

IX ENCONTRO VIRTUAL DO CONPEDI

CRIMINOLOGIAS E POLÍTICA CRIMINAL II

Todos os direitos reservados e protegidos. Nenhuma parte destes anais poderá ser reproduzida ou transmitida sejam quais forem os meios empregados sem prévia autorização dos editores.

Diretoria - CONPEDI

Presidente - Profa. Dra. Samyra Haydêe Dal Farra Napolini - FMU - São Paulo

Diretor Executivo - Prof. Dr. Orides Mezzaroba - UFSC - Santa Catarina

Vice-presidente Norte - Prof. Dr. Jean Carlos Dias - Cesupa - Pará

Vice-presidente Centro-Oeste - Prof. Dr. José Querino Tavares Neto - UFG - Goiás

Vice-presidente Sul - Prof. Dr. Leonel Severo Rocha - Unisinos - Rio Grande do Sul

Vice-presidente Sudeste - Profa. Dra. Rosângela Lunardelli Cavallazzi - UFRJ/PUCRio - Rio de Janeiro

Vice-presidente Nordeste - Prof. Dr. Raymundo Juliano Feitosa - UNICAP - Pernambuco

Representante Discente: Prof. Dr. Abner da Silva Jaques - UPM/UNIGRAN - Mato Grosso do Sul

Conselho Fiscal:

Prof. Dr. José Filomeno de Moraes Filho - UFMA - Maranhão

Prof. Dr. Caio Augusto Souza Lara - SKEMA/ESDHC/UFMG - Minas Gerais

Prof. Dr. Valter Moura do Carmo - UFERSA - Rio Grande do Norte

Prof. Dr. Fernando Passos - UNIARA - São Paulo

Prof. Dr. Edinilson Donisete Machado - UNIVEM/UENP - São Paulo

Secretarias

Relações Institucionais:

Prof. Dra. Claudia Maria Barbosa - PUCPR - Paraná

Prof. Dr. Heron José de Santana Gordilho - UFBA - Bahia

Profa. Dra. Daniela Marques de Moraes - UNB - Distrito Federal

Comunicação:

Prof. Dr. Robison Tramontina - UNOESC - Santa Catarina

Prof. Dr. Liton Lanes Pilau Sobrinho - UPF/Univali - Rio Grande do Sul

Prof. Dr. Lucas Gonçalves da Silva - UFS - Sergipe

Relações Internacionais para o Continente Americano:

Prof. Dr. Jerônimo Siqueira Tybusch - UFSM - Rio Grande do Sul

Prof. Dr. Paulo Roberto Barbosa Ramos - UFMA - Maranhão

Prof. Dr. Felipe Chiarello de Souza Pinto - UPM - São Paulo

Relações Internacionais para os demais Continentes:

Profa. Dra. Gina Vidal Marcilio Pompeu - UNIFOR - Ceará

Profa. Dra. Sandra Regina Martini - UNIRITTER / UFRGS - Rio Grande do Sul

Profa. Dra. Maria Claudia da Silva Antunes de Souza - UNIVALI - Santa Catarina

Educação Jurídica

Profa. Dra. Viviane Coêlho de Séllos Knoerr - Unicuritiba - PR

Prof. Dr. Rubens Beçak - USP - SP

Profa. Dra. Livia Gaigher Bosio Campello - UFMS - MS

Eventos:

Prof. Dr. Yuri Nathan da Costa Lannes - FDF - São Paulo

Profa. Dra. Norma Sueli Padilha - UFSC - Santa Catarina

Prof. Dr. Juraci Mourão Lopes Filho - UNICHRISTUS - Ceará

Comissão Especial

Prof. Dr. João Marcelo de Lima Assafim - UFRJ - RJ

Profa. Dra. Maria Creusa De Araújo Borges - UFPB - PB

Prof. Dr. Antônio Carlos Diniz Murta - Fumec - MG

Prof. Dr. Rogério Borba - UNIFACVEST - SC

C928

Criminologias e política criminal II [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Edith Maria Barbosa Ramos; Maiquel Ângelo Dezordi Wermuth ; Flavia Piccinin Paz – Florianópolis: CONPEDI, 2026.

Inclui bibliografia

ISBN: 978-65-5274-621-4

Modo de acesso: www.conpedi.org.br em publicações

Tema: Constituição, Processo e Justiça Social: o papel da jurisdição constitucional na efetivação de direitos

2. Criminologias. 3. Política criminal. IX Encontro Virtual do CONPEDI (2: 2026: Florianópolis, Brasil).

CDU: 34



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

IX ENCONTRO VIRTUAL DO CONPEDI

CRIMINOLOGIAS E POLÍTICA CRIMINAL II

Apresentação

O Grupo de Trabalho Criminologias e Política Criminal II, realizado no âmbito do IX Encontro Virtual do CONPEDI, em 22 de junho de 2026, reuniu pesquisadores de diferentes instituições brasileiras para debater temas centrais da criminologia contemporânea, das políticas criminais e dos direitos humanos. As apresentações evidenciaram a pluralidade de perspectivas teóricas e metodológicas que atualmente orientam a pesquisa jurídica nacional, proporcionando um espaço qualificado para o intercâmbio científico e para o aprofundamento de reflexões críticas acerca dos desafios enfrentados pelo sistema de justiça criminal.

A programação contemplou pesquisas dedicadas à análise das relações entre direito penal, seguridade social e políticas públicas, como o estudo "Entre a Repressão Penal e a Seguridade Social: a Vedação do Auxílio-Reclusão aos Dependentes de Integrantes de Organizações Criminosas pela Lei nº 15.358/2026", de Giovanna Duarte Fighera, Rodrigo Zimmermann Martins e Higor Lameira Gasparetto, bem como investigações sobre os impactos da política de drogas na seletividade penal, a exemplo de "Entre a Subjetividade da Lei e a Seletividade Penal: alguns efeitos sobre o encarceramento de mulheres negras no Brasil a partir da política de Guerra às Drogas", de Fernanda da Silva Lima, Rafaela Meyer Ielo de Oliveira e Fernanda Analu Marcolla, e de "Entre a Universalidade Formal e a Exclusão Material: Seletividade Penal, Política de Drogas e Camadas de Vulnerabilidade no Cárcere Brasileiro", de José Antonio Nunes Aguiar, Silvio Carlos Leite Mesquita e Jade Tereza Almeida Ferreira.

Também integraram o GT pesquisas voltadas à compreensão dos mecanismos estruturais de

A expansão das tecnologias de controle penal e seus impactos sobre os direitos fundamentais também esteve presente nas discussões, por meio dos trabalhos "Gestão Seletiva da Memória: Criminologia Crítica e Epistemologia da Prova frente à Portaria MJSP nº 1122/2026", de Laura Rosa Martins e Jaime Domingues Brito; "Cadeia de Custódia na Apreensão de Criptoativos: a Presunção de Inocência no Âmbito da Resolução 288/2024 do Conselho Nacional do Ministério Público", de Hernani Deon Klaus e Reginaldo Pereira; "Biovigilância Genética e Expansão do Poder Punitivo: análise da coleta compulsória de DNA no processo penal brasileiro", de Marcelo Yukio Misaka, Kauã de Oliveira Sanches e Luís Guilherme Augusti Sampaio; e "Hibridismo Criminal: a simbiose operacional entre o crime organizado e os crimes cibernéticos", de Lucas Allebrandt Peres, Eraldo Cruz Martins Filho e Renata Almeida da Costa.

