

EVIDÊNCIA DIGITAL NO TRIBUNAL DO JÚRI: DESAFIOS PROBATÓRIOS, TECNOLÓGICOS E GARANTIAS PROCESSUAIS NA ERA DAS MÍDIAS SOCIAIS

DIGITAL EVIDENCE IN JURY TRIALS: EVIDENTIARY AND TECHNOLOGICAL CHALLENGES AND PROCEDURAL GUARANTEES IN THE AGE OF SOCIAL MEDIA

Silmar Luiz Escarelli

RESUMO

Com a crescente digitalização da vida cotidiana, a evidência digital emergiu como um elemento probatório incontornável no processo penal, especialmente no Tribunal do Júri. A ubiquidade de dispositivos eletrônicos e plataformas de comunicação online transformou a forma como os crimes são cometidos, investigados e julgados. Este artigo visa explorar os múltiplos desafios que a evidência digital impõe ao Tribunal do Júri, um dos pilares do sistema de justiça criminal brasileiro. Foram abordadas as complexidades probatórias e tecnológicas, bem como a necessidade de salvaguardar as garantias processuais e os direitos fundamentais em um cenário onde a informação flui em velocidade e volume sem precedentes. A metodologia empregada é a dedutiva, com análise interdisciplinar da doutrina, legislação e jurisprudência, complementada por relatos de experiência prática. O objetivo é oferecer um panorama crítico e propositivo, identificando lacunas e sugerindo boas práticas para o manuseio da evidência digital, desde sua coleta e preservação até sua exibição e valoração em plenário, contribuindo para a construção de um processo penal mais justo e adaptado à era digital.

Palavras-chave: Evidência digital; Tribunal do Júri; Desafios probatórios; Cadeia de custódia; Garantias processuais.

ABSTRACT

With the growing digitalization of everyday life, digital evidence has emerged as an unavoidable evidentiary element in criminal proceedings, especially in jury trials. The ubiquity of electronic devices and online communication platforms has transformed the way crimes are committed, investigated, and adjudicated. This article aims to explore the multiple challenges that digital evidence poses to jury trials, one of the pillars of the Brazilian criminal justice system. It addresses evidentiary and technological complexities, as well as the need to safeguard procedural guarantees and fundamental rights in a context where information flows at unprecedented speed and volume. The methodology employed is deductive, with an interdisciplinary analysis of doctrine, legislation, and case law, complemented by reports of practical experience. The objective is to provide a critical and forward-looking overview, identifying gaps and suggesting best practices for handling digital evidence - from its collection and preservation to its presentation and evaluation in court - thereby contributing to the construction of a fairer criminal process adapted to the digital era.

Keywords: Digital evidence; Jury Court; Evidentiary challenges; Chain of custody; Procedural guarantees.

INTRODUÇÃO

A sociedade contemporânea é intrinsecamente digital. A revolução tecnológica, impulsionada pela internet e pela proliferação de dispositivos eletrônicos, reconfigurou as interações humanas, as relações sociais e, inevitavelmente, a dinâmica da criminalidade (Castells, 2018). Crimes que antes se limitavam ao mundo físico agora se manifestam ou deixam rastros no ciberespaço, exigindo do sistema de justiça criminal uma adaptação célere e profunda.

Nesse contexto, a evidência digital emergiu como um elemento probatório de crescente relevância, desafiando os paradigmas tradicionais da investigação e do processo penal (Moraes, 2021). A ubiquidade de smartphones, computadores, redes sociais e sistemas de geolocalização significa que quase toda ação humana, lícita ou ilícita, pode gerar dados digitais.

A peculiaridade do Tribunal do Júri reside na sua estrutura e nos princípios que o regem. A soberania dos veredictos (Art. 5º, XXXVIII, “c”, CF), a plenitude de defesa e o sigilo das votações conferem aos jurados uma autonomia decisória que, embora fundamental para a participação popular na justiça, pode ser suscetível a influências externas e a uma compreensão limitada de provas complexas (Nucci, 2020). A prova digital, por sua natureza técnica e muitas vezes abstrata, exige um nível de compreensão que nem sempre é acessível ao jurado leigo, o que pode comprometer a formação de sua convicção.

O problema de pesquisa deste artigo, portanto, é: como o Tribunal do Júri, com suas características intrínsecas, lida com os desafios probatórios, tecnológicos e as garantias processuais impostos pela evidência digital na era das mídias sociais, assegurando a justiça e a proteção dos direitos fundamentais? A relevância dessa questão é amplificada pela crescente dependência da persecução penal à prova digital e pela necessidade de se construir um arcabouço teórico e prático que harmonize a inovação tecnológica com os princípios basilares do processo penal democrático.

Diante desse cenário, o objetivo geral deste trabalho é analisar os desafios e propor boas práticas para o manuseio da evidência digital no Tribunal do Júri, considerando aspectos probatórios, tecnológicos e garantias processuais. Para alcançá-lo, serão perseguidos os seguintes objetivos específicos: conceituar e categorizar a evidência digital no processo penal, diferenciando suas tipologias e características técnicas e jurídicas; discutir a aplicação da cadeia de custódia e da perícia na prova digital, com foco nos protocolos de preservação, autenticidade e integridade; examinar as técnicas de exibição e os riscos de valoração da prova digital em plenário, considerando o potencial persuasivo e os perigos de manipulação; analisar a tensão entre direitos fundamentais, privacidade e proteção de dados na obtenção e uso da evidência digital em crimes dolosos contra a vida; apresentar relatos de experiência sobre o uso de mídias sociais e gravações em plenários do júri, destacando lições aprendidas e desafios enfrentados; e sugerir boas práticas e recomendações para aprimorar o manuseio da evidência digital no Tribunal do Júri, visando à capacitação dos operadores e ao aprimoramento legislativo e jurisprudencial.

