III CONGRESSO INTERNACIONAL DE DIREITO, POLÍTICAS PÚBLICAS, TECNOLOGIA E INTERNET

DIREITO PENAL E CIBERCRIMES I

D598
Direito penal e cibercrimes I [Recurso eletrônico on-line] organização III Congresso Internacional de Direito, Políticas Públicas, Tecnologia e Internet: Faculdade de Direito de Franca – Franca;

Coordenadores: Clóvis Alberto Volpe Filho, Helen Cristina de Almeida e Lucas Gonçalves da Silva – Franca: Faculdade de Direito de Franca, 2025.

Inclui bibliografia
ISBN: 978-65-5274-370-1
Modo de acesso: www.conpedi.org.br em publicações
Tema: Governança, regulação e o futuro da inteligência artificial.
1. Direito. 2. Políticas Públicas. 3. Tecnologia. 4. Internet. I. III Congresso Internacional de Direito, Políticas Públicas, Tecnologia e Internet (1:2025 : Franca, SP).

CDU: 34

III CONGRESSO INTERNACIONAL DE DIREITO, POLÍTICAS PÚBLICAS, TECNOLOGIA E INTERNET

DIREITO PENAL E CIBERCRIMES I

Apresentação

Entre os dias 30 de setembro e 3 de outubro de 2025, a Faculdade de Direito de Franca recebeu o III Congresso Internacional de Direito, Políticas Públicas, Tecnologia e Internet. O evento reuniu acadêmicos, profissionais, pesquisadores e estudantes, promovendo o debate interdisciplinar sobre o impacto das inovações tecnológicas no campo jurídico e nas políticas públicas. A programação envolveu Grupos de Trabalho (GTs) organizados para aprofundar temas específicos, abordando desde o acesso à justiça até as complexidades da regulação tecnológica, com ênfase na adaptação do sistema jurídico aos avanços da inteligência artificial e da automação.

O GT 9 examina as novas fronteiras do direito penal em meio à criminalidade virtual. As comunicações abordam o uso de reconhecimento facial, deepfakes e provas digitais, destacando riscos à privacidade e à integridade processual. O grupo busca construir parâmetros jurídicos que assegurem a proteção de direitos fundamentais diante dos desafios tecnológicos contemporâneos.

A CADEIA DE CUSTÓDIA E A CONFIABILIDADE DA PROVA DIGITAL NO PROCESSO PENAL: A APLICAÇÃO DA ABNT NBR ISO/IEC 27037:2013 COMO DIRETRIZ TÉCNICA DA PERÍCIA DIGITAL

THE CHAIN OF CUSTODY AND THE RELIABILITY OF DIGITAL EVIDENCE IN CRIMINAL PROCEEDINGS: THE APPLICATION OF ABNT NBR ISO/IEC 27037: 2013 AS A TECHNICAL GUIDELINE FOR DIGITAL FORENSICS

Caye Alves Costa
Marcelo Toffano

Resumo

Este trabalho analisa a importância da cadeia de custódia e da norma ABNT NBR ISO/IEC 27037:2013 no tratamento de provas digitais no processo penal. Dada sua fragilidade e fácil adulteração, é essencial adotar procedimentos que garantam a integridade e autenticidade dessas evidências. A união entre normas técnicas e jurídicas assegura a admissibilidade das provas, a proteção de direitos fundamentais e a legitimidade das decisões. A capacitação dos operadores do direito e a padronização dos procedimentos são indispensáveis. A pesquisa utilizou o método dedutivo, com abordagem documental e bibliográfica, para fundamentar teoricamente a análise desenvolvida.

Palavras-chave: Prova digital, Cadeia de custódia, Iso/iec 27037, Processo penal, Integridade da prova digital

Abstract/Resumen/Résumé

This study examines the importance of the chain of custody and the application of ABNT NBR ISO/IEC 27037:2013 in managing digital evidence in criminal proceedings. Due to its volatility and vulnerability to tampering, strict procedures are necessary to ensure the integrity and authenticity of such evidence. Integrating legal and technical standards is vital for admissibility, safeguarding fundamental rights, and ensuring judicial legitimacy. Training legal professionals and standardizing procedures are essential to strengthen criminal justice in the digital era. The research adopted the deductive method, using documentary and bibliographic techniques to support the theoretical basis of the proposed analysis.

