TECNOLOGIA E PROVA DIGITAL: DESAFIOS E PROPOSTAS PARA A CADEIA DE CUSTÓDIA NO JUDICIÁRIO

TECHNOLOGY AND DIGITAL EVIDENCE: CHALLENGES AND PROPOSALS FOR THE CHAIN OF CUSTODY IN THE JUDICIARY

Luiz Gabriel Batista Neves[1]
Fundação Visconde Cairu, FVC, Brasil
lgbneves@gmail.com

Hiuston César dos Santos Rosa[2]
Serviço Nacional de Aprendizagem Comercial, Senac, Brasil
hiustoncesar@gmail.com

DOI: https://doi.org/10.5281/zenodo.17914684

Resumo: A digitalização das relações sociais intensificou os desafios envolvendo a produção e a confiabilidade da prova digital no processo penal. A decisão da Quinta Turma do STJ, ao rejeitar *prints* coletados sem metodologia forense, reforça a importância da cadeia de custódia como garantia de autenticidade. Ferramentas como Cellebrite, Verifact, *blockchain* e inteligência artificial fortalecem a integridade e a rastreabilidade das evidências, embora suscitem preocupações éticas e de governança. O estudo aponta que padronização nacional, capacitação técnica e uso responsável da tecnologia são essenciais para conciliar eficiência investigativa e proteção de direitos fundamentais.

Palavras-chave: cadeia de custódia digital; Integridade probatória; inteligência artificial; *blockchain*; admissibilidade da prova.

Abstract: The digitalization of social interactions has heightened challenges related to the reliability of digital evidence in criminal proceedings. A recent ruling by Brazil's Superior Court of Justice, rejecting screenshots collected without forensic methodology, underscores the importance of maintaining a proper chain of custody. Tools such as Cellebrite, Verifact, blockchain and artificial intelligence enhance evidence integrity but raise ethical and governance concerns. This study concludes that national standardization, technical training and responsible technological adoption are essential to balancing investigative efficiency with the protection of fundamental rights.

Keywords: digital chain of custody; evidentiary integrity; artificial intelligence; blockchain; admissibility of evidence.

1. A fragilidade das provas digitais e a exigência de metodologia forense no STJ

A crescente digitalização das relações sociais e jurídicas tem trazido à tona desafios inéditos para o sistema de justiça, especialmente no que tange à produção, à admissibilidade, valoração e aos *standards* metodológicos de produção na prova digital. Em decisão paradigmática proferida em 2 de maio de 2024, a Quinta Turma do Superior Tribunal de Justiça (STJ) reafirmou a necessidade de rigor técnico na coleta de evidências digitais, ao rejeitar a utilização de capturas de tela (*prints*) de conversas de WhatsApp extraídas diretamente de um celular, sem o emprego de metodologia forense adequada (**Badaró**, 2024, p.7-9).

[1] Doutor em Direito pela Universidade Federal. Professor de Processo Penal da Fundação Visconde Cairu. Diretor do Instituto Brasileiro de Ciências Criminais (IBCCRIM). Ex-Presidente e Conselheiro do Instituto Baiano de Direito Processual Penal (IBADPP). ORCID: https://orcid.org/0000-0001-5236-6192. Currículo Lattes: http://lattes.cnpq.br/7040002320938435.

[2] MBA em Liderança, Inovação e Gestão 4.0 pela Pontifícia Universidade Católica do Rio Grande do Sul (PUC-RS). Bacharel em Ciência da Computação pela UNIPLI. Especialista em Inteligência Artificial. Possui certificações PMP, Cobit e ITIL. Atualmente é Assessor de Governança de TI do Departamento Nacional do Senac. ORCID: https://orcid.org/0009-0000-6029-9807. Currículo Lattes: http://lattes.cnpq.br/8531203266790093.