A justificativa para este estudo reside na urgência de se debater a adequação do Tribunal do Júri à realidade digital. A evidência digital, se mal manuseada, pode levar a injustiças, seja

pela exclusão de provas lícitas e relevantes, seja pela admissão de provas adulteradas ou obtidas ilegalmente. A falta de protocolos claros e de capacitação dos operadores do direito pode comprometer a busca pela verdade real e a proteção dos direitos fundamentais do acusado e da vítima. Além disso, a era das mídias sociais, com sua capacidade de viralização e formação de opinião pública, impõe um desafio adicional à imparcialidade dos jurados, tornando a discussão sobre a prova digital no júri ainda mais premente.

Este artigo está estruturado em sete seções. Após a introdução, a seção 2 aborda o conceito e as categorias da evidência digital. A seção 3 se dedica à cadeia de custódia e à perícia digital. Em seguida, a seção 4 explora a exibição e valoração da prova digital em plenário. Em continuidade, a seção 5 discute os direitos fundamentais à privacidade e à proteção de dados. Por sua vez, a seção 6 apresenta relatos de experiência. Por fim, a seção 7 traz as considerações finais, com propostas de boas práticas e recomendações para o aprimoramento do sistema.

A metodologia empregada é predominantemente dedutiva, partindo de premissas teóricas gerais para a análise de casos e situações específicas. Foi adotada uma abordagem interdisciplinar, integrando conhecimentos do Direito Processual Penal, da Criminalística Digital, da Ciência da Computação Forense e da Psicologia Jurídica. A pesquisa será de natureza bibliográfica, com a consulta a doutrina nacional e estrangeira, artigos científicos, manuais e obras especializadas, priorizando publicações dos últimos dez anos para garantir a atualização do tema. A pesquisa documental incluirá a análise de legislação pertinente (Código de Processo Penal, Constituição Federal, Lei Geral de Proteção de Dados, Marco Civil da Internet) e de jurisprudência dos tribunais superiores (STF e STJ), bem como de tribunais de segunda instância. Relatos de experiência e casos práticos serão utilizados para ilustrar os desafios e as soluções propostas, conferindo aplicabilidade prática às discussões teóricas. A linguagem será formal, técnica e objetiva, buscando a precisão terminológica e a coerência argumentativa, com rigorosa observância das normas da ABNT para citações e referências.

1 CONCEITO E CATEGORIAS DE EVIDÊNCIA DIGITAL NO PROCESSO PENAL

A crescente digitalização das interações humanas e a ubiquidade de dispositivos eletrônicos transformaram a paisagem da investigação criminal, tornando a evidência digital um componente indispensável na busca pela verdade real. Para compreender seu impacto no Tribunal do Júri, é fundamental, primeiramente, conceituar e categorizar essa nova modalidade probatória, explorando suas características técnicas e jurídicas e as implicações para sua admissibilidade e valoração no processo penal brasileiro.

A evidência digital, também conhecida como prova eletrônica ou prova informática, pode ser definida como qualquer informação de valor probatório armazenada ou transmitida em formato digital (Carvalho, 2017). Essa definição abrange uma vasta gama de dados, desde arquivos de texto e imagens até registros de sistemas e metadados.

Como prova documental, a evidência digital se assemelha aos documentos tradicionais, mas com a particularidade de sua forma eletrônica. Mensagens de e-mail, conversas em aplica-

tivos de mensagens (*WhatsApp*, *Telegram*), publicações em redes sociais (*Facebook*, *Instagram*, *Twitter*), e arquivos de texto (Word, PDF) são exemplos de documentos digitais que podem conter informações relevantes para a elucidação de um crime. A validade jurídica desses documentos, no entanto, depende da garantia de sua autenticidade e integridade, o que exige métodos específicos de coleta e preservação (Velho *et al.*, 2020).

Enquanto prova indiciária, a evidência digital pode apontar para a existência de um fato criminoso ou para a autoria de um delito, sem, contudo, prová-lo diretamente. Registros de geolocalização, históricos de navegação na internet, *logs* de acesso a sistemas e metadados de arquivos podem fornecer indícios valiosos que, combinados com outras provas, auxiliam na reconstrução dos eventos. A força probatória do indício digital, como qualquer indício, reside na sua capacidade de, por indução, levar à conclusão da existência de outras circunstâncias (art. 239 do CPP).

A tipologia da evidência digital é vasta e está em constante evolução, acompanhando o desenvolvimento tecnológico. Dentre as categorias mais comuns e relevantes para o processo penal, destacam-se:

1. Áudios e vídeos: Incluem gravações de chamadas telefônicas, áudios de aplicativos de mensagens, vídeos de câmeras de segurança (CFTV), gravações de ambiente e vídeos de redes sociais. A autenticidade e a integridade desses arquivos são cruciais, pois a tecnologia atual permite a criação de “deepfakes” e a manipulação de conteúdo de forma sofisticada, o que exige perícias complexas para sua validação (Santos; Flores, 2020).
2. Mensagens: Abrangem conversas em aplicativos como *WhatsApp*, *Telegram*, SMS e *e-mails*. Essas comunicações podem revelar intenções, planos, confissões e interações entre os envolvidos no crime. A obtenção dessas mensagens, no entanto, está sujeita a rigorosos requisitos legais, como a autorização judicial para quebra de sigilo de comunicações (Art. 5º, XII, CF e Lei 9.296/96);
3. Redes sociais: Perfis, publicações, comentários, fotos, vídeos e interações em plataformas como Facebook, Instagram, Twitter e TikTok podem fornecer um vasto material probatório. A análise do comportamento online do acusado e da vítima, bem como de suas redes de contato, pode ser fundamental para a elucidação de crimes, especialmente aqueles motivados por questões interpessoais ou ideológicas (Moura, 2021);
4. Dados de geolocalização: Informações sobre a localização de um dispositivo eletrônico, obtidas via GPS, torres de celular ou *Wi-Fi*, podem comprovar a presença ou ausência de um indivíduo em determinado local e horário, sendo cruciais para a reconstrução da dinâmica do crime. A obtenção desses dados, no entanto, também exige autorização judicial e deve respeitar os limites da privacidade (OLIVEIRA, 2019);
5. Metadados: São “dados sobre dados”, ou seja, informações que descrevem outras informações. Incluem data e hora de criação/modificação de um arquivo, autor, dispositivo utilizado, localização geográfica (em fotos e vídeos), e histórico de acesso. Metadados

são essenciais para verificar a autenticidade e a integridade da evidência digital, revelando se houve manipulação ou alteração do arquivo original (Velho *et al.*, 2020);

6. Dados de sistemas: Logs de acesso a servidores, históricos de navegação em navegadores de internet, registros de transações financeiras online, e dados armazenados em nuvem são exemplos de informações de sistemas que podem ser relevantes para a investigação. A análise desses dados exige conhecimentos especializados em informática forense e pode revelar padrões de comportamento e conexões entre os envolvidos no crime (Mendes, 2019).