Keywords/Palabras-claves/Mots-clés: Digital evidence, Chain of custody, Iso/iec 27037, Criminal procedure, Digital evidence integrity

1 INTRODUÇÃO

A digitalização das relações sociais impõe desafios significativos ao processo penal, especialmente no que tange à produção e à admissibilidade de provas digitais. A volatilidade e a facilidade de manipulação dessas evidências exigem rigorosos procedimentos para assegurar sua integridade e autenticidade.

No contexto atual, a crescente digitalização das interações humanas tem ampliado a relevância das evidências digitais no processo penal. A natureza volátil e facilmente manipulável dessas evidências impõe desafios significativos à sua admissibilidade e confiabilidade. Nesse cenário, a cadeia de custódia emerge como um instrumento essencial para assegurar a integridade e autenticidade das provas digitais.

A referida norma técnica internacional estabelece critérios e procedimentos que visam garantir que as evidências digitais sejam tratadas de forma padronizada e rastreável, desde a sua origem até a sua apresentação em juízo. Essa padronização é essencial para evitar alegações de quebra de integridade ou de contaminação da prova, o que poderia comprometer sua admissibilidade. No ordenamento jurídico brasileiro, a incorporação de práticas que assegurem a cadeia de custódia tornou-se ainda mais relevante com a positivação do instituto nos artigos 158-A a 158-F do CPP, os quais delimitam, de forma clara, as fases de controle da prova e as responsabilidades dos agentes envolvidos.

A pesquisa busca responder à seguinte questão de pesquisa: Em que medida a aplicação da norma ABNT NBR ISO/IEC 27037:2013 contribui para garantir a integridade, autenticidade e admissibilidade da prova digital no processo penal?

Este estudo analisa a relevância da cadeia de custódia e da aplicação das diretrizes técnicas estabelecidas pela ABNT NBR ISO/IEC 27037:2013 no tratamento das provas digitais no processo penal. Diante da volatilidade e da susceptibilidade à adulteração das evidências digitais, torna-se imprescindível a adoção de procedimentos rigorosos que assegurem sua integridade e autenticidade.

Para tanto, a pesquisa parte de uma abordagem doutrinária e normativa fazendo jus a técnica de pesquisa documental e bibliográfica, com análise de dispositivos legais, jurisprudência recente e padrões técnicos aplicáveis, buscando evidenciar a importância de uma atuação técnica e juridicamente qualificada no manejo das provas digitais.

O referencial teórico é composto por autores como Andrade (2017) e Lopes Jr. (2021), no campo do processo penal; Silva (2019), no que tange às provas digitais; e Rezende (2020) e

Tosta (2022), quanto à aplicação das normas técnicas da ISO no contexto da perícia digital. A análise demonstra que a implementação eficaz de protocolos técnicos reconhecidos internacionalmente como os previstos na ABNT NBR ISO/IEC 27037:2013 é condição indispensável para a confiabilidade da prova digital e sua validade no processo penal contemporâneo.

2 A prova digital no processo penal

2.1 O surgimento e a evolução da prova digital

A prova digital é aquela obtida ou gerada em ambiente eletrônico, como dados armazenados em dispositivos, comunicações eletrônicas e arquivos de mídia. Por ser intangível, volátil e facilmente alterável, exige cuidados técnicos específicos em sua coleta, preservação e análise.

Para ser aceita no processo penal, sua integridade e autenticidade devem ser garantidas desde a origem até sua apresentação em juízo, sob risco de violar princípios como o devido processo legal e a ampla defesa.

Entre suas peculiaridades estão a imaterialidade, a dependência de ferramentas específicas para acesso, a facilidade de modificação sem vestígios visíveis e a possibilidade de cópias idênticas ao original (ALBECHE, 2023).

A dispersão dos dados como em servidores na nuvem ou dispositivos móveis traz desafios quanto à competência jurisdicional e à apreensão. Por isso, peritos e autoridades devem seguir protocolos técnicos e legais para garantir a rastreabilidade e validade jurídica das provas (RIZZARDO, 2024; SILVA; OLIVEIRA, 2025).