O caso envolvia uma organização criminosa, cujos integrantes foram investigados com base em prints obtidos pela polícia, sem qualquer documentação da cadeia de custódia ou do uso de ferramentas especializadas. O relator, ministro Joel Ilan Paciornik, destacou que a manipulação de dados digitais pode ocorrer de forma imperceptível, o que compromete a confiabilidade da prova. Assim, a decisão enfatizou que a ausência de laudo técnico e de registro formal das etapas de extração e preservação dos dados configura uma quebra da cadeia de custódia, inviabilizando sua utilização como prova válida no processo penal (**Badaró**, 2024).

A cadeia de custódia, nesse contexto, é o conjunto de procedimentos que assegura a autenticidade, a integridade e a rastreabilidade da prova, desde sua coleta até sua apresentação em juízo. A quebra dessa cadeia — como ocorreu no caso analisado — compromete a credibilidade da evidência, pois não há garantias de que os dados não foram alterados, corrompidos ou manipulados ao longo do processo (**Brasil**, 2025).

Essa posição do STJ representa um avanço na consolidação de critérios técnicos e jurídicos para a admissibilidade de provas digitais, alinhando-se às melhores práticas internacionais em matéria de segurança da informação e proteção de direitos fundamentais. A exigência de metodologia forense e de documentação rigorosa não apenas garante a integridade da prova, mas também resguarda o devido processo legal, evitando condenações baseadas em elementos potencialmente adulterados.

Essa decisão também oportuniza uma discussão sobre o papel das tecnologias inovadoras voltadas para a validação e preservação de provas em caráter digital. Soluções de IA podem ser aplicadas na detecção de violações ou alterações de arquivos, na validação de metadados e na identificação de incongruências. Por sua vez, o blockchain vem a ser uma alternativa eficaz para registrar, de forma confiável, às etapas da cadeia de custódia.

O Informativo 869 do STJ (**Brasil**, 2025) introduz uma distinção relevante: quando a coleta é feita por autoridade policial exige-se observância estrita à cadeia de custódia (arts. 158-A a 158-F do Código de Processo Penal — CPP); quando realizada por particular, os *prints* podem ser admitidos como prova, desde que não haja indícios de adulteração e sejam confirmados em juízo. Essa diferenciação busca equilibrar a proteção contra fraudes com a realidade prática, especialmente em casos de violência doméstica, nos quais a palavra da vítima assume especial relevância probatória, conforme a Jurisprudência em Teses 231 (**Brasil**, 2024a).

Essa evolução normativa reforça a importância da cadeia de custódia como garantia de confiabilidade, mas também reconhece situações em que a prova digital, mesmo sem metodologia forense, pode ser válida para proteger direitos fundamentais. No mesmo sentido, o STF, no Tema 237, consolidou o entendimento de que é lícita a gravação ambiental feita por um dos interlocutores, sem autorização judicial, quando destinada à defesa própria (**Brasil**, 2009).

Essa tese dialoga com a admissibilidade de *prints* obtidos por particulares, pois ambos os casos se fundamentam no exercício legítimo da ampla defesa.

2. A quebra da cadeia de custódia nas provas digitais: riscos, ferramentas e a realidade brasileira

A cadeia de custódia é um dos pilares da confiabilidade probatória no processo penal, seja nos casos em que as provas são obtidas através da autoridade policial ou quando é obtido por particular. No contexto das provas digitais, sua observância torna-se ainda mais crítica, dadas a volatilidade, a fragilidade e a facilidade de manipulação dos dados eletrônicos. A legislação brasileira, por meio dos artigos 158-A a 158-F do CPP, introduzidos pela Lei 13.964/2019 (Pacote Anticrime), estabelece os parâmetros para a preservação da integridade probatória desde a coleta até o descarte da evidência (**Brasil**, 1941).