O enfrentamento ao crime organizado e às novas configurações da criminalidade constituiu outro eixo de reflexão, reunindo contribuições como "Facções Criminosas no Brasil e Custo da Atividade Delitiva: Fundamentos para um Modelo Repressivo de Enfrentamento Estatal à Luz do Direito Penal do Inimigo e da Análise Econômica do Crime", de Pedro Henrique Fidelis Costa, e "A Rota Bioceânica e os Desafios da Segurança Fronteiriça: impactos sociais e humanos diante da criminalidade transnacional", de Cauê Coutinho Netto.

As discussões sobre execução penal, sistema prisional e alternativas à resposta estritamente retributiva foram representadas pelos trabalhos "Falar com os Homens é Proteger as Mulheres: Grupos Reflexivos para Autores de Violência Doméstica no Sistema Prisional", de Ana Maria Rodrigues da Cunha e Claudia Luiz Lourenço; "Sistema Progressivo de Pena: uma revisão sistemática sobre livramento condicional e progressão de regime a partir da Plataforma CAPES", de Deylane Azevedo Moraes Leite; "Direito Penal, Criminologia Crítica e Direitos Fundamentais: diagnóstico das violações em Pedrinhas sob o prisma da legitimidade do direito de punir", de Antonio Coêlho Soares Junior, Anália Márcia Gracinda Marques dos Santos e Maria Luiza Rolim Ribeiro; e "A 'Psicopatia' Infantojuvenil: desafios e

O conjunto dos trabalhos evidencia a atualidade e a relevância dos debates contemporâneos em torno da criminologia, das políticas criminais e dos direitos humanos. Apesar da diversidade temática, as pesquisas convergem para uma preocupação comum: compreender criticamente os limites, as racionalidades e os impactos do poder punitivo em sociedades marcadas por profundas desigualdades sociais. Destaca-se, nesse contexto, a forte presença da criminologia crítica como referencial teórico capaz de problematizar a seletividade penal, o encarceramento em massa, a criminalização de grupos vulnerabilizados e as novas formas de vigilância e controle social.

As apresentações também demonstraram a crescente interdisciplinaridade da pesquisa jurídica brasileira, incorporando contribuições provenientes da sociologia, da ciência política, da economia, dos estudos de gênero e raça, da criminologia, da ciência da informação e das tecnologias digitais. Tal pluralidade permitiu ampliar a compreensão dos desafios contemporâneos relacionados à expansão do sistema penal, às transformações da criminalidade organizada, à proteção dos direitos fundamentais e à construção de políticas públicas orientadas pelos valores do Estado Democrático de Direito.

Os coordenadores registram seu agradecimento a todos os autores, avaliadores e participantes pelas relevantes contribuições apresentadas durante o GT, cuja qualidade científica e diversidade temática enriqueceram os debates realizados no IX Encontro Virtual do CONPEDI. Os estudos reunidos nestes anais constituem importante contribuição para o fortalecimento da pesquisa em criminologia e política criminal, reafirmando o compromisso da comunidade acadêmica com a produção de conhecimento crítico, rigoroso e socialmente comprometido.

Edith Maria Barbosa Ramos

Maiquel Ângelo Dezordi Wermuth

CADEIA DE CUSTÓDIA NA APREENSÃO DE CRIPTOATIVOS: A PRESUNÇÃO DE INOCÊNCIA NO ÂMBITO DA RESOLUÇÃO 288/2024 DO CONSELHO NACIONAL DO MINISTÉRIO PÚBLICO

CHAIN OF CUSTODY IN THE SEIZURE OF CRYPTO ASSETS: THE PRESUMPTION OF INNOCENCE WITHIN THE SCOPE OF RESOLUTION 288 /2024 OF THE NATIONAL COUNCIL OF THE PUBLIC PROSECUTOR'S OFFICE

**Hernani Deon Klaus
Reginaldo Pereira**

Resumo

O artigo explora a complexidade da cadeia de custódia da prova digital no cenário penal brasileiro, contextualizando a fragilidade dos vestígios eletrônicos e a necessidade de garantir sua integridade frente à crescente dependência em investigações. O trabalho tem como objetivo principal analisar as implicações ao princípio da presunção de inocência e às normas de salvaguarda da Lei Geral de Proteção de Dados (LGPD) decorrentes da liquidação de criptoativos na fase processual prevista Resolução CNMP nº 288/2024 e nas potencialidades da utilização da tecnologia Blockchain, como meio de custódia dessas modalidades de prova. A pesquisa é analítica, guiada pelo método indutivo, e empregada revisão bibliográfica, análise documental e jurisprudencial como técnicas de pesquisa. O texto trata inicialmente da relevância constitucional da cadeia de custódia e das possibilidades oferecidas pela tecnologia Blockchain na tutela da integridade de provas digitais. Aborda, em seguida, os aspectos da Resolução CNMP nº 288/2024 que, ao prever a liquidação imediata de criptoativos apreendidos, colide com a finalidade da cadeia de custódia e viola a presunção de inocência. Conclui-se que, ao prever a liquidação imediata de ativos virtuais apreendidos, a Resolução CNMP nº 288/2024 apresenta-se incoerente ao sistema processual e viola a presunção de inocência, fato que a torna, ao mesmo tempo inconstitucional e inoportuna, dada a capacidade de custódia de provas digitais oferecida pela tecnologia Blockchain.

Palavras-chave: Apreensão de criptoativos, Blockchain, Cadeia de custódia, Presunção de inocência, Resolução cnmp nº 288/2024

integrity and "sameness" of the evidence, hindering the full exercise of the adversarial principle over the original corpus delicti. The study concludes that, although blockchain technology offers mechanisms for immutability and traceability, the state management of these assets must prioritize the preservation of evidentiary integrity over mere collection efficiency, under penalty of unconstitutionality due to the anticipation of the effects of the sentence.

Keywords/Palabras-claves/Mots-clés: Seizure of crypto assets, Blockchain, Chain of custody, Principle of presumption of innocence, Cnmp resolution no. 288/2024

1 INTRODUÇÃO

No cenário penal, em particular sobre a dependência crescente de vestígios eletrônicos em investigações e processos judiciais, vê-se desafios inéditos, notadamente em razão da fragilidade inerente às provas digitais. A facilidade com que podem ser alteradas, suprimidas ou adulteradas apresentam patente problematização nos procedimentos adotados pelos órgãos persecutórios, naquilo que concerne a integridade e autenticidade dessas evidências.

À guisa de ilustração, criptoativos são utilizados para transações ilícitas em âmbito global, com uma estimativa de US\$ 154 bilhões recebidos por endereços de criptomoedas associadas a atividades ilícitas em 2025 (Chainalysis, 2026).

A cadeia de custódia emerge como um pilar fundamental, não apenas como um procedimento técnico, mas como um mecanismo essencial que se presta a garantir diversos aspectos constitucionais, como o devido processo legal, o contraditório e a ampla defesa, salvaguardando a licitude e a idoneidade do material probatório.

A linha trilhada por este estudo direciona-se à análise constitucional da sistemática de liquidação imediata de ativos em investigações criminais, adotada pela Resolução CNMP nº 288/2024. A pesquisa é analítica, guiada pelo método indutivo, empregando-se a revisão bibliográfica e as análises documental e jurisprudencial como técnicas de pesquisa.

Para que se tenha ideia da importância do tema, a discussão transcende a mera técnica, adentrando em questões cruciais de privacidade e garantias individuais, especialmente quando medidas precipitadas podem ocasionar a violação da presunção de inocência.

É nesse ponto que se delinea a principal tensão abordada. De um lado, tem-se a robustez tecnológica da *blockchain* e sua capacidade de prover um rastro incorruptível para as transações digitais e, por conseguinte, para a prova. E, de outro, o desafio de harmonizar essa imutabilidade com direitos fundamentais como o direito à privacidade e o direito ao esquecimento, previstos na Lei Geral de Proteção de Dados (LGPD), além das implicações de normativas recentes, como a Resolução nº 288/2024 do Conselho Nacional do Ministério Público (CNMP).