2.2 A cadeia de custódia aplicada a prova digital

A cadeia de custódia, recentemente positivada no ordenamento jurídico brasileiro por meio da Lei nº 13.964/2019, representa um conjunto de procedimentos destinados a documentar, de forma contínua e ininterrupta, o histórico de manipulação da prova, desde sua obtenção até sua apresentação em juízo. No caso específico das provas digitais, a observância rigorosa desses procedimentos ganha contornos ainda mais relevantes, dada a vulnerabilidade dessas evidências à modificação, à destruição ou à contaminação.

De acordo com o artigo 158-B do Código de Processo Penal, a cadeia de custódia compreende o “conjunto de todos os procedimentos utilizados para manter e documentar a

história cronológica do vestígio coletado em locais ou em vítimas de infração penal" (BRASIL, 1941).

A aplicação da cadeia de custódia em ambiente digital requer, ainda, a utilização de ferramentas específicas que permitam a verificação de integridade dos dados, como os algoritmos de *hash* (funções de resumo criptográfico) (AVELAR et al., 2024) Tais mecanismos possibilitam a geração de códigos únicos associados a determinado conjunto de dados, de modo que qualquer alteração, por mínima que seja, modifique o valor *hash* correspondente, evidenciando a quebra da integridade da prova.

A inobservância da cadeia de custódia pode levar à exclusão da prova, por violar o contraditório, a ampla defesa e a legalidade processual. Aury Lopes Jr. sustenta que a quebra dessa cadeia gera a ilicitude da prova por derivação, tornando-a imprestável.

Do mesmo modo, Gustavo Badaró afirma que a ruptura compromete a autenticidade e a confiabilidade da evidência, enquanto Geraldo Prado a entende como um controle da "mesmidade" da prova cuja violação afeta o próprio valor epistêmico do elemento probatório. Guilherme Nucci, por sua vez, considera que a regulamentação da cadeia é um avanço, e sua inobservância pode acarretar nulidade processual.

Especialistas em provas digitais, como Avelar, Faucz, Sampaio, Gina Muniz, Kist, Furtado Mendes e Guimarães Mendes Neto, ressaltam que a fragilidade das evidências eletrônicas exige rigor absoluto. Falhas na verificação de integridade (como ausência de hash), documentação incompleta ou transporte inadequado comprometem a admissibilidade da prova e a própria busca pela verdade real.

A cadeia de custódia envolve etapas como: reconhecimento, isolamento, fixação, coleta, acondicionamento, transporte, recebimento, processamento, armazenamento e descarte, conforme os arts. 158-B a 158-F do CPP (BRASIL, 1941). Cada fase deve ser devidamente documentada, com identificação dos responsáveis e dos procedimentos adotados.

A afirmação de que a natureza volátil das evidências digitais eleva a cadeia de custódia a um papel ainda mais crítico é um consenso inegável na doutrina contemporânea, e por razões que transcendem a mera formalidade. Diferentemente das provas físicas, que possuem uma tangibilidade e uma resistência intrínseca à manipulação, os dados digitais são caracterizados por sua extrema mutabilidade e fragilidade. Um simples erro na coleta, um lapso na documentação, um manuseio inadequado ou mesmo uma falha na preservação do ambiente digital de onde foram extraídos podem, de fato, alterar irreversivelmente a essência da evidência. Essa vulnerabilidade inerente compromete sua integridade e, consequentemente, sua validade em juízo. Qualquer falha nesse processo meticuloso tem o potencial de levar à

inadmissibilidade da prova, um desfecho que impacta diretamente a eficácia da persecução penal e a busca pela verdade, podendo, inclusive, culminar em absolvições por insuficiência ou ilicitude probatória.

Nesse contexto de fragilidade e necessidade de rigor, a visão crítica de Alexandre Morais da Rosa assume particular relevância. Com sua abordagem que integra a Teoria dos Jogos e a Hermenêutica Filosófica, Morais da Rosa sublinha que a construção da verdade no processo penal é um ato complexo, permeado por vieses cognitivos e suscetível a manipulações. Para ele, a cadeia de custódia, especialmente no ambiente digital, não é apenas um protocolo técnico-legal, mas um requisito epistemológico fundamental para a validade do conhecimento que a prova pode gerar. Em suas palavras, negligenciar a cadeia de custódia em um ambiente tão frágil como o digital é abrir mão da segurança sobre a origem e integridade da prova, comprometendo a legitimidade do resultado e a própria justiça do "jogo" processual. A transparência e a auditabilidade de cada passo na custódia da evidência digital tornam-se, assim, um requisito indispensável para evitar que a decisão judicial seja baseada em elementos duvidosos, forjados ou contaminados, resguardando a integridade do processo e a confiança na administração da justiça.