Apesar dos avanços normativos, a implementação efetiva desses dispositivos ainda enfrenta obstáculos significativos no sistema de justiça brasileiro, sobretudo no âmbito das provas digitais. A inexistência de protocolos técnicos padronizados e a insuficiente capacitação dos agentes públicos têm contribuído para recorrentes quebras na cadeia de custódia, o que compromete a validade das evidências apresentadas e acentua a insegurança jurídica no processo penal (**Lima**, 2022).

2.1. Ferramentas forenses: Cellebrite e Verifact

Entre as ferramentas recomendadas para garantir a integridade das provas digitais, destacam-se Cellebrite e Verifact, ambas amplamente utilizadas para assegurar a cadeia de custódia e a autenticidade das evidências.

A Cellebrite é um *software* forense reconhecido internacionalmente, utilizado por órgãos de investigação no Brasil e no mundo. Ele permite a extração, análise e preservação de dados de dispositivos móveis, gerando relatórios detalhados e *hashes* criptográficos que comprovam a integridade das informações coletadas.

O Verifact, por sua vez, é uma solução nacional voltada para a lavratura de atas notariais digitais e validação de provas eletrônicas, utilizando recursos como registro em *blockchain* e certificação digital para garantir que os dados não sejam adulterados. Essa ferramenta é especialmente útil para validar *prints*, áudios e vídeos apresentados por particulares, conferindo robustez probatória.

O uso dessas ferramentas é essencial para evitar a quebra da cadeia de custódia, pois permite: a) extração sem alteração dos dados originais; b) geração de *logs* e relatórios técnicos detalhados; c) Preservação da cronologia da prova; d) Rastreabilidade e auditabilidade completa dos procedimentos.

Contudo, a realidade brasileira ainda apresenta desafios: o uso dessas soluções permanece restrito a núcleos especializados, como laboratórios de informática forense dos Ministérios Públicos e Polícias Civis. Em muitas delegacias e unidades judiciais, a coleta de provas digitais continua sendo feita de forma precária, com capturas de tela simples, cópias manuais e ausência de documentação técnica, o que aumenta o risco de nulidades processuais (**Reis Junior**, 2025).

2.2. A urgência da padronização nacional

A falta de um padrão normativo nos procedimentos levou o CNJ a promover uma discussão sobre a necessidade de padronizar a cadeia de custódia digital em nível nacional. Atores da área entendem que, não havendo uma instrução normativa coesa, as decisões judiciais tenderão a ser diferentes umas das outras, o que acarretará insegurança jurídica e dificultará a atuação das autoridades investigativas (**Pires; Costa**, 2025).

A Portaria 82/2014 da Secretaria Nacional de Segurança Pública, embora tenha estabelecido diretrizes para a cadeia de custódia, aplica-se apenas à Força Nacional. Já o CPP, mesmo após a reforma, ainda trata com mais profundidade os vestígios físicos, deixando lacunas quanto às provas digitais (**Pires; Costa**, 2025).

https://doi.org/10.5281/zenodo.17914684

2.3. *Blockchain* e inteligência artificial

No contexto de autenticidade, integridade e rastreabilidade das provas digitais, duas tecnologias vêm se consolidando como aliadas fundamentais do sistema de justiça: a inteligência artificial (IA) e o *blockchain*. A IA consiste em sistemas computacionais capazes de simular habilidades humanas, como análise, interpretação e tomada de decisão baseada em dados, contribuindo diretamente para a verificação técnica das evidências. Por sua vez, o blockchain representa uma estrutura digital descentralizada, responsável pelo registro de informações em blocos encadeados e imutáveis, assegurando que os dados permaneçam íntegros e não sejam alterados sem deixar vestígios. A sinergia entre essas tecnologias oferece mecanismos eficazes para validar provas digitais, especialmente diante dos riscos de manipulação e da quebra da cadeia de custódia, fortalecendo a segurança jurídica e a confiabilidade no processo judicial.