O ponto, porém, é que, por meio da referida Resolução, certas disposições, notadamente aquelas que orientam a “liquidação imediata” de ativos virtuais apreendidos, parecem colidir frontalmente com a própria finalidade da cadeia de custódia. Vale dizer, uma resolução normativa que vem para agregar valor à atuação do órgão persecutório, justamente no que diz respeito a apreensão de “ativos virtuais”, atribui um ônus prematuro ao investigado, violando, em essência, a presunção de inocência que deve prevalecer até a condenação transitada em julgado.

É, portanto, nítido o caráter multidisciplinar e crítico deste trabalho, que busca não apenas explorar o potencial técnico da *blockchain* na segurança da prova digital, mas também questionar as implicações jurídicas de sua gestão por parte dos órgãos estatais, propondo uma reflexão sobre a necessidade de um arcabouço normativo que realmente concilie a inovação tecnológica com as garantias constitucionais, garantindo a justiça e a integridade do processo penal na esfera digital.

2 A RELEVÂNCIA CONSTITUCIONAL DA CADEIA DE CUSTÓDIA

No caso da cadeia de custódia da prova digital, tem-se constatado, cada vez mais, uma tendência à precipitação investigativa. A celeridade, embora compreensível diante da volatilidade e dinâmica própria dos ambientes digitais, acaba por fomentar práticas que suprimem etapas essenciais para garantir a integridade das evidências. A busca pela rápida persecução penal, especialmente em crimes envolvendo sistemas descentralizados ou ativos criptográficos, muitas vezes leva à negligência quanto à formalização da cadeia de custódia, cuja observância é condição para a validade da prova no processo penal.

Essa negligência é ainda mais problemática quando se consideram as características próprias das provas digitais. Ao contrário de objetos físicos, que demandam acesso físico e deixam vestígios materiais de sua manipulação, as provas digitais, tais como registros em servidores, arquivos criptografados, transações em *blockchain*, comunicações interceptadas, entre outras, são notoriamente frágeis. Pequenas alterações imperceptíveis a olho nu podem comprometer completamente a autenticidade e a integridade do conteúdo, sem que isso seja, de imediato, detectável pelos operadores do direito.

É nesse contexto que a cadeia de custódia assume papel central: ela não é um formalismo burocrático, mas um instrumento técnico-processual que garante o controle epistêmico da prova. A cadeia de custódia funciona, como se demonstrará adiante, como base para a observância dos princípios constitucionais.

Não é por acaso que os tribunais superiores reconhecem a nulidade de provas coletadas antes da Lei nº 13.964, de 2019, que incluiu os artigos referentes a cadeia de custódia no Código de Processo Penal¹.

A obtenção das provas na fase inquisitorial vem embutida de uma série de procedimentos a serem observados, sejam relacionados ao modo como são autorizadas pelo magistrado, ou pelo modo como são manuseadas.

¹ “mesmo para fatos anteriores a 2019, é necessário avaliar a preservação da cadeia de custódia” (Brasil, STJ, 2023).

Nesse contexto, a admissibilidade da prova constitui uma espécie de avaliação preliminar, podendo inadmiti-la se for ilícita. O que nos permite trazer essa interpretação é a literalidade do disposto pelo artigo 5º da Constituição Federal, em seu inciso LVI: “*são inadmissíveis, no processo, as provas obtidas por meios ilícitos*”.

Para Gustavo Badaró:

A admissão ou deferimento das provas se dá por decisão judicial. Correlato à proposição de provas lícitas é o direito de exclusão das provas inadmissíveis. A inadmissibilidade é uma sanção processual que visa a impedir que provas viciadas ingressem no processo e possam influenciar, de alguma forma, o convencimento judicial (Badaró, 2008. p. 204).

Ao falar sobre o direito de participar, se contrapor e ser informado sobre todos os atos probatório (contraditório), Aury Lopes Júnior (2019), pelo corpo de sua obra, dispõe que, após a postulação da prova (primeira fase) feita pela parte interessada, a admissibilidade vem como um segundo filtro, feito pelo juiz. Em outras palavras, a (in)admissibilidade da prova ilícita é desenvolvida pelo magistrado logo após a postulação.

A questão é que avaliar uma prova coletada sem observância aos procedimentos da cadeia de custódia, assume elevada relevância, sendo capaz de impedir a movimentação da máquina estatal. Afinal, quando não for possível constatar a trajetória ou a ordem cronológica da prova, principalmente digital, os indícios de adulteração já se fazem presentes.

O simples fato de as autoridades encarregadas pelas investigações não seguirem os devidos procedimentos já confere, sob uma análise lógica e legal, indícios suficientes para concluir que sua fé pública deve ser relativizada.

Aquilo que se observa na prática — em que o Magistrado posterga a análise das nulidades da prova para o momento da valoração — não confere, sob uma interpretação doutrinária, a devida credibilidade ao Código de Processo Penal (CPP) e à própria Constituição Federal (CF). Afinal, como já referido, a admissibilidade da prova integra a segunda fase de sua trajetória processual, funcionando como um dos primeiros filtros que, indiscutivelmente, deve impedir que provas ilícitas ingressem no processo, evidentemente e diversamente de pensamentos voltados a analisá-la na fase da valoração (quarta fase).

A prova sequer deve ingressar no processo. Entretanto, caso algum vestígio manifestamente ilícito venha a embasar a denúncia, a defesa do réu, assim como deve ser, poderá alegar a falta ou ausência dos procedimentos descritos pelos artigos 158-A a 158-F do CPP, logo na defesa preliminar ou resposta à acusação. É neste momento em que contestar-se-á sua integridade.

Convém mencionar que este é o momento oportuno, por duas razões: i) a jurisprudência dos Tribunais Superiores é pacífica ao rechaçar a estratégia processual denominada nulidade de algibeira, a qual ocorre quando a defesa não alega a existência de vício formal em momento oportuno, quedando-se inerte até que seja verificado, no futuro, que a tese acarretará mais benefícios ao agente, em explícita ofensa aos princípios da boa-fé processual e da cooperação (Brasil, STJ, 2023); e ii) a falta de fundamentação em decisões que confirmam o recebimento da denúncia, gera constrangimento ilegal passível de discussão em *habeas corpus*.

O Min. Felix Fischer, relatando Acórdão unânime da 5ª Turma do STJ, alerta:

Se não fosse necessário exigir que o Magistrado apreciasse as questões relevantes trazidas pela defesa – sejam preliminares ou questões de mérito – seria inócua a previsão normativa que assegura o oferecimento de resposta ao acusado (Brasil, STJ, 2010).

Aqui, o que importa ressaltar é que a falta de tratamento adequado a prova tem seu momento de violação anterior ao processo, por andar em desconformidade com uma garantia exposta pela Constituição Federal. Ademais, a impossibilidade de se visualizar a totalidade do caminho percorrido pela prova já a torna inadmissível. Veja-se, no ponto, às disposições da Quinta Turma do Superior Tribunal de Justiça:

No caso dos autos, a polícia não documentou nenhum dos atos por ela praticados na arrecadação, armazenamento e análise dos computadores apreendidos durante o inquérito, nem se preocupou em apresentar garantias de que seu conteúdo permaneceu íntegro enquanto esteve sob a custódia policial. Como consequência, não há como assegurar que os dados informáticos periciados são íntegros e idênticos aos que existiam nos computadores do réu. 8. Pela quebra da cadeia de custódia, são inadmissíveis as provas extraídas dos computadores do acusado, bem como as provas delas derivadas, em aplicação analógica do art. 157, § 1º, do CPP (Brasil, STJ, 2023).