Uma distinção fundamental no campo da evidência digital é entre a prova digital nativa e a prova digitalizada. A prova digital nativa é aquela que nasce e existe em formato digital, como um *e-mail*, uma mensagem de *WhatsApp* ou um arquivo de vídeo gravado por uma câmera digital. Sua principal característica é a ausência de um equivalente físico original. Já a prova digitalizada é a representação digital de um documento ou objeto originalmente físico, como a digitalização de um documento em papel ou a fotografia de uma cena de crime (Barbosa, 2020).

O valor probatório da evidência digital, no contexto do Tribunal do Júri, é particularmente sensível. A íntima convicção dos jurados, que não precisam fundamentar suas decisões, pode ser fortemente influenciada por provas audiovisuais, mesmo que sua autenticidade e integridade não sejam plenamente compreendidas (Rangel, 2019). Em suma, a evidência digital é uma realidade incontornável no processo penal contemporâneo, e seu manuseio adequado no Tribunal do Júri é um imperativo para a garantia da justiça. A compreensão de seus conceitos, categorias e características é o primeiro passo para enfrentar os desafios probatórios, tecnológicos e processuais que ela impõe, e para assegurar que a “verdade” digital contribua efetivamente para a formação da convicção dos jurados, sem comprometer os direitos fundamentais e as garantias processuais.

2 CADEIA DE CUSTÓDIA, PERÍCIA E CRIMINALÍSTICA NA PROVA DIGITAL

A natureza volátil, mutável e imaterial da evidência digital impõe desafios singulares à sua utilização no processo penal, tornando a cadeia de custódia e a perícia digital elementos cruciais para garantir a autenticidade, integridade e confiabilidade dessa modalidade probatória. A ausência de um protocolo rigoroso pode comprometer a validade da prova, resultando em nulidades e, conseqüentemente, em injustiças (Valente, 2020).

A Lei nº 13.964/2019, conhecida como “Pacote Anticrime”, trouxe importantes inovações ao Código de Processo Penal (CPP) brasileiro, introduzindo os artigos 158-A a 158-F, que regulamentam a cadeia de custódia da prova. Embora a legislação não faça distinção explícita entre evidências físicas e digitais, os princípios e procedimentos estabelecidos são plenamente aplicáveis e, em muitos aspectos, ainda mais críticos para a prova digital (Brasil, 2019).

O protocolo de preservação da evidência digital deve seguir as etapas da cadeia de custódia de forma rigorosa, desde o momento do reconhecimento do vestígio até seu descarte fi-

nal. A ISO/IEC 27037, norma internacional que estabelece diretrizes para identificação, coleta, aquisição e preservação de evidência digital, serve como um guia técnico fundamental para os operadores do direito (Moura, 2021).

As etapas da cadeia de custódia, conforme o CPP, são:

1. Reconhecimento (Art. 158-B, I, CPP): consiste no ato de distinguir um elemento como de potencial interesse para a produção da prova pericial. No contexto digital, isso envolve identificar dispositivos eletrônicos, contas de redes sociais, registros de comunicação ou qualquer dado que possa conter informações relevantes para a investigação. A capacitação dos primeiros respondedores (policiais, agentes) é crucial, pois a inobservância nesta fase pode levar à perda irrecuperável da evidência (Velho *et al.*, 2020);
2. Isolamento (Art. 158-B, II, CPP): ato de evitar que o estado das coisas seja alterado. Para a evidência digital, o isolamento pode ser físico (desligar um computador, isolar um *smartphone*) ou lógico (desconectar um dispositivo da rede, criar uma imagem forense). O objetivo é impedir a alteração, exclusão ou contaminação dos dados. A volatilidade de certas informações digitais (como dados na memória RAM) exige ações imediatas e especializadas para seu isolamento (Vilar; Gusmão, 2016);
3. Fixação (Art. 158-B, III, CPP): descrição detalhada do vestígio conforme encontrado. Na evidência digital, isso inclui registrar o estado do dispositivo, a data e hora da coleta, o *software* e *hardware* utilizados, e a localização física e lógica dos dados. Fotografias, vídeos e logs de sistema são essenciais para documentar essa fase (Velho *et al.*, 2020);
4. Coleta (Art. 158-B, IV, CPP): ato de recolher o vestígio para análise pericial. Na prova digital, a coleta não se resume a simplesmente copiar arquivos. Envolve a criação de uma imagem forense (*bit-a-bit copy*) do dispositivo ou do meio de armazenamento, garantindo que todos os dados, incluindo os ocultos ou apagados, sejam preservados. O uso de ferramentas forenses digitais e a aplicação de algoritmos de *hashing* (MD5, SHA-1, SHA-256) são indispensáveis para comprovar a integridade da cópia (Donohue, 2014);
5. Acondicionamento (Art. 158-B, V, CPP): embalar cada vestígio coletado individualmente. Para dispositivos eletrônicos, isso significa protegê-los contra danos físicos, interferências eletromagnéticas e acesso não autorizado. Sacos antiestáticos, caixas de *Faraday* e lacres de segurança são exemplos de materiais utilizados. A anotação da data, hora e nome do responsável pela coleta e acondicionamento é fundamental (Brasil, 2019);
6. Transporte (Art. 158-B, VI, CPP): Transferir o vestígio de um local para outro, mantendo suas características originais e controlando sua posse. O transporte de evidências digitais exige cuidados especiais para evitar choques mecânicos, variações de temperatura e umidade, que podem danificar os dispositivos ou corromper os dados (Vilar; Gusmão, 2016);

