

PROVAS DIGITAIS NA PERSECUÇÃO CRIMINAL: CONFIABILIDADE EPISTÊMICA DE *PRINT SCREEN* DE MENSAGENS DE APLICATIVOS À LUZ DAS DECISÕES DO STJ

DIGITAL EVIDENCE IN CRIMINAL PROSECUTION: THE EPISTEMIC RELIABILITY OF APP MESSAGE *SCREENSHOTS* UNDER THE JURISPRUDENCE OF THE SUPERIOR COURT OF JUSTICE (STJ)

Pedro Henrique Rodrigues dos Santos¹

RESUMO

O artigo se propõe à realização de uma análise sobre a (in)admissibilidade das conversas realizadas em aplicativos e o uso de *prints* delas como provas no processo penal, a partir da posição estabelecida pelo Superior Tribunal de Justiça (STJ). Para esse fim, após ser feito uma breve contextualização sobre o surgimento das provas digitais e a necessidade de se repensar formas de assegurar a sua confiabilidade epistêmica, serão analisados casos que foram apreciados pelo STJ sobre o assunto e quais foram as diretrizes estabelecidas para a (in)admissibilidade desse tipo de evidência e a forma de sua valoração, no âmbito do processo penal. Os julgados selecionados serão os principais precedentes que atualmente norteiam a interpretação e a aplicação da matéria em questão e refletem a orientação consolidada da Corte sobre o tema. A escolha desses julgados visará assegurar a coerência entre os objetivos propostos pelo trabalho e a realidade jurisprudencial, permitindo uma análise crítica e atualizada da forma como o STJ vem tratando o assunto.

Palavras-chave: processo penal; prova digital; conversas em aplicativo; *print screen*; cadeia de custódia da prova; confiabilidade epistêmica da evidência.

¹ Bacharel em Direito pela Universidade Federal de Juiz de Fora – UFJF. Pós-graduado em Direito Penal e Processo Penal pela Faculdade de Direito do Vale do Rio Doce – Fadivale. Assessor de Juiz.

ABSTRACT

This article aims to conduct an analysis of the (in)admissibility of conversations carried out through messaging applications and the use of screenshots thereof as evidence in criminal proceedings, based on the position established by the Brazilian Superior Court of Justice (STJ). To that end, following a brief contextualization regarding the emergence of digital evidence and the need to rethink mechanisms for ensuring its epistemic reliability, the paper will examine cases that have been adjudicated by the STJ on the matter, as well as the guidelines established for the (in)admissibility of this type of evidence and the manner in which it should be evaluated within the framework of criminal procedure. The selected rulings comprise the main precedents that currently guide the interpretation and application of the issue in question and reflect the Court's consolidated jurisprudence on the subject. The selection of these decisions aims to ensure consistency between the objectives proposed by this study and the prevailing judicial reality, thereby enabling a critical and up-to-date analysis of how the STJ has been addressing the matter.

Keywords: criminal proceedings; digital evidence; conversations in apps; *print screen*; chain of custody of evidence; epistemic reliability of evidence.

“É sobre a prova que versam as prescrições legais mais importantes em matéria de processo criminal.” (MITTERMAIER, 2008, p. 20)

1 – INTRODUÇÃO

Nossa era é acertadamente chamada de "era digital", em razão da ampla utilização de tecnologias digitais, como computadores e celulares, os quais provocam uma crescente "virtualização" das mais variadas atividades humanas. Essa nova era, dominada pela tecnologia, além de criar novas dinâmicas advindas da hiperconectividade social, tem ensejado grandes desafios à sociedade,

especialmente pela fragmentação das relações sociais propiciadas pela internet, tornando as interações comunitárias mais fluidas e "líquidas" (BAUMAN, 2001).

A virtualização da sociedade também impacta o sistema de justiça, seja em sua forma de funcionamento (como o processo eletrônico e o "Juízo 100% digital") ou no modo de lidar com os novos conflitos advindos desta realidade.