2.3 A ABNT NBR ISO/IEC 27037:2013 como Diretriz Técnica

A adoção da ABNT NBR ISO/IEC 27037:2013 proporciona maior segurança jurídica, reduzindo o risco de contaminação ou adulteração das provas digitais. Além disso, promove a padronização dos procedimentos periciais, facilitando a cooperação entre diferentes órgãos e jurisdições

A ABNT NBR ISO/IEC 27037:2013 estabelece diretrizes específicas para o tratamento de evidências digitais, abordando aspectos como: a identificação: determinação de dados ou dispositivos que possam conter informações relevantes para a investigação; coleta: Extração de dados de maneira que preserve sua integridade, utilizando métodos forenses apropriados; aquisição: Criação de cópias forenses dos dados, garantindo que os originais permaneçam inalterados; preservação: armazenamento seguro das evidências, com documentação detalhada de todas as ações realizadas.

Apesar das diretrizes estabelecidas, a aplicação prática da cadeia de custódia em evidências digitais enfrenta desafios, como: capacitação técnica: necessidade de profissionais treinados em técnicas forenses digitais para realizar a coleta e análise adequadas; infraestrutura adequada: disponibilidade de ferramentas e ambientes seguros para o armazenamento e análise

de dados digitais; padronização de procedimentos: implementação uniforme das diretrizes da ISO/IEC 27037:2013 em todas as fases da investigação e processamento judicial. A ausência de uma abordagem padronizada pode comprometer a admissibilidade das provas e, consequentemente, a efetividade da justiça penal.

Além disso, é importante considerar o papel da tecnologia na modernização da prática jurídica. A integração de ferramentas tecnológicas, como softwares de análise forense e sistemas de gerenciamento de evidências, pode otimizar os processos e aumentar a eficiência das investigações.

Por fim, a ABNT NBR ISO/IEC 27037:2013 não é apenas uma norma técnica; ela representa um compromisso com a justiça e a verdade. A sua adoção e implementação rigorosa são fundamentais para assegurar que as evidências digitais sejam tratadas de maneira adequada, contribuindo para a efetividade do sistema penal e a proteção dos direitos fundamentais dos cidadãos. Assim, todos nós, como operadores do direito, temos a responsabilidade de promover e defender a integridade das evidências digitais, assegurando que a justiça prevaleça em um mundo cada vez mais digitalizado.

2.4 Consequências da inobservância das diretrizes técnicas e legais

A inobservância das diretrizes da ABNT NBR ISO/IEC 27037:2013 e das normas legais sobre cadeia de custódia pode comprometer a admissibilidade da prova digital no processo penal, ensejando sua exclusão com base na teoria dos frutos da árvore envenenada. Esta doutrina, oriunda do direito norte-americano e consolidada pela Suprema Corte dos EUA, veda o uso de provas derivadas de obtenção ilícita, por violarem o devido processo legal e os direitos fundamentais.

No Brasil, essa teoria foi incorporada ao ordenamento jurídico, especialmente através do princípio da legalidade e do devido processo legal, previstos na Constituição Federal. A aplicação da teoria no contexto brasileiro é vista como uma forma de garantir a proteção dos direitos fundamentais, assegurando que provas obtidas em desacordo com a legislação ou normas técnicas, como as da ABNT NBR ISO/IEC 27037:2013, sejam desconsideradas no âmbito do processo penal.

Essa integração de uma teoria estrangeira à legislação brasileira demonstra a flexibilidade do direito brasileiro em absorver conceitos que visam a proteção dos direitos humanos e a integridade do processo penal, refletindo um compromisso com a justiça e a legalidade. O uso da teoria dos frutos da árvore envenenada, portanto, é um mecanismo

importante para a salvaguarda dos direitos fundamentais no Brasil, evitando que práticas ilegais contaminem o sistema judicial (LOPES, JR. AURY, 2021)

Além da inadmissibilidade da prova, a inobservância dos protocolos de integridade e autenticidade pode comprometer toda a linha probatória construída com base em elementos digitais, gerando nulidades processuais e afetando diretamente a formação do convencimento judicial.