Ainda que, em tese, se possa sustentar que a inobservância da cadeia de custódia configure mera nulidade relativa, o entendimento das egrégias Cortes Superiores caminha no sentido de reconhecer como inadmissíveis as provas cuja obtenção desconsidera os procedimentos destinados à preservação da integridade e confiabilidade das fontes.

No expressivo dizer de Antonio Magalhães (2013, p. 24), as garantias previstas na Constituição integram “barreiras de proteção, as defesas contra a utilização arbitrária do poder”.

É nelas, vale dizer, que a cadeia de custódia tem sua essência. Conquanto seja um procedimento, à primeira vista, de natureza processual, sua presença possui relevância constitucional, ao passo que garante a devida atenção aos princípios do contraditório, ampla defesa e presunção de inocência. Relevante, no ponto, as palavras do Ministro Ribeiro Dantas:

A cadeia de custódia tem como objetivo garantir a todos os acusados o devido processo legal e os recursos a ele inerentes, como a ampla defesa, o contraditório e, principalmente, o direito à prova lícita. O instituto abrange todo o caminho que deve ser percorrido pela prova até sua análise pelo magistrado, sendo certo que qualquer interferência durante o trâmite processual pode resultar na sua imprestabilidade (Brasil, STJ, 2019).

A disposição é absolutamente segura: a observância garante os princípios constitucionais, enquanto a inobservância leva a imprestabilidade da prova.

2.1 TRAZENDO A DEBATE A FACILIDADE NA ADULTERAÇÃO DE PROVAS DIGITAIS

Afora o exposto, oportuno frisar que a cadeia de custódia toma relevância no Brasil apenas em 2014, a partir de contribuições de Geraldo Prado, voltadas à análise da cadeia de custódia e sua repercussão no processo penal brasileiro. Nessas reflexões, o autor destacava a imprescindibilidade de garantir à defesa pleno conhecimento das fontes probatórias, sobretudo em razão de práticas anteriores à introdução da fase de admissibilidade da acusação, marcadas pela ocultação de informações pelas autoridades estatais. Afinal, como pontua o próprio Prado, dificilmente quem age de forma ilícita no momento da colheita da prova permitirá que tal ilicitude transpareça no curso processual (Prado, 2014. p. 48).

Não é por acaso que Parodi (2024), em sua obra *“Perícia defensiva em provas digitais no processo penal”*, refere que essa proteção do indivíduo no processo penal, de ser processado por provas íntegras, não só não depende da recente positivação, mas presta-se a preservar os princípios constitucionais.

Embora, à primeira vista, possa parecer um formalismo excessivo exigir a observância rigorosa dos procedimentos previstos para a cadeia de custódia, é imprescindível reafirmar a primazia do princípio da legalidade, que, como sustenta o autor, não pode ser relativizado com base na fé pública do agente responsável pela investigação, mesmo que frequentemente invocado para justificar o descumprimento dos trâmites legais. O destaque é que esse argumento não tem o condão de suprir a ausência de garantia quanto à origem e integridade da prova:

A fé pública, então, pode ser presumida, até prova em contrário, em relação à legalidade dos atos realizados pelo agente e à moralidade de tais atos. A moralidade, por sua vez, está relacionada à adoção dos outros princípios de boa-fé e probidade, afastando, entre outros, o conceito que "os fins justificam os meios" (Parodi, 2024).

É cediço que a ignorância da Lei é inescusável (Art. 21 do CP). Tal afirmativa é ainda mais válida quando diz respeito à atuação de um agente público, que, em seus atos, deve respeitar o princípio da legalidade (Art. 37 da CF).

Na mesma linha de raciocínio, a Corte Cidadã tem entendido:

É ônus do Estado comprovar a integridade e confiabilidade das fontes de prova por ele apresentadas. É incabível, aqui, simplesmente presumir a veracidade das alegações estatais, quando descumpridos os procedimentos referentes à cadeia de custódia (Brasil, STJ, 2023).

Como acentuado pelo trabalho de Lorenzo Parodi (2024), o largo espectro de possibilidades de adulteração de provas toma especial relevância no campo digital. Embora, normalmente, as evidências digitais possam conferir maior grau de validação por seus receptores, são facilmente adulteradas. Tanto é assim que expõe um tópico específico em sua obra, destacando as diversas maneiras de se modificar uma prova digital de forma indetectável, inclusive, com a própria utilização do código *hash* (espécie de impressão digital da informação, tradução livre).

Embora a jurisprudência pátria tenha avançado, assim como se pode ver pelos precedentes já citados, se tem a falsa percepção de que o órgão acusatório, em hipótese alguma, poderá adulterar uma prova e vir a prejudicar o réu.

O ponto é que há espaço para adulterações, muitas vezes, pela ausência de técnica no manuseio da prova, e não necessariamente pela má-fé dos agentes responsáveis. E é justamente por essa razão que os precedentes reconhecem a cadeia de custódia como instrumento indispensável à veracidade e confiabilidade da prova, funcionando como garantia da lisura de sua origem e preservação.

A título de exemplo, a Quinta Turma do STJ já a conceituou a cadeia de custódia em evidente consonância com a ideia de ‘veracidade’ do conteúdo coletado, senão vejamos:

A principal finalidade da cadeia de custódia é garantir que os vestígios deixados no mundo material por uma infração penal correspondem exatamente àqueles arrecadados pela polícia, examinados e apresentados em juízo (Brasil, STJ, 2023).

Embora os procedimentos da cadeia de custódia, previstos nos dispositivos do processo penal sejam diversos, pode-se afirmar, em termos gerais, que todos convergem para dois objetivos fundamentais: garantir a integralidade e a integridade da prova. São conceitos distintos, mas interdependentes. É a pura observância aos trâmites legais que permite os sujeitos do processo verificarem, primeiramente, se todos os vestígios estão disponíveis (integralidade), para, somente então, avaliar a autenticidade e veracidade (integridade).

Para esclarecer, Lorenzo Parodi (2024, p. 63/64) traz conceitos bastante precisos sobre autenticidade e veracidade de provas digitais. Em primeiro lugar, a autenticidade:

diz respeito à comprovação que o arquivo (ou documento) em análise foi efetivamente produzido por quem detinha a competência legal para tal produção e não sofreu quaisquer mudanças desvirtuadoras em momentos posteriores à sua criação.

Evidente que um documento pode ser autêntico, mas ao mesmo tempo conter informações falsas (ou seja, não ser verídico). Pensemos, por exemplo, num documento digital criado por um colaborador, que tinha competência legal para criar tal documento, mas o criou para fornecer informações falsas (ideologicamente falsas) no âmbito de seu acordo de colaboração premiada.

Poderá se dizer que o documento é absolutamente autêntico, mesmo assim não será verídico, pois as informações nele contidas serão falsas, apesar de lá inseridas por quem detinha competência legal para tanto.

Em outras palavras, autêntico deve ser o arquivo que mantém íntegra sua origem e forma, revelando-se como resultado de uma produção legítima e tecnicamente rastreável, independentemente da veracidade material de seu conteúdo. O que se preserva é a fidedignidade do trajeto documental: é autêntico porque foi gerado por quem tinha competência para tanto e não foi adulterado desde então, ainda que o conteúdo ali registrado possa vir a ser ideologicamente falso.

Já no tocante a veracidade, Lorenzo Parodi (2025, p. 63/64) traz um conceito absolutamente vinculado a origem, senão vejamos:

A conferência da veracidade do conteúdo de provas digitais pode ser uma atividade muito complexa e de êxito incerto, a depender do tipo de arquivo digital e, sobretudo, do tipo de informações a serem verificadas e de sua real origem.

De forma geral, é necessário ponderar inicialmente qual a origem do material digital para poder ter uma ideia a respeito da possível autenticidade e veracidade dele.