Hoje não é incomum páginas de redes sociais serem usadas para comprovar situações jurídicas: o Tribunal Regional Federal da 4ª Região (TRF4) entendeu que foto em rede social somada a depoimentos de testemunhas comprovariam o vínculo de uma mulher com segurado falecido, de forma a justificar o pagamento de pensão por morte; uma trabalhadora no Rio Grande do Norte, que prestava serviços como babá, conseguiu comprovar a existência de vínculo empregatício tendo como prova conversas estabelecidas com a reclamada pelo aplicativo WhatsApp; o Tribunal Regional do Trabalho da 1ª Região (TRT/RJ) confirmou demissão por justa causa de uma enfermeira que teria apresentado atestado médico falso para justificar sua ausência ao serviço entre os dias 15 e 21 de agosto de 2012, sendo que fotos e comentários postados no Facebook, comprovaram que a funcionária, no mesmo período do afastamento, estava participando da 16ª Maratona do Rio de Janeiro; o Superior Tribunal de Justiça (STJ) decidiu que a divulgação de conversas mantidas por aplicativo de Whatsapp dá azo à reparação por dano moral (BRASIL, 2021).

Tais exemplos mostram que a crescente complexidade tecnológica exige a rápida adaptação do direito diante da desmaterialização – virtualização – das relações comunitárias e da crescente integração entre o físico e o digital, tornando-se essencial repensar os padrões normativos e processuais para lidar com as novas dinâmicas descortinadas na vida comunitária pela revolução tecnológica que está em curso.

No âmbito do direito probatório, a questão se torna ainda mais tormentosa, seja pela facilidade de alteração das provas digitais ou da existência de dúvidas quanto a integridade dos elementos colhidos a partir de equipamentos eletrônicos (notebooks, smartphone, tablets etc.), sobretudo diante da realidade de grande volatilidade dos dados telemáticos e de sua maior suscetibilidade a alterações, o que deve orientar o julgador a adotar uma postura de maior prudência, não tomando

acriticamente esses dados como fatos verdadeiros em si mesmos, sem necessidade de validação externa.

Diante desta realidade, o presente artigo destina-se à realização de uma breve investigação acerca da (in)admissibilidade e valoração das mensagens obtidas por meio de aplicativos de comunicação (WhatsApp, Telegram, Instagram etc.)² através de *print screen*³, no âmbito da persecução penal, abordando criticamente casos apreciados pelo STJ⁴, sob uma ótica que leve em conta a confiabilidade epistêmica desses meios de provas no âmbito do processo penal.

2 – PROVAS DIGITAIS OU *DIGITAL EVIDENCE*

A palavra prova, derivada do latim *proba*, de *probare*, implica demonstrar, reconhecer, formar juízo de algo. De forma geral, os tratados de direito definem prova como tudo que contribui para a formação do convencimento do magistrado, a fim de demonstrar, com veracidade, os fatos alegados pelas partes no processo.

Já as fontes de prova, ou seja, meio pelos quais elas são obtidas, são as pessoas (ofendido, acusado, perito, testemunha etc.) ou coisas (documentos em sentido amplo) das quais procedem as provas. Tudo que possa servir para esclarecer o fato criminoso é fonte de prova. Elas são anteriores ao processo, ou seja, derivam do fato delituoso independentemente da existência do processo. A partir delas é possível o conhecimento, por exemplo, de quais pessoas presenciaram o fato e podem servir como testemunhas. Estas, por sua vez, são introduzidas ao processo através dos meios de prova (COSTA, 2023).

Diante da importância da matéria, nada mais natural que ela encontre regulamentação legal. No que diz respeito à esfera criminal, a legislação que lida com a matéria de forma geral é o Decreto-Lei nº 3.689 de 03 de outubro de 1941 – Código de Processo Penal, que, em sua redação original, tratou das provas no seu

² As mensagens de aplicativos (app messages) referem-se às mensagens trocadas através de aplicativos de mensagens, como o WhatsApp, Telegram, Signal, entre outros. Esses aplicativos permitem que os usuários enviem e recebam mensagens de texto, fotos, vídeos, áudios e outros tipos de conteúdo, oferecendo uma alternativa à comunicação por SMS.

³ Ou seja, captura de tela (*screenshot*), a imagem da tela de um dispositivo eletrônico.

⁴ O Superior Tribunal de Justiça, por atribuição da própria constituição federal, é a corte responsável por uniformizar a interpretação da lei federal em todo o País.

Título VII (art. 155 ao art. 250) onde dispunha sobre exame de corpo de delito e das perícias em geral, do interrogatório do acusado, da inquirição do ofendido, das testemunhas, do reconhecimento de pessoas e coisas, acareações, documentos, indícios e das buscas e apreensões.