Em especial o Superior Tribunal de Justiça já estabeleceu em seu AEARESP 2342908 (AgRg nos EDcl no AREsp 2342908 / MG) que a cadeia de custódia deve ser mantida para assegurar que os dados coletados correspondam exatamente àqueles analisados e apresentados em juízo sendo que a falta de apresentação dos códigos hash impossibilitou a verificação da integridade das provas, levando à conclusão de que são inadmissíveis as evidências extraídas sem essa garantia, assim as provas foram consideradas inadmissíveis devido à quebra da cadeia de custódia.

Portanto, a aplicação das diretrizes técnicas da ABNT NBR ISO/IEC 27037:2013, aliada ao cumprimento rigoroso dos dispositivos legais que regem a cadeia de custódia, constitui requisito indispensável para assegurar a higidez das provas digitais. Trata-se de um imperativo tanto jurídico quanto técnico, cuja inobservância pode não apenas comprometer a admissibilidade da prova, mas também violar garantias constitucionais fundamentais, como o contraditório, a ampla defesa e a presunção de inocência.

3 CONCLUSÃO

A confiabilidade da prova digital no processo penal exige o rigor na cadeia de custódia e a aplicação de diretrizes técnicas, como a ABNT NBR ISO/IEC 27037:2013. A integração entre normas jurídicas e padrões técnicos assegura a integridade das evidências digitais, protegendo direitos fundamentais e fortalecendo a justiça penal.

Diante da crescente digitalização das relações, o sistema de justiça precisa adaptar-se, garantindo segurança jurídica sem comprometer a eficácia da persecução penal. O correto manuseio das provas digitais da coleta à valoração depende do domínio jurídico e técnico sobre os procedimentos.

A falta de conformidade com esses padrões compromete não só a admissibilidade da prova, mas a credibilidade do Judiciário. Por isso, é urgente investir em capacitação, tecnologia forense e protocolos operacionais unificados.

Conclui-se que o tratamento da prova digital deve ser interdisciplinar, unindo Direito

e tecnologia, em respeito ao Estado de Direito e às garantias constitucionais. A conformidade técnica não é mero formalismo é compromisso com a justiça.

REFERÊNCIAS

ACADEMIA DE FORENSE DIGITAL. ISO 27037: diretrizes para identificação, coleta, aquisição e preservação de evidência digital. Disponível em: https://academiadeforensedigital.com.br/iso-27037-identificacao-coleta-aquisicaoepreservacao-de-ev. Acesso em: 10 abr. 2025.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). NBR ISO/IEC 27037: diretrizes para identificação, coleta, aquisição e preservação de evidência digital. Rio de Janeiro, 2013. Disponível em: https://www.abntcatalogo.com.br/norma.aspx?ID=307273. Acesso em: 11 maio 2025.

AVELAR, Daniel Ribeiro Surdi de; FAUCZ, Rodrigo; SAMPAIO, Denis; MUNIZ, Gina. **Sistema de justiça criminal: cadeia de custódia no contexto das provas digitais**. 2024. Disponível em: https://www.conjur.com.br/2024-mar-30/cadeia-de-custodia-da-prova-digital/. Acesso em: 04 jul. 2025.

BITENCOURT, Cezar Roberto. Tratado de direito penal: parte geral 1. 15. ed. rev., atual. e ampl. São Paulo: Saraiva, 2010.

BERTOLUCCI, Maria Cristina. A cadeia de custódia das provas digitais: desafios e perspectivas. Revista Brasileira de Direito Processual Penal, São Paulo, v. 4, n. 2, p. 325-352, 2020.

BRASIL. Código penal. Decreto-lei nº 2.848, de 7 de dezembro de 1940. Diário Oficial [da] República Federativa do Brasil, Rio de Janeiro, 7 dez. 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm.

BRASIL. Decreto-Lei nº 3.689, de 3 de outubro de 1941. Código de Processo Penal. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm. Acesso em: 15 maio 2025.

INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO (ITI). Cartilha de segurança para internet: evidências digitais e cadeia de custódia. Brasília: ITI, 2023. Disponível em: https://cartilha.cert.br/. Acesso em: 4 jul. 2025.

LOPES Jr., Aury. Direito processual penal. 18. ed. São Paulo: Saraiva Educação, 2021.

SOUZA, Ricardo Luiz Gebrim de. Provas digitais e a cadeia de custódia no processo penal brasileiro. Rio de Janeiro: Juspodivm, 2021.