03/2026
DOI: https://doi.org/10.70579/rfd.v2i1.149

como violação de garantias fundamentais, aproximando-se das hipóteses de nulidade absoluta, por afetar diretamente a estrutura do processo (Badaró, 2022).

Além disso, a análise evidencia que a fragmentação da cadeia decisória em sistemas automatizados impõe desafios à atribuição de responsabilidade. A participação de múltiplos agentes — desenvolvedores, operadores, gestores e sistemas técnicos — dificulta a identificação de responsabilidades, exigindo a adoção de mecanismos de governança capazes de assegurar accountability e controle sobre o processo de produção da evidência (Binenbojm, 2019).

Por outro lado, os resultados também indicam que a utilização de sistemas automatizados pode ampliar a capacidade investigativa e a eficiência na análise de grandes volumes de dados. A aplicação de técnicas de inteligência artificial permite identificar padrões complexos, detectar inconsistências e reconstruir fluxos informacionais de maneira mais precisa. No entanto, esse ganho de eficiência não elimina a necessidade de controle jurídico, devendo ser acompanhado por mecanismos que garantam transparência, rastreabilidade e respeito às garantias processuais.

A discussão evidencia, portanto, que a incorporação da inteligência artificial no campo probatório produz uma tensão entre eficiência técnica e garantias jurídicas. De um lado, os sistemas automatizados ampliam a capacidade de produção e análise de evidências; de outro, introduzem riscos e limitações que desafiam os modelos tradicionais de validação da prova.

Nesse cenário, a governança de IA emerge como elemento central para a construção de novos parâmetros de controle probatório. A adoção de práticas voltadas à rastreabilidade, auditabilidade, reprodutibilidade e responsabilidade permitem reduzir a incerteza associada aos sistemas automatizados, contribuindo para a construção de um modelo de prova digital mais confiável e compatível com as exigências do processo penal contemporâneo.

Por fim, os resultados indicam que a superação dos desafios identificados não depende da rejeição das tecnologias automatizadas, mas da sua integração a um modelo

Edition: Vol. 02 | Nº. 01 | (2026)
Publication: 31/03/2026
DOI: https://doi.org/10.70579/rfd.v2i1.149

normativo capaz de assegurar o equilíbrio entre inovação e proteção de direitos fundamentais. A construção de uma abordagem ampliada da cadeia de custódia e a consolidação de práticas de governança de IA configuram, nesse contexto, caminhos necessários para a adaptação do Direito às transformações tecnológicas em curso.

9 CONCLUSÃO

A incorporação de sistemas de inteligência artificial na produção de evidências digitais representa uma inflexão relevante no campo do direito probatório, exigindo a revisão de categorias tradicionais à luz das novas condições tecnológicas. Ao longo deste estudo, demonstrou-se que a prova algorítmica não pode ser compreendida como um artefato isolado, mas como resultado de um processo técnico contínuo, condicionado por múltiplas variáveis que influenciam diretamente sua confiabilidade.

A análise evidenciou que a cadeia de custódia, tal como concebida nos modelos tradicionais, revela-se insuficiente diante da complexidade dos ambientes automatizados. A necessidade de incorporar elementos como logs, metadados, parâmetros de execução, versionamento de modelos e registros de processamento aponta para a construção de uma abordagem ampliada, aqui compreendida como cadeia de custódia digital expandida, capaz de assegurar níveis mais elevados de integridade e rastreabilidade da evidência.

No campo jurídico, verificou-se que a confiabilidade da prova digital está diretamente relacionada à possibilidade de sua verificação independente. A ausência de documentação adequada do processo técnico compromete o exercício do contraditório e da ampla defesa, afetando a validade da prova e podendo ensejar sua desconsideração. Nesse contexto, a integridade probatória passa a ser entendida não apenas como preservação do resultado, mas como transparência e auditabilidade do processo que o originou.

Além disso, a identificação de riscos técnicos — como opacidade algorítmica, vieses estatísticos, mutabilidade dos sistemas e dependência de infraestruturas externas

Edition: Vol. 02 | Nº. 01 | (2026)
Publication: 31/03/2026
DOI: https://doi.org/10.70579/rfd.v2i1.149

— evidencia que a utilização de tecnologias automatizadas introduz novas fontes de incerteza no campo probatório. Tais riscos, longe de serem meramente operacionais, assumem relevância jurídica, na medida em que podem comprometer a confiabilidade da evidência sem deixar marcas evidentes no resultado final.

Diante desse cenário, a governança de inteligência artificial emerge como elemento central para a construção de novos parâmetros de controle probatório. A adoção de práticas voltadas à rastreabilidade, auditabilidade, reprodutibilidade e accountability permite mitigar os riscos identificados e assegurar maior transparência na produção da evidência digital. A integração entre governança técnica e controle jurídico revela-se, portanto, condição indispensável para a preservação das garantias fundamentais no contexto de crescente automação.

Por fim, conclui-se que a adaptação do direito probatório às transformações tecnológicas não exige a rejeição dos sistemas automatizados, mas sua incorporação crítica e regulada. A construção de uma cadeia de custódia digital expandida e a consolidação de modelos de governança compatíveis com as exigências do processo penal contemporâneo configuram caminhos necessários para assegurar que a inovação tecnológica permaneça subordinada à proteção de direitos fundamentais, à transparência e ao controle jurídico da prova.

REFERÊNCIAS

BADARÓ, Gustavo Henrique Righi Ivahy. **Processo penal.** 8. ed. São Paulo: Revista dos Tribunais, 2022.

BINENBOJM, Gustavo. **Uma teoria do direito administrativo: direitos fundamentais, democracia e constitucionalização**. 3. ed. Rio de Janeiro: Renovar, 2019.

CASEY, Eoghan. **Digital evidence and computer crime: forensic science, computers and the internet**. 3. ed. Amsterdam: Academic Press, 2011.

CARRIER, Brian. **File system forensic analysis**. Boston: Addison-Wesley, 2005.

Edition: Vol. 02 | Nº. 01 | (2026)
Publication: 31/03/2026
DOI: https://doi.org/10.70579/rfd.v2i1.149

FACCIA, Alessio; MOSTEFAOUI, Ghita. Fraud detection and prevention using artificial intelligence: a systematic review. **Journal of Financial Crime,** v. 29, n. 3, p. 1–17, 2022.

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

KROLL, Joshua A. et al. Accountable algorithms. **University of Pennsylvania Law Review,** v. 165, n. 3, p. 633–705, 2017.

LOPES JR., Aury. **Direito processual penal.** 20. ed. São Paulo: Saraiva, 2023.

MITTELSTADT, Brent Daniel et al. The ethics of algorithms: mapping the debate. ***Big Data & Society***, v. 3, n. 2, 2016.

NIST. **Digital Evidence Guidelines**. Gaithersburg: National Institute of Standards and Technology, 2014.

POLLITT, Mark. An ad hoc review of digital forensic models. In: **Proceedings of the Second International Workshop on Systematic Approaches to Digital Forensic Engineering**. Washington: IEEE, 2007.

RAJI, Inioluwa Deborah et al. Closing the AI accountability gap: defining an end-to-end framework for internal algorithmic auditing. In: **Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency**. New York: ACM, 2020. p. 33–44.

VEALE, Michael; VAN KLEEK, Max; BINNS, Reuben. Fairness and accountability design needs for algorithmic support in high-stakes public sector decision-making. In: **Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems.** New York: ACM, 2018.