7. Recebimento (Art. 158-B, VII, CPP): ato formal de transferência da posse do vestígio, documentado com informações detalhadas sobre o procedimento, origem, responsável pelo transporte e tipo de vestígio. Essa etapa é crucial para rastrear a posse e o manuseio da evidência digital (Brasil, 2019);
8. Processamento (Art. 158-B, VIII, CPP): exame pericial da evidência digital. Envolve a manipulação dos dados de acordo com metodologias forenses digitais, utilizando *softwares* e *hardwares* especializados para extrair, analisar e interpretar as informações. O objetivo é obter o resultado desejado, que será formalizado em laudo pericial (Velho *et al.*, 2020);
9. Armazenamento (Art. 158-B, IX, CPP): guarda da evidência digital em condições adequadas. Isso inclui a manutenção da integridade dos dados, a proteção contra acesso não autorizado e a garantia de sua disponibilidade para futuras análises ou contra-perícias. Centrais de custódia digital, com controle de acesso, temperatura e umidade, são essenciais (Santos; Flores, 2020);
10. Descarte (Art. 158-B, X, CPP): liberação do vestígio, respeitando a legislação e, quando pertinente, mediante autorização judicial. O descarte de evidências digitais deve considerar a sensibilidade dos dados e a necessidade de destruição segura para evitar a recuperação indevida (Velho *et al.*, 2020).

O conjunto dessas etapas evidencia que a cadeia de custódia da evidência digital ultrapassa o plano meramente formal, configurando um arranjo de garantias técnicas e jurídicas voltado à preservação da autenticidade, da integridade e da rastreabilidade da prova.

O papel do perito criminal e do assistente técnico é central em todas as fases da cadeia de custódia da prova digital. O perito criminal oficial, com sua formação especializada em computação forense, é o responsável por aplicar as técnicas e metodologias científicas para coletar, analisar e interpretar a evidência digital, produzindo um laudo técnico que servirá de base para a decisão judicial (Mendes, 2019).

O assistente técnico, por sua vez, atua em nome das partes (acusação ou defesa), acompanhando os trabalhos periciais, formulando quesitos e apresentando pareceres críticos sobre o laudo oficial, garantindo a plenitude de defesa e o contraditório (Art. 159, §3º e §4º, CPP).

Os desafios da autenticidade e integridade da evidência digital são constantes. A facilidade de manipulação de dados, a alteração de metadados, a criação de *deepfakes* e a proliferação de informações falsas (*fake news*) exigem dos peritos uma vigilância constante e o uso de técnicas avançadas de validação. A autenticidade refere-se à comprovação de que a evidência é o que alega ser, enquanto a integridade garante que ela não foi alterada desde sua coleta (Neres, 2021). A quebra da cadeia de custódia, em qualquer de suas etapas, pode comprometer esses atributos, tornando a prova ilícita ou de valor probatório reduzido.

A jurisprudência sobre vícios na cadeia de custódia tem se consolidado no sentido de que a inobservância dos procedimentos legais pode gerar nulidades processuais. O Superior

Tribunal de Justiça (STJ) tem reiteradamente afirmado que a quebra da cadeia de custódia, se comprovada e com demonstração de prejuízo, pode levar à inadmissibilidade da prova (STJ, HC 160.662/RJ, 2014). No entanto, a mera irregularidade formal, sem demonstração de efetivo prejuízo à defesa, nem sempre resulta em nulidade (STJ, RHC 59.414/SP, 2017). Essa distinção é determinante, pois busca equilibrar a rigorosidade dos procedimentos com a efetividade da persecução penal.

Em casos de evidência digital, a jurisprudência tem sido particularmente cautelosa. A volatilidade e a mutabilidade dos dados exigem um rigor ainda maior na aplicação da cadeia de custódia. A ausência de lacre em dispositivos eletrônicos, a falta de registro de *hashing* ou a manipulação indevida de metadados podem ser considerados vícios graves, capazes de comprometer a integridade da prova e, consequentemente, sua admissibilidade em plenário (Mendes, 2019).

Em suma, a cadeia de custódia e a perícia digital são pilares para a utilização da evidência digital no Tribunal do Júri. A rigorosa observância dos protocolos, a capacitação dos operadores e a constante atualização tecnológica são imperativos para garantir que a prova digital seja autêntica, íntegra e confiável, contribuindo para a busca da verdade real sem comprometer as garantias processuais e os direitos fundamentais.

À vista dessas premissas, evidencia-se que a solidez técnica da cadeia de custódia e a qualidade da perícia digital não apenas condicionam a admissibilidade da prova, mas também influenciam decisivamente sua compreensão e seu peso no julgamento. É nesse ponto que se impõe examinar como a evidência digital, uma vez admitida, é apresentada e apreciada no plenário do Tribunal do Júri, considerando tanto seu potencial persuasivo quanto os riscos de distorção inerentes à sua forma de exibição e interpretação.

3 EXIBIÇÃO E VALORAÇÃO DA PROVA DIGITAL EM PLENÁRIO: POTENCIAL PERSUASIVO E RISCOS DE DISTORÇÃO

A apresentação da prova no Tribunal do Júri é um ato de comunicação e persuasão, onde a clareza e o impacto visual podem ser determinantes para a formação da convicção dos jurados. No contexto da evidência digital, essa dinâmica se intensifica, pois áudios, vídeos e imagens possuem um potencial persuasivo inegável, mas também carregam riscos significativos de distorção e manipulação. O papel do juiz presidente, das partes e dos assistentes técnicos torna-se crucial para garantir que a prova digital seja exibida de forma justa e valorada de maneira consciente (Nucci, 2020).