2.4. Blockchain como registro imutável de provas

O *blockchain* permite registrar evidências digitais de forma descentralizada e criptografada, criando um *hash* (algo como uma trilha auditável) que conserva a ordem temporal e, principalmente, a integridade dos dados. Cada etapa da coleta, armazenamento e exibição da prova pode ser devidamente documentada em blocos encadeados ou acorrentados (daí o nome *blockchain*, onde *block* significa bloco e *chain*, corrente), que são impossíveis de serem violados sem deixar vestígios.

Segundo **Costa** (2025), o *blockchain* atende aos requisitos do Código de Processo Civil, especialmente os artigos 369 e 441, que exigem meios legítimos e tecnicamente confiáveis para a produção de provas digitais. A lavratura de atas de constatação por advogados, quando registrada em *blockchain*, confere robustez probatória e segurança jurídica inquestionável (**Araújo**, 2023).

Além disso, estudos como o da Universidade Federal de Minas Gerais demonstram que o *blockchain* é compatível com os princípios da cadeia de custódia previstos no artigo 158-A do CPP, podendo ser utilizada para preservar vestígios digitais em investigações criminais.

2.5. IA na verificação técnica das provas

A IA contribui diretamente para a verificação da autenticidade das provas digitais, por meio de algoritmos capazes de: (i) analisar metadados de arquivos, identificando alterações, duplicações ou inconsistências; (ii) detectar manipulações em imagens, vídeos e documentos; (iii) classificar evidências com base em padrões de confiabilidade e jurisprudência; (iv) gerar relatórios técnicos automatizados, que podem ser anexados aos autos como suporte à admissibilidade da prova.

Essas funcionalidades são especialmente úteis em casos como o do *HC* 828.054/RN, julgado pelo STJ, em que a ausência de metodologia forense levou à anulação de *prints* de celular como prova. A IA poderia ter sido utilizada para verificar a integridade dos dados e identificar possíveis manipulações, enquanto o *blockchain* garantiria o registro imutável da coleta e preservação da prova.

2.6. Sinergia tecnológica: IA + *blockchain*

A integração entre IA e *blockchain* permite uma validação probatória completa, combinando: registro imutável da cadeia de custódia; verificação automatizada da integridade dos dados; auditoria contínua dos acessos e manipulações; classificação inteligente das evidências com base em jurisprudência e padrões técnicos.

Essa sinergia fortalece a segurança jurídica, reduz o risco de fraudes e aumenta a confiabilidade das provas digitais apresentadas em juízo, contribuindo para decisões mais justas e tecnicamente embasadas.

3. Desafios éticos da IA e do *blockchain* no Judiciário

A incorporação de tecnologias disruptivas como a IA e o *blockchain* ao sistema judiciário brasileiro tem gerado avanços significativos em termos de celeridade, eficiência e organização de dados. No entanto, esses benefícios vêm acompanhados de complexos desafios éticos, que exigem atenção redobrada por parte dos operadores do direito, legisladores e desenvolvedores de tecnologia (**Cunha**, 2024).

3.1. Proteção de dados e privacidade

A Lei Geral de Proteção de Dados (LGPD) estabelece, em seu artigo 20, o direito à revisão de decisões automatizadas. Isso implica que qualquer uso de IA no Judiciário deve respeitar os direitos fundamentais à privacidade e à autodeterminação informativa, especialmente em processos que envolvem dados sensíveis (**Brasil**, 2018).

O *blockchain* possui um paradoxo que merece atenção, pois, ao mesmo tempo em que oferece segurança da informação e imutabilidade, também traz à tona preocupações com a anonimização e rastreabilidade de dados pessoais. Ter os registros de forma descentralizada, como a tecnologia se propõe, torna a aplicação de princípios jurídicos, como o direito ao esquecimento, bastante difícil, fazendo com que seja necessário pensarmos em modelos híbridos de governança da informação.