Em seguida, será necessário analisar como tal material foi obtido e custodiado, para verificar se as informações nele contidas podem ter sido adulteradas e, com isso, não serem mais verídicas (em tudo ou em parte).

Por ser algo mais subjetivo, conclui destacando a necessidade de avaliar eventuais interesses que originário detentor da prova possa ter:

Por fim, é sempre interessante avaliar se o proprietário, fonte ou criador original do material digital em análise poderia ter alguma razão para inserir informações não verídicas em momento anterior à sua aquisição por parte das autoridades (PARODI, 2025, p. 63/64.)

É por isso que a discussão sobre a cadeia de custódia em provas digitais eleva a necessidade do pleno acesso à integralidade do material, porquanto é essencialmente com esse passe irrestrito que se pode analisar o caminho percorrido pela prova desde o início. Não é por acaso que o autor discorreu sobre a relevância da análise da origem do objeto, seja pela competência da pessoa que confeccionou o documento (por exemplo) tido como prova, ou do local originário em que o arquivo estava armazenado antes de sua extração.

Sob todos os aspectos que se queira analisar, manejar uma prova digital depende de técnica e registro constante dos procedimentos. Já se falou sobre isso linhas acima, mas o acesso

integral é essencial para o desate da causa, especialmente quando se quer analisar a cadeia de custódia de uma prova digital.

Ora, se a justa causa de uma ação penal é pautada em prova da qual os acusados não possuem acesso à sua totalidade, ter-se-á uma afronta direta às garantias e princípios fundamentais dispostos pela Constituição pátria e, por consectário lógico, uma nulidade absoluta.

Essa é a própria *ratio essendi* (razão de ser, tradução do autor) da Súmula Vinculante nº 14 do STF. É legítimo que o Ministério Público selecione os elementos que embasarão a denúncia. Entretanto, os demais documentos ou informações colhidos na investigação, ainda que não utilizados diretamente na peça acusatória, devem permanecer acessíveis à defesa. Esse é, portanto, o conceito mais pragmático e análogo da integralidade probatória.

Assim, considera-se extremamente categórica a afirmação do eminente Ministro Rogério Schietti Cruz, de que a produção de uma contraprova, pela defesa, é comprometida quando o acesso integral não é visualizado:

O comportamento do titular da ação penal, com o respaldo judicial, de privar a defesa do acesso à integralidade dos elementos probatórios relativos à imputação, compromete a idoneidade do processo – como espaço civilizado, ético e paritário de solução de uma controvérsia penal – e afeta, significativamente, a capacidade defensiva de, no momento oportuno, refutar a acusação e produzir contraprova. (Brasil, STJ, 2021).

E considerando as disposições apontadas, a privação das partes ao acesso integral aos elementos probatórios é o ponto central para se constatar os exigidos indícios de adulteração.

Por um lado, a falta de acesso compromete a capacidade defensiva², especialmente porque a simples observância de elementos que não estão disponíveis é condição apta a prejudicar os princípios do contraditório e ampla defesa, afastando a impugnação ou a produção de contraprova. E da mesma forma se dá em uma quebra na cadeia de custódia.

Apenas para ilustrar, a inviabilidade de produzir uma contraprova frente ao acesso parcial aos elementos probatórios é essencialmente danosa. Seja porque essa limitação compromete a veracidade dos fatos e a própria idoneidade do caminho percorrido, ou por levar as partes a terem que trabalhar com duas possibilidades simultâneas: (i) apresentar teses voltadas à impugnação da prova flagrantemente ilegal; ou (ii) estruturar, ao mesmo tempo, meios destinados à defesa de contraprovas ilícitas.

² conclusão exposta pela Sexta Turma do STJ ao tratar sobre a integralidade, no RHC 114.683/RJ, de relatoria do Ministro Rogério Schietti Cruz, em 2021.

Trabalhar com essas duas hipóteses em paralelo, sem saber qual delas será acatada, coloca a defesa em uma posição absolutamente descentrada. Isso porque, além da incerteza sobre as provas, a parte ainda precisa formular uma resposta probatória sem conhecer, de forma plena, o conteúdo que está sendo ocultado ou suprimido.

Um exemplo concreto dessa dificuldade é a tentativa de apresentar um álibi sem ter acesso completo às informações que compõem o contexto da acusação. Ora, há como demonstrar que o acusado estava em outro local, ou realizando outra atividade, sem saber exatamente o horário dos fatos, os dados técnicos dos registros utilizados contra ele, ou sequer os metadados que sustentam a imputação?

A título ilustrativo, imagine-se alguém acusado de ter transferido valores suspeitos para uma carteira de criptomoeda vinculada a um crime. A defesa, para comprovar que tal operação não partiu do acusado, poderia apresentar os logs de acesso de sua carteira digital, registros bancários, ou mesmo a geolocalização de seus dispositivos no momento da transação.

Ocorre que, sem acesso aos dados originais da acusação — como o *timestamp* (registro temporal, tradução do autor) da transação na *Blockchain* (cadeia de blocos, tradução do autor), os IPs (*Internet Protocols* - Protocolos de Internet), ou os dispositivos interceptados — torna-se praticamente inviável reconstruir tecnicamente o que de fato ocorreu. A ausência de dados impede que se comprove, por exemplo, que a operação foi forjada, realizada por terceiros, ou que houve acesso indevido ao terminal.

Portanto, o problema não reside apenas na estratégia processual, mas na própria impossibilidade material de defesa: não se pode refutar aquilo que não se conhece integralmente.

Por todo o exposto, percebe-se que a narrativa sobre a quebra da cadeia de custódia tem seguido um caminho distorcido: presume-se a lisura da atuação investigativa, invertendo-se indevidamente o ônus da prova para exigir que o acusado demonstre indícios de adulteração, quando, em verdade, a discussão deveria voltar-se àquelas questões iniciais tratadas por Geraldo Prado, sobre a violação aos princípios constitucionais. Conforme já referido, as adulterações podem ser indetectáveis, e é justamente o papel do Estado comprovar que o caminho percorrido pela prova foi íntegro.

Ainda que as garantias constitucionais sustentem a obrigatoriedade de se preservar a origem e a integridade da prova, é no campo técnico que a efetivação desses direitos encontra seus maiores desafios. Nesse contexto, torna-se indispensável considerar modelos de implementação tecnológica da cadeia de custódia digital.

3 BLOCKCHAIN E A LIQUIDAÇÃO DA PROVA: ANÁLISE DA RESOLUÇÃO CNMP 288/2024

Sobre as particularidades da *blockchain*, a cadeia de custódia digital, embora ainda em fase de amadurecimento em seu uso legal, revela-se uma aplicação promissora dessa tecnologia no ambiente forense. Surgida com a criptomoeda Bitcoin em 2008, a *blockchain* constitui um livro-razão seguro, compartilhado e distribuído, que permite o registro e o acompanhamento de recursos sem a necessidade de uma autoridade central confiável. A essência dessa tecnologia está na capacidade de gravar transações de forma permanente, de modo que não podem ser apagadas, apenas atualizadas sequencialmente, mantendo um rastro histórico inalterável e tornando a modificação de conteúdo praticamente inviável (Petroni; Gonçalves, 2018). Essa característica inerente à *blockchain* se amolda quase que perfeitamente a cadeia de custódia digital, garantindo que as evidências permaneçam disponíveis e intactas pelo tempo necessário para análises periciais, consultas judiciais e utilização em processos.

Os métodos forenses tradicionais podem não ser totalmente adequados para a coleta, armazenamento e verificação de evidências digitais, dada sua natureza volátil e suscetível a alterações indetectáveis, conforme já adiantado. Entretanto, a *blockchain* apresenta algumas soluções (Petroni; Gonçalves, 2018).