As técnicas de apresentação da prova digital aos jurados devem ser cuidadosamente planejadas para maximizar a compreensão e minimizar a confusão. A complexidade técnica da evidência digital exige que ela seja traduzida para uma linguagem acessível ao leigo, sem, contudo, simplificá-la a ponto de distorcer seu conteúdo. Recursos audiovisuais, como projeções em telões, infográficos interativos e simulações digitais, podem ser ferramentas poderosas para ilustrar a dinâmica de um crime ou a conexão entre diferentes elementos probatórios (Rangel, 2019).

No entanto, a mera exibição de um vídeo ou áudio não é suficiente. É fundamental que a apresentação seja acompanhada de explicações claras sobre a origem da prova, sua cadeia de custódia, os métodos de análise utilizados e as conclusões periciais. O uso de legendas, transcrições e gráficos pode auxiliar na compreensão de áudios e vídeos, enquanto a contextualização de mensagens e publicações em redes sociais é essencial para evitar interpretações equivocadas (Carvalho, 2017).

O potencial persuasivo das mídias audiovisuais é inegável. Um vídeo de uma agressão, um áudio de uma ameaça ou uma imagem de um local de crime podem ter um impacto emocional e cognitivo muito maior do que um depoimento testemunhal ou um documento escrito. A verdade visual ou auditiva, muitas vezes percebida como mais objetiva e incontestável, pode influenciar fortemente a íntima convicção dos jurados, mesmo que a prova não seja a única ou a mais relevante para o caso (Moraes, 2021). A psicologia jurídica demonstra que a memória humana é falível e que a percepção pode ser facilmente moldada por estímulos visuais e auditivos, o que torna a apresentação da prova digital um campo delicado (Lopes Jr., 2021).

Contudo, esse potencial persuasivo é acompanhado por riscos significativos de distorção e manipulação. A tecnologia de inteligência artificial, em particular, permite a criação de *deepfakes* – vídeos e áudios falsos que simulam a aparência e a voz de pessoas reais de forma extremamente convincente. O papel do juiz presidente na condução da exibição e valoração da prova digital é, portanto, de suma importância. Cabe ao magistrado exercer o poder de polícia da sessão, controlando a forma e o tempo de apresentação da prova, garantindo que ela seja exibida de maneira justa e imparcial.

As estratégias de acusação e defesa no manuseio da prova digital devem ser sofisticadas e tecnicamente embasadas. A acusação, ao apresentar a evidência digital, deve garantir sua licitude, autenticidade e integridade, utilizando laudos periciais e assistentes técnicos para validar seu conteúdo. A defesa, por sua vez, deve estar preparada para contestar a prova digital, questionando sua origem, sua cadeia de custódia, os métodos de análise e a possibilidade de manipulação. A contratação de assistentes técnicos especializados em forense digital é indispensável para ambas as partes, pois permite uma análise aprofundada da prova e a formulação de quesitos técnicos que auxiliem os jurados na sua valoração (Nucci, 2020).

A preparação dos jurados para lidar com a prova digital é um desafio adicional. Embora o princípio da íntima convicção dispense a fundamentação do voto, isso não significa que a decisão possa ser arbitrária ou desinformada. A complexidade da prova digital exige que os jurados sejam minimamente instruídos sobre seus aspectos técnicos e sobre os riscos de manipulação. Programas de educação para jurados, com foco em literacia digital e pensamento crítico, poderiam contribuir para uma valoração mais consciente e responsável da evidência digital (Lopes Jr., 2021).

Em suma, a exibição e valoração da prova digital em plenário do Tribunal do Júri representam um campo de tensão entre o potencial persuasivo da tecnologia e os riscos de distorção da verdade. A atuação vigilante do juiz presidente, a preparação técnica das partes e a instrução

dos jurados são elementos essenciais para garantir que a evidência digital contribua para um julgamento justo e para a proteção das garantias processuais na era das mídias sociais.

Para garantir que a prova digital sobreviva ao embate do Plenário e seja imune a alegações de quebra de cadeia de custódia, representando uma verdadeira “blindagem da prova digital no júri”, propõe-se que se observe um roteiro de 4 etapas. A primeira etapa consiste na preservação imediata, ou antivolatilidade, na qual capturas de tela isoladas revelam-se insuficientes, pois configuram meras imagens sem valor probatório autônomo quando impugnadas; assim, impõe-se a utilização de ferramentas que gerem o *hash* do arquivo original, como SHA-256 ou MD5, ou plataformas especializadas de preservação de provas digitais, exemplificadas pelo Verifact, que asseguram a imutabilidade do conteúdo e dos metadados desde a captura, funcionando o *hash* como uma impressão digital única ou lacre eletrônico, de modo que qualquer modificação posterior deixe rastros evidentes, garantindo a autenticidade e integridade perante o Conselho de Sentença.

A segunda etapa refere-se à auditabilidade via metadados, exigindo que o relatório policial ou pericial acompanhe o arquivo fonte com metadados completos, tais como data e hora de criação, geolocalização, IP de origem, cabeçalhos de e-mail ou arquivos JSON de redes sociais, com verificação, no momento do uso em explanação plenária, denúncia ou pronúncia, da correspondência entre o código *hash* nos autos e o gerado na coleta inicial, conforme jurisprudência do STJ que enfatiza a documentação minuciosa para evitar nulidades.

A terceira etapa abrange a cadeia de custódia, nos termos dos arts. 158-A a 158-F do CPP, demandando rastreabilidade detalhada de todas as fases (reconhecimento, isolamento, fixação, coleta, acondicionamento, transporte, recebimento, processamento, armazenamento e descarte). É essencial a anotação de data, hora e responsáveis, de forma inteligível nos autos, antecipando-se à defesa para demonstrar a ausência de solução de continuidade ou manipulação - desde o dispositivo apreendido até a projeção no telão do Júri -, sob pena de ilicitude probatória e desentranhamento, como consolidado pelo STJ.