3.2. Responsabilidade e *accountability*

A adoção de sistemas automatizados no Judiciário impõe a necessidade de definir claramente quem responde por erros ou abusos cometidos por algoritmos. A ausência de um marco regulatório específico para IA e *blockchain* no Brasil ainda gera insegurança jurídica. O PL 2.338/2023, em tramitação no Senado, busca estabelecer diretrizes para o desenvolvimento ético da IA, mas ainda carece de regulamentações setoriais voltadas ao Judiciário.

3.3. Capacitação e governança tecnológica

A superação desses desafios passa pela capacitação dos operadores do direito e pela criação de estruturas de governança tecnológica. É fundamental que magistrados, servidores e advogados compreendam o funcionamento das ferramentas digitais, participem da sua implementação e atuem como guardiões dos princípios constitucionais frente à inovação (**CNJ**, 2024).

4. Conclusão: inovação tecnológica e responsabilidade no Direito brasileiro

Conforme a decisão da Quinta Turma do STJ, que tratou da rejeição de provas digitais coletadas sem uma metodologia adequada, revelou-se a cautela existente e cada vez maior com a integridade e a confiabilidade das evidências no universo digital. O tom da decisão esclarece que o Judiciário brasileiro se mantém vigilante quanto às transformações tecnológicas e, principalmente, demonstra que estamos preparados para introduzi-las de forma gradual e estratégica no sistema de justiça do nosso País.

IA e *blockchain*, usados de maneira conjunta e integrada, podem resultar em soluções interessantes para gargalos históricos do

sistema de justiça, principalmente no que tange à perecibilidade das provas digitais. Não obstante, essas mesmas tecnologias trazem consigo novos dilemas éticos, que precisam ser regulados com perspicácia humana e, principalmente, devem ser acompanhados de constante capacitação e treinamento dos operadores do Direito.

Para que tenhamos um sistema de justiça transparente, justo e acessível a todos, é primordial fazer um uso responsável e consciente das novas tecnologias, sempre lançando mão de elementos como explicabilidade, proteção de dados, autonomia judicial e *accountability* (responsabilização). Vale ressaltar que, para atingirmos tal objetivo, precisamos ter sempre em mente que a inovação nunca pode se sobrepor à justiça em si. Ao contrário disso, ela deve potencializá-la, sempre respeitando os direitos fundamentais, para que a confiança da sociedade nas instituições seja fortalecida.

A conclusão de todo o assunto, considerando as abordagens anteriores, é que, em um futuro breve, o Direito terá, em sua atuação, a ética, a colaboração e a solidez técnica como premissas. Caberá a todos os atores envolvidos — juristas, profissionais de tecnologia da informação e da inovação, bem como gestores públicos — a missão de interligar a tradição jurídica às novas tecnologias, para que o progresso se transfigure em um sistema de justiça pleno.

Informações adicionais e declarações dos autores (integridade científica)

Declaração de conflito de interesses: os autores confirmam que não há conflitos de interesses na condução desta pesquisa e na redação deste artigo. **Declaração de autoria:** somente os pesquisadores que cumprem os requisitos de autoria deste artigo são listadas como autores; todos os coautores são totalmente responsáveis por este trabalho em sua totalidade.

Declaração de originalidade: os autores garantiram que o texto aqui publicado não foi publicado anteriormente em nenhum outro recurso e que futuras republicações somente ocorrerão com a indicação expressa da referência desta publicação original; eles também atestam que não há plágio de terceiros ou autoplágio.

Como citar (ABNT Brasil)

NEVES, Luiz Gabriel Batista; ROSA, Hiuston César dos Santos. Tecnologia e prova digital: desafios e propostas para a cadeia de custódia no Judiciário. *Boletim IBCCRIM*, São Paulo, v. 34, n. 398, p. 28-31, 2026. DOI: doi.org/10.5281/zenodo.17914684. Disponível em: https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/2654. Acesso em: 1 jan. 2026.