Modelos de arquitetura baseados em *smart contracts* (contratos inteligentes, tradução do autor), aplicados a plataformas *blockchain*, permitem a formação de uma cadeia de custódia digital mais segura e transparente. Os *smart contracts* são programas autoexecutáveis armazenados na rede que automatizam e gerenciam a custódia das evidências. Uma vez implantados, não podem ser modificados, assegurando a integridade do processo (Petroni; Gonçalves, 2018).

Essa estrutura impõe, por design, integridade, transparência, autenticidade e auditabilidade, o que demonstra harmonia absoluta com os conceitos de rastreabilidade e cadeia de custódia forense. Essa deve ser a essência para que os dados lógicos sejam admissíveis em uma ação penal, pois a cadeia de custódia digital deve demonstrar a integridade e autenticidade dos dados, com registros detalhados de coleta, extração, análise, armazenamento e transferência (Silva, 2024).

Em determinados aspectos já vem-se sustentando que a transição para a documentação eletrônica com suporte em *blockchain* melhora a legibilidade, a autenticidade e a utilidade dos documentos, otimizando a interação entre as partes interessadas no devido processo legal (Silva, 2024).

Ocorre que, embora a dinâmica da rede *blockchain* ofereça transparência inerente e mecanismos de segurança robustos — como criptografia e imutabilidade de registros — que podem alinhar-se e fortalecer a cadeia de custódia, o direcionamento é outro quando busca-se atender aos princípios da LGPD (Lei Geral de Proteção de Dados). Não há dúvida sobre a existência de uma tensão palpável e desafiadora entre sua natureza descentralizada, que distribui o controle por múltiplos nós independentes, e a estrutura legal da LGPD, projetada primordialmente para regular sistemas de gerenciamento de dados centralizados, onde uma entidade única assume responsabilidade clara e auditável (Silva, 2024).

Vale destacar, por exemplo, a dificuldade na aplicação da exclusão de dados pessoais (o "direito ao esquecimento"), já que uma vez registrados na cadeia, os dados se tornam praticamente impossíveis de apagar sem comprometer a integridade da rede inteira.

As principais complicações da tecnologia com a LGPD residem na natureza fundamentalmente diferente de como cada uma opera. Por um lado, a *blockchain* registra informações de forma permanente e imutável, enquanto a LGPD garante o direito ao esquecimento, que permite ao titular dos dados solicitar que suas informações sejam apagadas de um sistema quando elas não forem mais necessárias para a finalidade pela qual foram coletadas, ou em outras situações previstas em lei.

Vale relembrar, também, que a rede é descentralizada. Ou seja, não possui uma única entidade ou servidor central que controla todos os dados pessoais daqueles que utilizam. A LGPD, porém, exige a clara identificação de um "Controlador" (quem decide sobre o tratamento dos dados) e de um "Operador" (quem realiza o tratamento dos dados em nome do controlador).

De forma bem sucinta, sem qualquer intenção de esgotar o mérito dessa questão, vale mencionar que alguns autores, como Fabian Andrade Silva (2024), já expõem propostas e novas abordagens para conciliar a robustez da rede com as exigências da LGPD, por meio de modelos computacionais que apresentam uma “abordagem híbrida de armazenamento”. Assim, não só integrar-se-á ferramentas de segurança avançada para controlar o acesso granular aos dados — por meio de contratos inteligentes e permissões criptografadas —, mas também garante o rastreamento preciso e auditável de todas as alterações ao longo do ciclo de vida dos dados pessoais, promovendo uma ponte entre a descentralização tecnológica e as demandas legais, e dando início à uma forma para uma adoção mais segura e ética da *blockchain* no contexto brasileiro.

Em outras palavras, a solução de Fabian (2024), e de outras abordagens similares, geralmente envolvem, em síntese, não armazenar os dados pessoais sensíveis diretamente na *blockchain*, mas utilizá-la para garantir a integridade e rastreabilidade, valendo-se da gestão de

acesso e permissões fora da rede, que, por sua vez, permanecem sob o controle de sistemas que podem atender às exigências da LGPD, como o direito ao esquecimento levantando linhas acima. Permitindo, por óbvio, aproveitar os benefícios da tecnologia na segurança da prova digital, ao mesmo tempo em que se respeitam os direitos fundamentais de privacidade e proteção de dados.

A preocupação com a privacidade dos dados pode, à primeira vista, parecer incompatível com a necessidade de se garantir a cadeia de custódia, especialmente porque a essência da *blockchain* reside na imutabilidade e no registro permanente das informações, características que, somadas ao alto grau de anonimato nos registros da rede e à ausência de um "controlador de dados" central, tornam o debate ainda mais complexo. Justamente por conta do anonimato e da facilidade de transferência de ativos dentro da rede, em 2024, o Conselho Nacional do Ministério Público aprovou a Resolução nº 288, para disciplinar a gestão, apreensão, custódia e liquidação de ativos virtuais definidos na Lei nº 14.478, de 21 de dezembro de 2022.

O referido texto apresenta recomendações pontuais que, do ponto de vista da apreensão correta dos ativos, podem trazer avanços significativos para persecuções penais envolvendo transações em *blockchain*. Contudo, ele também pode evidenciar uma visão limitada sobre o cenário atual, especialmente considerando o perfil dos usuários da tecnologia.

Há dois eixos, por assim dizer, que podem ser adotados pelos usuários e podem reduzir ou elevar o grau de complexidade em uma apreensão de ativos referentes a ilícitos penais. Um, é relativo à utilização de plataformas centralizadas para realizar as operações de criptoativos que, sem maiores complicações, permite o bloqueio de toda a carteira de forma simplificada, por simples comunicação entre Poder Judiciário e empresa privada.

Ocorre que, embora muitos usuários iniciem operações em plataformas centralizadas, o estudo de Milorava (2024) demonstrou que fatores como "Inovação Pessoal em TI (PIIT)" e "Consciência Tecnológica (TA)" influenciam significativamente a intenção de adotar a autocustódia. Segundo a pesquisa:

Nossa análise de 131 respondentes diversos revela que as Condições Facilitadoras (FC), aprimoradas pela inclusão da Consciência Tecnológica (TA), juntamente com a Inovação Pessoal em TI (PIIT) e a Influência Social (SI), influenciam significativamente a intenção de adotar carteiras de criptomoedas de autocustódia (Milorava, 2024, tradução nossa).³

³ Texto original: *Our analysis of 131 diverse respondents reveals that Facilitating Conditions (FC), enhanced by the inclusion of Technology Awareness (TA), along with Personal Innovativeness in IT (PIIT) and Social Influence (SI), significantly influence the intention to adopt self-custody cryptocurrency wallets.*

Ponto básico, no contexto da apreensão de criptoativos, é estabelecer uma clara distinção entre os casos de criptoativos em custódia do investigado e os casos em que está sob a custódia de uma plataforma de negociações (*exchange*). Na hipótese de o investigado ser o detentor das chaves privadas, ele possui a autonomia e a capacidade de gerenciar e dispor dos criptoativos, usufruindo dos poderes inerentes à sua posse.

Na segunda hipótese, o investigado possui saldos de criptoativos registrados em seu nome junto a uma *exchange*. Nesse cenário, a realidade é que os ativos digitais pertencentes ao investigado estão sob a custódia da própria *exchange*, uma vez que é essa instituição que detém as chaves privadas e, conseqüentemente, exerce o controle efetivo sobre os criptoativos. E nessa hipótese, a apreensão será relativamente simples, análoga àquela observada nas ordens de bloqueio de valores em moeda fiduciária depositados em instituições financeiras. A simples comunicação da ordem judicial, atualmente operacionalizada pelo sistema Bacenjud, é suficiente para que a instituição se abstenha de qualquer movimentação solicitada pelo titular dos valores, aguardando uma decisão judicial em sentido contrário.