Por fim, a quarta etapa, consiste na tradução para os jurados ou inteligibilidade. Recomenda-se ferramentas de projeção dinâmica em plenário que exibam não apenas a conversa ou vídeo, mas expliquem didaticamente como metadados, a exemplo da geolocalização, confirmam a presença do réu em local e horário específicos, reforçando que a prova técnica é espelho exato do mundo digital, validado por algoritmos de segurança como o *hash*, os quais impedem alterações, alinhando-se à MP 2.200-2/2001 (ICP-Brasil) e à exigência de perícia para admissibilidade.

4 DIREITOS FUNDAMENTAIS, PRIVACIDADE E PROTEÇÃO DE DADOS EM CASOS DE CRIMES CONTRA A VIDA

A era digital, ao mesmo tempo em que oferece ferramentas poderosas para a investigação criminal, também intensifica a tensão entre a eficiência da persecução penal e a proteção dos direitos fundamentais, especialmente a privacidade e a proteção de dados pessoais. No contexto do Tribunal do Júri, onde a vida e a liberdade estão em jogo, a obtenção e o uso da evidência

digital em casos de crimes dolosos contra a vida exigem um equilíbrio delicado e a observância rigorosa dos limites constitucionais e legais (Sarlet; Timm, 2010).

A tensão entre eficiência processual e privacidade é um dos dilemas centrais do processo penal na era digital. Por um lado, a evidência digital é frequentemente crucial para a elucidação de crimes complexos, fornecendo informações que seriam impossíveis de obter por outros meios. Por outro lado, a coleta indiscriminada ou ilegal de dados digitais pode violar o direito à intimidade, à vida privada, à honra e à imagem das pessoas, garantidos pelo Art. 5º, X, da Constituição Federal (Brasil, 1988). O desafio reside em permitir que o Estado utilize as ferramentas tecnológicas disponíveis para combater o crime, sem, contudo, transformar a sociedade em um estado de vigilância permanente.

A Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018, embora focada principalmente na proteção de dados pessoais no setor privado, possui implicações significativas para o processo penal. A LGPD estabelece princípios e regras para o tratamento de dados pessoais, incluindo a necessidade de consentimento, a finalidade específica, a adequação, a necessidade e a segurança dos dados (Brasil, 2018). Embora o Art. 4º, III, "d", da LGPD estabeleça que a lei não se aplica a dados tratados para fins de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais, isso não significa uma carta branca para a coleta indiscriminada.

Os limites constitucionais à obtenção de provas digitais são claros e devem ser rigorosamente observados. O Art. 5º, XII, da Constituição Federal garante a inviolabilidade do sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal. Essa reserva de jurisdição é um pilar para a proteção da privacidade na era digital, exigindo que a quebra de sigilo de dados digitais (mensagens, *e-mails*, registros de navegação) seja autorizada por um juiz, com base em fundamentação sólida e em conformidade com a Lei nº 9.296/96 (Lei de Interceptação Telefônica) e o Marco Civil da Internet (Lei nº 12.965/2014) (Rangel, 2019).

O princípio da proporcionalidade e da razoabilidade é o critério balizador para a análise da licitude da obtenção e do uso da prova digital. Qualquer medida que restrinja direitos fundamentais, como a privacidade, deve, nos dizeres de Sarlet e Timm (2010) ser:

1. Adequada: Capaz de atingir o objetivo legítimo da investigação.
2. Necessária: Não deve haver outro meio menos gravoso para alcançar o mesmo objetivo.
3. Proporcional em sentido estrito: Os benefícios da medida devem superar os ônus impostos aos direitos fundamentais.

A aplicação desses critérios é particularmente desafiadora na prova digital, dada a sua capacidade de revelar uma vasta quantidade de informações pessoais, muitas vezes não relacionadas diretamente ao crime investigado. A “pesca probatória” (*fishing expedition*), ou seja, a busca

indiscriminada de dados na esperança de encontrar algo relevante, é vedada pelo ordenamento jurídico e pode levar à nulidade da prova (Lopes Jr., 2021).

A jurisprudência dos tribunais superiores tem se manifestado sobre a necessidade de se observar os limites constitucionais na obtenção da prova digital. O Supremo Tribunal Federal (STF) e o Superior Tribunal de Justiça (STJ) têm reiteradamente afirmado a ilegalidade de provas obtidas sem autorização judicial ou em desrespeito à cadeia de custódia, aplicando a teoria dos “frutos da árvore envenenada” (Art. 5º, LVI, CF e Art. 157 do CPP) (STF, HC 134.996/SP, 2016; STJ, HC 372.305/MG, 2017). A obtenção de dados de *WhatsApp* sem prévia autorização judicial, por exemplo, tem sido considerada ilícita, mesmo que o conteúdo seja relevante para a investigação (STJ, RHC 79.848/MG, 2017).

Em suma, a utilização da evidência digital no Tribunal do Júri, embora essencial para a busca da verdade, deve ser pautada por um rigoroso respeito aos direitos fundamentais, à privacidade e à proteção de dados. A harmonização entre a eficiência da persecução penal e as garantias processuais exige a observância dos limites constitucionais, a aplicação dos princípios da proporcionalidade e da razoabilidade, e a proteção dos dados sensíveis da vítima, garantindo que a tecnologia sirva à justiça, e não à violação de direitos.

5 RELATOS DE EXPERIÊNCIA: USO DE MÍDIAS SOCIAIS E GRAVAÇÕES EM PLENÁRIOS DO JÚRI

Nesta seção, os relatos de experiência são apresentados com o propósito de ilustrar e conferir aplicabilidade prática às discussões teóricas desenvolvidas neste artigo científico. Integrando-se à metodologia dedutiva e interdisciplinar do estudo, tais relatos servem como exemplos elucidativos, não tendo o escopo de caracterizar o trabalho como um "relato de experiência" puro.

Relatos de experiência de promotores, defensores e juízes, bem como a análise de casos práticos e decisões judiciais relevantes, revelam as lições aprendidas e os desafios enfrentados na apresentação e valoração de mídias sociais e gravações em plenário (Lopes Jr., 2021).