Referências

ARAÚJO, Matheus. Inteligência artificial, blockchain e a cadeia de custódia da prova no processo penal. *Revista da Universidade Federal de Minas Gerais*, Belo Horizonte, v. 30, e47605, 2023. Disponível em: https://periodicos.ufmg.br/index.php/revistadaufmg/article/view/47605/. Acesso em: 1 dez. 2025.

BADARÓ, Gustavo Henrique Righi Ivahy. Os standards metodológicos de produção na prova digital e a importância da cadeia de custódia. *Boletim IBCCRIM*, São Paulo, v. 29, n. 343, p. 7-9, 2024. Disponível em: https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/1325. Acesso em: 1 dez. 2025.

BRASIL. *Decreto-lei nº 3.689, de 3 de outubro de 1941*. Código de Processo Penal. Rio de Janeiro: Presidência da República, 1941. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm. Acesso em: 10 dez. 2025.

BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 10 dez. 2025.

BRASIL. Superior Tribunal de Justiça. *Informativo de Jurisprudência, n. 869, 4 nov. 2025*. Disponível em: https://processo.stj.jus.br/docs_internet/informativos/PDF/Inf0869.pdf. Acesso em: 10 dez. 2025.

BRASIL. Superior Tribunal de Justiça. *Jurisprudência em Teses*, n. 231, mar. 2024a. Disponível em: https://scon.stj.jus.br/SCON/GetPDFJT?edicao=231

BRASIL. Superior Tribunal de Justiça. Quinta Turma não aceita como provas prints de celular extraídos sem metodologia adequada. *Notícias do STJ*, 2 maio 2024b. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/2024/02052024-Quinta-Turma-nao-aceita-como-provas-prints-de-celular-extraidos-sem-metodologia-adequada.aspx. Acesso em: 1 dez. 2025.

BRASIL. Supremo Tribunal Federal. *Tema 237 - Gravação ambiental realizada por um dos interlocutores sem conhecimento do outro*. Brasília: STF, 2009.

CONSELHO NACIONAL DE JUSTIÇA. *Guia de boas práticas para o uso de IA no Judiciário*. Publicado em 2024.

COSTA, Daniela. *Blockchain* e prova digital: cumprindo os requisitos do CPC para autenticidade e cadeia de custódia. *Jusbrasil*, 11 mar. 2025. Disponível em: https://www.jusbrasil.com.br/artigos/blockchain-e-prova-digital-cumprindo-os-requisitos-do-cpc-para-autenticidade-e-cadeia-de-custodia/3163635953. Acesso em: 10 dez. 2025.

CUNHA, Marcos. Ética e Inteligência Artificial no Judiciário: desafios e perspectivas. *Revista Brasileira de Direito Digital*, v. 6, n. 2, 2024.

LIMA, Elpídio Júnior das Neves. A cadeia de custódia de provas digitais: efeitos jurídicos e práticos. *Revista CNMP*, 2022.

MACHADO, Ana Paula. *Blockchain* e privacidade: compatibilidades e tensões com a LGPD. *Revista de Direito*, v. 3, n. 1, 2023.

PIRES, Placidina; COSTA, Adriano Sousa. Necessidade de padronização pelo CNJ da cadeia de custódia da prova digital. *Consultor Jurídico*, 23 jul. 2025. Disponível em: https://www.conjur.com.br/2025-jul-23/necessidade-de-padronizacao-pelo-conselho-nacional-de-justica-da-cadeia-de-custodia-da-prova-digital/. Acesso em: 10 dez. 2025.

PRADO, Geraldo. *A cadeia de custódia no processo penal*. São Paulo: Marcial Pons, 2019.

REIS JUNIOR, Almir Santos; VARGAS, Ana Luiza Yumi. Cadeia de custódia nas provas digitais: desafios e estratégias para a preservação da integridade probatória. *Revista FSA*, Teresina, v. 22, n. 4, abr. 2025. Disponível em: http://www4.unifsa.com.br/revista/index.php/fsa/article/view/3100. Acesso em: 10 dez. 2025.