Já nos casos em que os criptoativos estão sob o controle direto do investigado, a solução se mostra mais complexa. Dada a natureza digital e intangível dos criptoativos, a mera apreensão física dos dispositivos que armazenam as chaves privadas não se revela uma medida eficaz para a sua constrição. Assim, a retenção de celulares, *desktops*, laptops ou *coldwallets* é inócua, pois o acesso às chaves privadas e a subsequente movimentação dos valores podem ser realizados remotamente, mediante a utilização de senhas (*pins*) ou da frase de recuperação (*seed phrase*) das carteiras digitais. Contudo, uma vez concretizada a movimentação desses criptoativos para uma carteira custodiada pelo Estado, a irreversibilidade da operação é um fato, em virtude da imutabilidade dos registros confirmados na *blockchain*.

A Resolução 288/24 do CNMP aborda essa diferenciação, estabelecendo procedimentos distintos para cada situação. O artigo 4º da proposta regulamenta a situação em que os criptoativos estão sob a guarda das *exchanges*, bastando a emissão de uma ordem judicial para que essas entidades procedam ao bloqueio da movimentação dos ativos digitais. Enquanto o art. 5º prevê que, no cumprimento das diligências de apreensão de criptoativos cujas chaves privadas estejam em poder do investigado, a ordem judicial seja executada de imediato, com a transferência instantânea dos criptoativos para endereços públicos sob o domínio do Estado. Visando, por consectário lógico, mitigar os riscos de frustração da medida por acesso remoto de terceiros alheios à diligência.

Durante a tramitação da Proposição nº 1.00343/2023-31, um dos pontos debatidos pelo relator Jaime De Cassio Miranda em seu voto, foi a previsão da "liquidação imediata" dos ativos apreendidos. Em sua fundamentação acolheu a sugestão de supressão da expressão "imediata" no § 4º, inciso VI, do art. 5º, sob a justificativa de que a independência funcional do Ministério Público (art. 127, § 1º, da CF/88) conferiria ao órgão a discricionariedade para escolher o momento oportuno da conversão dos ativos em moeda fiduciária.

Sendo cada órgão de execução (Promotores de Justiça e Procuradores dos mais diferentes ramos do Ministério Público da União e dos Ministérios Públicos dos Estados) dotado de independência funcional suficiente para conduzir as apurações da forma que melhor lhe aprouver a consciência, também lhe cabe a escolha do momento mais oportuno para a liquidação de ativos, considerando a sua natureza e as suas características, além da sua alta volatilidade, que pode resultar até mesmo danos ao Sistema Financeiro Nacional, se considerarmos as altas significativas e quedas bruscas no seu valor, quando da troca do ativo virtual por moeda fiduciária (CNMP, 2024).

O que se critica nesse estudo vem justamente nesse ponto. Embora a expressão tenha sido retirada do art. 5º, que trata do requerimento judicial de apreensão, ela permaneceu hígida no *caput* do art. 8º, que estabelece que o membro do Ministério Público “deverá adotar todas as providências cabíveis visando obter autorização judicial para sua imediata liquidação”.

Insuficiente, portanto, a evocação do relator, já que a expressão “imediata” permaneceu no art. 8º que dispõe sobre a exata mesma medida.

A fundamentação apresentada nesse procedimento, embora politicamente palatável para a classe ministerial, é juridicamente equivocada ao tratar a liquidação como uma faculdade decorrente da consciência do promotor. O óbice à liquidação imediata de ativos de um investigado não decorre da autonomia do órgão acusador, mas sim do princípio da presunção de inocência (art. 5º, LVII, da CF/88). Liquidar ativos virtuais — bens que, por natureza, possuem alta volatilidade e potencial de valorização — antes de uma sentença condenatória transitada em julgado equivale à antecipação dos efeitos da pena.

O Estado retira do investigado não apenas a posse do bem, mas o próprio acesso integral à prova aos operadores do direito. A preservação da cadeia de custódia se esvai e eventual solução absolutória fará com que a devolução do valor em moeda fiduciária não venha a corresponder ao verdadeiro patrimônio do indivíduo.

Não é preciso aprofundar às relações de mercado para mencionar que os criptoativos possuem determinado valor de mercado e apresentam grande volatilidade em curtos períodos de tempo.

Não se nega que a apreensão do produto do crime (criptoativos) e a transferência à uma carteira custodiada pelo Estado é necessária para acautelar a investigação. Contudo, operar no sentido da imediata troca dos ativos por uma *stablecoin* viola, além da presunção de inocência, a própria cadeia de custódia.

Aqui, alguns pontos são fundamentais para analisar a coerência da Resolução. Em primeiro lugar, retira-se o acesso integral à prova e viola-se os artigos federais da preservação da prova. Por consequência, apesar das transações serem rastreáveis e imutáveis, permitindo conferir quais redes e criptoativos foram utilizados no suposto ilícito, a *blockchain* apresenta grande variedade de redes e fatores de mercado que podem impedir a liquidação da totalidade dos criptoativos. Ou seja, além de questionável sob a perspectiva da integridade, tal procedimento apresenta impasses, notadamente quando a liquidação integral se mostrar inviável, seja por ausência de liquidez de mercado, seja pela impossibilidade de conversão em moeda fiduciária devido à natureza do bem virtual. Ademais, a imediata liquidação equivale a apreender bens objeto do crime e vendê-los para obter dinheiro vivo, retirando aos operadores do direito e peritos a possibilidade de acesso íntegro ao objeto conforme encontrado.

Aliás, vale reprisar que a volatilidade do mercado pode beneficiar ou prejudicar o investidor em poucos meses. Entretanto, a venda desses ativos, antes de qualquer sentença condenatória, produz efeitos irreversíveis àquele que está sendo investigado.

Em outros termos, apreende-se os alegados objetos do crime, procedendo a conversão em moeda fiduciária, sem qualquer relevância aparente - exceto pela volatilidade do mercado, que pouco importa a uma ação penal, já que os ativos poderiam permanecer em custódia exclusiva do Estado.

Embora a *blockchain* ofereça a segurança e a imutabilidade necessárias à validação probatória em ambiente virtual, a Resolução nº 288/2024 do CNMP, ao tentar normatizar o tema, incorre em vícios de inconstitucionalidade. É imperativo reprisar que a busca pela eficácia punitiva encontra limite intransponível nas garantias fundamentais e na preservação da prova.

4 CONCLUSÃO

Abrindo um breve parêntesis, não é demasiado destacar que a cadeia de custódia da prova digital não é um mero formalismo, devendo ser compreendida como um instrumento indispensável ao controle epistêmico da prova e à garantia dos direitos fundamentais. Nesse sentido, a diretriz de “liquidação imediata” de criptoativos apreendidos, estabelecida pela Resolução nº 288/2024 do CNMP, fomenta uma medida equivocada, tecnicamente precipitada, em razão de três eixos, por assim dizer.

Primeiro, a doutrina e a jurisprudência do STJ (Brasil, STJ, 2023) estabelecem que a finalidade precípua da cadeia de custódia é garantir a “mesmidade” da prova, assegurando que o elemento valorado em juízo seja idêntico ao coletado. A liquidação, leia-se conversão dos criptoativos do investigado em *stablecoin*, promove a destruição prematura do “corpo de delito” digital, impedindo que a defesa e peritos exerçam o contraditório sobre o objeto em sua forma nativa e original.

Segundo, a gestão de ativos virtuais deve ser regida pelo Princípio da Precaução, que impõe ao Estado o dever de adotar à medida que cause o menor dano potencial ao investigado diante de incertezas científicas e volatilidade de mercado (Marinho, 2025). A liquidação antecipada ignora que, em caso de futura absolvição, a devolução de valores em moeda fiduciária raramente recomporá o patrimônio original, restando patente a antecipação dos efeitos da pena e violação direta à presunção de inocência.