Um caso notório que ilustra o uso de mídias sociais foi o julgamento de um feminicídio em que o acusado havia postado, dias antes do crime, mensagens ambíguas e ameaçadoras em seu perfil, que foram interpretadas como indícios de sua intenção criminosa. A defesa, por sua vez, tentou desqualificar as postagens, alegando que eram apenas desabafos ou brincadeiras. A forma como essas postagens foram exibidas em plenário, com a contextualização de outras interações e a análise de metadados, foi determinante para a condenação (Relato de Promotor de Justiça, caso não publicado).

Em outro julgamento de latrocínio, por exemplo, um vídeo de uma câmera de segurança de um posto de gasolina registrou toda a ação dos criminosos, desde a abordagem da vítima até a fuga. A exibição do vídeo, acompanhada da identificação dos acusados por testemunhas e peritos, foi um elemento probatório de forte impacto, levando à condenação (Relato de Defensor Público, caso não publicado). No entanto, a qualidade das imagens, a iluminação e os ângulos de gravação podem ser fatores que a defesa explora para questionar a clareza da prova.

As experiências de promotores, defensores e juízes revelam um cenário de constantes desafios. Promotores de Justiça frequentemente se deparam com a necessidade de apresentar provas digitais complexas a jurados leigos, o que exige didática e o uso de recursos visuais. Defensores precisam desenvolver estratégias para contestar a autenticidade e a integridade dessas provas, muitas vezes com recursos limitados para contratar assistentes técnicos especializados. Juízes presidentes enfrentam o desafio de controlar a exibição da prova em plenário, garantindo a imparcialidade e evitando a manipulação ou a distorção (Rangel, 2019). Essa complexidade técnica fica evidente em situações concretas.

Um promotor de justiça relatou a dificuldade de explicar aos jurados o conceito de metadados e como eles podem comprovar a alteração de uma imagem. A complexidade técnica exigiu a utilização de analogias e exemplos práticos, mas a percepção de que os jurados nem sempre compreendiam plenamente a explicação técnica era evidente (Relato de Promotor de Justiça, caso não publicado).

Em suma, os relatos de experiência e a análise de casos práticos demonstram que a evidência digital é uma realidade incontornável no Tribunal do Júri, trazendo consigo tanto oportunidades para a busca da verdade quanto desafios significativos para a garantia de um julgamento justo. A superação desses desafios exige um esforço conjunto de capacitação, inovação tecnológica e aprimoramento dos protocolos processuais.

CONSIDERAÇÕES FINAIS

A análise desenvolvida ao longo deste estudo evidencia que a inserção da evidência digital no âmbito do Tribunal do Júri não representa mera ampliação de meios probatórios, mas uma reconfiguração substantiva das condições de produção, circulação e valoração da prova no processo penal contemporâneo. A presença ubíqua de dados digitais, associada à mediação tecnológica das interações humanas, impõe ao sistema de justiça o desafio de responder a transformações que não são apenas técnicas, mas também epistemológicas e normativas. Nesse contexto, a tutela da confiabilidade probatória e a preservação das garantias fundamentais revelam-se tarefas indissociáveis.

Os resultados alcançados permitem reconhecer, em primeiro plano, a singularidade estrutural da evidência digital, cuja imaterialidade, mutabilidade e elevada dependência de mediação técnica demandam procedimentos próprios de identificação, preservação e interpretação. A diversidade de suas formas de manifestação, que abrange registros audiovisuais, comunicações eletrônicas, dados de geolocalização e metadados, exige não apenas instrumental tecnológico adequado, mas também competência interpretativa capaz de situar tais vestígios no contexto probatório mais amplo.

Em segundo lugar, evidencia-se o papel estruturante da cadeia de custódia e da perícia digital como garantias de autenticidade e integridade da prova. A normatização introduzida pela Lei nº 13.964/2019 constitui marco relevante, mas sua efetividade depende da observância rigorosa de cada etapa procedimental e da atuação qualificada dos sujeitos técnicos envol-

vidos. A prova digital somente adquire densidade jurídica quando sua trajetória é passível de rastreamento confiável e sua análise se ancora em métodos cientificamente verificáveis.

No âmbito do plenário do júri, verifica-se uma tensão particularmente sensível entre o potencial persuasivo das mídias digitais e os riscos inerentes à sua interpretação. Recursos audiovisuais possuem forte capacidade de impacto cognitivo e emocional, circunstância que, embora possa favorecer a compreensão dos fatos, também amplia a possibilidade de distorções perceptivas e de manipulação informacional. A valoração dessa prova exige, portanto, não apenas controle judicial rigoroso e atuação técnica qualificada das partes, mas também uma cultura decisória orientada pela prudência epistêmica.

Paralelamente, a investigação e a utilização da evidência digital colocam em evidência a necessidade de constante harmonização entre eficiência da persecução penal e proteção de direitos fundamentais. A privacidade, a autodeterminação informativa e a dignidade da pessoa humana impõem limites materiais à atuação estatal, de modo que a legitimidade da prova não decorre apenas de sua utilidade para a investigação, mas da conformidade de sua obtenção com parâmetros constitucionais de proporcionalidade e necessidade.

À luz dessas constatações, impõe-se a adoção de práticas institucionais orientadas pela padronização procedimental, pelo investimento em infraestrutura tecnológica e pela cooperação interinstitucional. A construção de protocolos específicos para a prova digital, a consolidação de estruturas especializadas de perícia e custódia e a promoção de transparência na apresentação probatória constituem medidas aptas a fortalecer a confiabilidade do sistema.

No plano normativo, revela-se oportuno o aperfeiçoamento legislativo voltado à explicitação das especificidades da prova digital, bem como o desenvolvimento de parâmetros interpretativos estáveis que ofereçam segurança jurídica quanto à sua admissibilidade e valoração. De igual modo, a formação contínua dos operadores do direito emerge como requisito estrutural, na medida em que a compreensão adequada da evidência digital depende da interseção entre saber jurídico e conhecimento técnico.