Terceiro, diferentemente das justificativas para adotar a alienação imediata como parte fundamental da persecução, vê-se que a própria arquitetura *blockchain* oferece soluções de autocustódia e notariação descentralizada que tornam a venda do bem desnecessária para fins de segurança. A adoção de contratos inteligentes para automatizar a coleta e a rastreabilidade das evidências, por exemplo, faz com que múltiplos atores (Polícia, MP, Defesa) auditem a integridade e o histórico de manuseio do ativo (Silva, 2024).

Também, a adoção da identidade autossobrerana (do inglês *Self-Sovereign Identity* – SSI) e as provas de conhecimento zero (do inglês *Zero-Knowledge Proofs* – ZKP) explicam o controle de acesso em cadeias de custódia digitais, permitindo que o usuário detenha controle total sobre seus dados identitários através dos identificadores descentralizados (DIDs) e das credenciais verificáveis (do inglês *Verifiable Credentials* – VCs). Enquanto a SSI elimina a necessidade de repositórios centrais vulneráveis a vazamentos, a técnica de ZKP permite que um perito ou autoridade prove que possui as permissões necessárias para acessar uma evidência⁴ sem revelar qualquer dado pessoal sensível ou o valor exato de seus atributos para o sistema verificador (Moraes, 2025).

Em vez de alienar o bem por receio de manipulação ou falta de controle, o Estado pode implementar um sistema de gestão de evidências onde o acesso é controlado de forma granular por credenciais verificáveis, como o formato *AnonCreds*⁵, que suporta ZKPs. Permitindo, portanto, que os operadores do direito auditem a integridade e o histórico de manuseio do ativo sem que a posse física ou a natureza nativa do criptoativo seja alterada (Moraes, 2025).

⁴ por exemplo: “nível de autorização ≥ 2 ”

⁵ o termo *AnonCreds* refere-se a *Anonymous Credentials* (Credenciais Anônimas).”

Em conclusão, a independência funcional do Ministério Público, utilizada pelo voto condutor na Proposição nº 1.00343/2023-31 (que aprova a Resolução nº 288/2024 do CNMP) não pode servir para dar a falsa permissão ao órgão persecutório para violar a presunção de inocência. A preservação da integridade probatória e o respeito às garantias constitucionais devem prevalecer sobre a mera eficiência arrecadatória, assegurando que o avanço tecnológico sirva como escudo às garantias fundamentais e não como instrumento de arbítrio estatal em patente violação a presunção de inocência.

5 REFERÊNCIAS

BADARÓ, Gustavo Henrique Righi Ivahy. **Direito processual penal**. Rio de Janeiro: Elsevier, 2008;

BRASIL. Superior Tribunal de Justiça. ***Agravo Regimental no Habeas Corpus n. 746.715/SE***. Relatora: Ministra Laurita Vaz. Sexta Turma. Diário da Justiça Eletrônico, Brasília, DF, 26 maio 2023;

BRASIL. Superior Tribunal de Justiça. ***Agravo Regimental no Recurso em Habeas Corpus n. 143.169/RJ***. Relator: Ministro Messod Azulay Neto; Relator para o acórdão: Ministro Ribeiro Dantas. Quinta Turma. Julgado em 7 fev. 2023. Diário da Justiça Eletrônico, Brasília, DF, 2 mar. 2023;

BRASIL. Superior Tribunal de Justiça. ***Habeas Corpus n. 138.089/SC***. Relator: Ministro Felix Fischer. Quinta Turma. Julgado em 2 mar. 2010. Diário da Justiça Eletrônico, Brasília, DF, 22 mar. 2010;

BRASIL. Superior Tribunal de Justiça. ***Recurso em Habeas Corpus n. 77.836/PA***. Relator: Ministro Ribeiro Dantas. Quinta Turma. Julgado em 5 fev. 2019. Diário da Justiça Eletrônico, Brasília, DF, 12 fev. 2019;

BRASIL. Superior Tribunal de Justiça. ***Recurso em Habeas Corpus n. 114.683/RJ***. Relator: Ministro Rogerio Schietti Cruz. Sexta Turma. Julgado em 13 abr. 2021. Diário da Justiça Eletrônico, Brasília, DF, 27 abr. 2021;

BRASIL. Supremo Tribunal Federal. **Súmula Vinculante n. 14**, de 2 fev. 2009. Disponível em: <https://portal.stf.jus.br/jurisprudencia/sumariosumulas.asp?base=26&sumula=1230>. Acesso em: 25 jul. 2025;

BRASIL. *Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD)*. Diário Oficial da União, Brasília, DF, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 25 jul. 2025;

CHAINALYSIS. **The 2025 Crypto Crime Report**. New York: Chainalysis, 2025;

BRASIL. Conselho Nacional do Ministério Público. **Voto do Relator na Proposição nº 1.00343/2023-31**. Relator: Conselheiro Jaime de Cassio Miranda. Brasília, DF: CNMP, 13 mar. 2024.

CONSELHO NACIONAL DO MINISTÉRIO PÚBLICO. **Resolução n. 288, de 19 de março de 2024**. Disciplina a atuação dos membros do Ministério Público em feitos envolvendo a apreensão, custódia e liquidação de ativos virtuais e dá outras providências. *Diário Oficial da União*, Brasília, DF, 19 mar. 2024. Disponível em: <https://www.cnmp.mp.br/portal/images/CALJ/resolucoes/RESOLUO-288-2024--CNMP.pdf>. Acesso em: 25 jul. 2025.

GOMES FILHO, Antonio Magalhães. **A motivação das decisões penais**. São Paulo: Revista dos Tribunais, 2013;

LOPES JR., Aury. **Direito processual penal**. 16. ed. São Paulo: Saraiva Educação, 2019;

MARINHO, Marianna Rezende de Lucena. **A (i)licitude das provas geradas por inteligência artificial em compliance criminal no processo penal: *blockchain* como possível solução**. 2025. Dissertação (Mestrado em Direito e Ciência Jurídica) – Faculdade de Direito, Universidade de Lisboa, Lisboa, 2025.

MILORAVA, Dmitrii. **Do users understand and want self-custody?: insights from an extended UTAUT perspective**. Master's thesis – University of Twente, Enschede, 2024;

MORAES, Luan Diniz. **Cadeia de Custódia Forense Usando Hyperledger Fabric e Controle de Acesso via Hyperledger Identus**. 2025. 131 f. Trabalho de Conclusão de Curso (Graduação em Ciências da Computação) – Centro Tecnológico, Universidade Federal de Santa Catarina, Florianópolis, 2025;

PARODI, Lorenzo. **Perícia defensiva em provas digitais no processo penal: origem, custódia, integridade e integridade**. São Paulo: Thomson Reuters Brasil, 2024;

PETRONI, Benedito Cristiano Ap.; GONÇALVES, Rodrigo Franco. **Smart contracts baseados em *blockchain* na cadeia de custódia digital: uma proposta de arquitetura**. In: THE TENTH INTERNATIONAL CONFERENCE ON FORENSIC COMPUTER SCIENCE AND CYBER LAW, 2018;

PRADO, Geraldo. **Prova penal e sistema de controle epistêmicos: a quebra da cadeia de custódia das provas obtidas por métodos ocultos**. São Paulo: Marcial Pons, 2014;

SILVA, Fabian Andrade et al. **Modelo computacional para cadeia de custódia digital: identificação e coleta com base em tecnologia *blockchain***. 2024. Dissertação (Mestrado em Computação Aplicada) – Universidade Tecnológica Federal do Paraná, Curitiba, 2024;