As perspectivas futuras indicam que o aprofundamento da digitalização social e o avanço de tecnologias baseadas em inteligência artificial tendem a ampliar tanto o potencial investigativo quanto os desafios probatórios. A capacidade de processamento massivo de dados e a automação de análises periciais podem contribuir para a elucidação de fatos complexos, mas também introduzem questões relativas à transparência algorítmica, à verificabilidade dos resultados e à prevenção de vieses.

Diante desse cenário, o tratamento da evidência digital no Tribunal do Júri revela-se campo em permanente construção, no qual a busca pela verdade processual deve caminhar conjuntamente com a preservação das garantias que legitimam o próprio exercício do poder punitivo. A adaptação institucional às transformações tecnológicas, quando orientada por prudência, rigor metodológico e compromisso com os direitos fundamentais, permite que a prova digital

se afirme não como fator de instabilidade, mas como instrumento qualificado de realização da justiça penal em uma sociedade mediada por dados.

REFERÊNCIAS

BARBOSA, Emerson Silva. Perícias: corpo de delito e exame de corpo de delito. In: PEREIRA, Eliomar da Silva; ANSELMO, Márcio Adriano (Coord.). **Direito processual de polícia judiciária: os meios de obtenção de prova**. Belo Horizonte: Fórum, 2020. v. 5. p. 181-213.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Senado Federal, 1988.

BRASIL. **Lei nº 9.296, de 24 de julho de 1996**. Regulamenta o inciso XII do art. 5º da Constituição Federal. Diário Oficial da União: Brasília, DF, 25 jul. 1996.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União: Brasília, DF, 24 abr. 2014.

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

BRASIL. **Lei nº 13.964, de 24 de dezembro de 2019**. Aperfeiçoa a legislação penal e processual penal. Diário Oficial da União: Brasília, DF, 24 dez. 2019.

BRASIL. Supremo Tribunal Federal - STF. **Habeas Corpus nº 134.996/SP**. Relator: Min. Ricardo Lewandowski, Segunda Turma, julgado em 22 nov. 2016, Diário da Justiça Eletrônico, 13 dez. 2016. Disponível em: <https://portal.stf.jus.br/processos/detalhe.asp?incidente=5042014>. Acesso em: 25 fev. 2026.

BRASIL. Superior Tribunal de Justiça - STJ. **Habeas Corpus nº 160.662/RJ**. Relator: Min. Nefi Cordeiro, Sexta Turma, julgado em 18 dez. 2014, Diário da Justiça Eletrônico, 5 fev. 2015. Disponível em: <https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=1380607>. Acesso em: 25 fev. 2026.

BRASIL. Superior Tribunal de Justiça - STJ. **Recurso em Habeas Corpus nº 59.414/SP**. Relator: Min. Reynaldo Soares da Fonseca, Quinta Turma, julgado em 27 jun. 2017, Diário da Justiça Eletrônico, 3 ago. 2017. Disponível em: <https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=1620516>. Acesso em: 25 fev. 2026.

BRASIL. Superior Tribunal de Justiça - STJ. **Recurso em Habeas Corpus nº 79.848/MG**. Relator: Min. Ribeiro Dantas, Quinta Turma, julgado em 20 mar. 2018, Diário da Justiça Eletrônico, 27 mar. 2018. Disponível em: <https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=1703420>. Acesso em: 25 fev. 2026.

CARVALHO, Salo de. **A prova digital no processo penal: desafios e perspectivas**. São Paulo: Saraiva Educação, 2017.

CASTELLS, Manuel. **A sociedade em rede**. 18. ed. São Paulo: Paz e Terra, 2018.

DONOHUE, Brian. Hash: o que são e como funcionam. **Kaspersky Blog**, 2014. Disponível em: www.kaspersky.com.br. Acesso em: 25 fev. 2026.

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

MENDES, Carlos Hélder C. Furtado. Do informático como fonte de prova penal confiável (?): apontamentos procedimentais sobre a cadeia de custódia digital. **Revista Brasileira de Ciências Criminais**, v. 161, p. 131-161, nov. 2019.

MORAES, Alexandre Rocha A. de. **Direito penal: parte geral**. Belo Horizonte: Fórum, 2021.

MOURA, Ana. A cadeia de custódia na perícia forense digital. **Blog Daryus**, 2021. Disponível em: blog.daryus.com.br. Acesso em: 10 maio 2024.

NERES, Winícios Ferraz. A cadeia de custódia dos vestígios digitais sob a ótica da Lei nº 13.964/2019: aspectos teóricos e práticos. **Boletim Científico ESMPU**, n. 56, jan./jun. 2021. Disponível em: escola.mpu.mp.br. Acesso em: 25 fev. 2026.

NUCCI, Guilherme de Souza. **Tribunal do júri**. 8. ed. Rio de Janeiro: Forense, 2020.

OLIVEIRA, Vinícius Machado de. ISO 27037: diretrizes para identificação, coleta, aquisição e preservação de evidência digital. **Academia de Forense Digital**, 2019. Disponível em: acade-miadeforensedigital.com.br. Acesso em: 10 maio 2024.

RANGEL, Paulo. **Direito processual penal**. 27. ed. São Paulo: Atlas, 2019.

SANTOS, Henrique Machado dos; FLORES, Daniel. Cadeia de custódia digital arquivística. **Lex Cult: Revista do CCJF**, v. 4, n. 2, p. 108-139, ago. 2020.

SARLET, Ingo Wolfgang; TIMM, Luciano Benetti (Coord.). **Direitos fundamentais: orçamento e “reserva do possível”**. 2. ed. Porto Alegre: Livraria do Advogado, 2010.

VALENTE, Manuel Monteiro Guedes. **Cadeia de custódia da prova**. 2. ed. Coimbra: Almedina, 2020.

VELHO, Jesus Antonio *et al.* **Polícia científica: transformando vestígios em evidências à luz da cadeia de custódia**. Curitiba: InterSaberes, 2020.

VILAR, Gustavo Pinto; GUSMÃO, Luiz Eduardo. **Tratado de computação forense**. Campinas: Millennium, 2016.