Desde sua redação original, o Código de Processo Penal de 1941 vem passando por atualizações legislativas pontuais visando o aperfeiçoamento da persecução penal.⁵ Além das reformas ao Código de Processo Penal, o legislador também estabeleceu legislações especiais para dispor sobre o direito probatório de forma específica.⁶

No entanto, até o presente momento não há uma regulamentação legal dispondo de forma satisfatória sobre as denominadas "provas digitais" no âmbito do processo penal. Isso, em parte, é justificado pela novidade do assunto, uma vez que apenas nos últimos anos esse tema tem demandado uma atenção mais detida dos operadores do direito, o que sequer era cogitado nos idos da década de 40, quando foi editado o Código de Processo Penal.

A despeito da ausência de tratamento legal da questão, a doutrina há décadas já vem se debruçando sobre o assunto, buscando delimitar conceitualmente a matéria, estabelecendo requisitos, critérios e filtros que auxiliem na sistematização racional de sua operacionalização, de modo a auxiliar a atividade judicial e também evitar-se o arbítrio e o subjetivismo no âmbito da persecução penal.

Nesse cenário, THAMAY e TAMER (2020) definem a prova digital como

o instrumento jurídico vocacionado a demonstrar a ocorrência ou não de determinado fato e suas circunstâncias, tendo ele ocorrido total ou parcialmente em meios digitais ou, se fora deles, esses sirvam como instrumento para sua demonstração. A prova digital é o meio de demonstrar a ocorrência de um fato ocorrido em meio digital, ou que tem no meio digital um instrumento de demonstração de determinado fato de seu conteúdo.

⁵ Merecem destaque a Reforma de 2008 – com as Leis nº 11.689/2008, 11.690/2008 e 11.719/2008 – que produziu significativas mudanças no procedimento dos julgamentos do Tribunal do Júri, nas disposições relativas ao direito probatório e aos direitos do ofendido, e no procedimento comum do processamento das ações penais; as alterações provocadas pela Lei nº 12.403/2011, que alterou os regimes jurídicos da prisão processual, fiança, liberdade provisória e demais cautelares; e as alterações realizadas pela Lei nº 13.964/2019 ("Pacote Anticrime").

⁶ A título de exemplo, cita-se a Lei nº 9.296/1996 que regulamenta a interceptação telefônica e a Lei nº 12.850/2013, que regulamenta a colaboração premiada e a infiltração de agentes.

VAZ (2012, p. 61), em tese doutoral específica sobre o assunto, define as provas digitais (ou *digital evidence*) como “os dados em forma digital (no sistema binário) constantes de um suporte eletrônico ou transmitidos em rede de comunicação, os quais contêm a representação de fatos ou ideias”. Elas podem ser encontradas no disco rígido de um computador, em celulares, e-mails, *pen drives* etc.

A partir desta definição, percebe-se que as provas digitais caracterizam uma nova realidade no âmbito do direito probatório, principalmente no que diz respeito a sua extração, conservação e apresentação em juízo. E é justamente por isso que a literatura especializada vem apontando diversas características que distinguem as provas digitais em relação às demais espécies de prova.

As características essenciais das provas digitais que têm sido apontadas pela literatura especializada sobre o tema é a imaterialidade, a volatilidade, o desprendimento do suporte físico, a suscetibilidade de clonagem e a necessidade de intermediação (CAVET, 2024; THAMAY; TAMER, 2022; SAAD GIMENES; ROSSI; PARTATA, 2024).

Conforme explicam SAAD, ROSSI e PARTATA (2024, p. 5):

(...) [a] **imaterialidade**, por exemplo, diz respeito à “natureza impalpável” da prova, pois os dados em formato digital não são nada além de impulsos de corrente elétrica, aos quais se atribui um sentido informacional após um processo de interpretação de uma linguagem não natural. Por ser imaterial, aponta-se também a **volatilidade** como característica: os dados digitais são frágeis e podem sofrer variações (propositais ou involuntárias), bastando, para tanto, a simples modificação da sequência numérica que os compõe. As provas digitais também apresentam integral **desprendimento do suporte físico** onde estão registradas, de modo que as informações produzidas e/ou armazenadas podem ser transferidas para outros dispositivos ou formas de armazenamento sem perder sua essência. Esta característica liga-se diretamente com a **suscetibilidade de clonagem**, o que significa dizer que estes dados permitem a realização de cópias – fiéis, idênticas e infinitas – dos arquivos digitais, desde que se promova o espelhamento dos elementos coletados. Por fim, aponta-se a **necessidade de intermediação de equipamento**: como o dado digital é uma simples sequência numérica que, isoladamente, pouco significa para o ser humano, torna-se necessário o uso de equipamentos que processem essas informações e as disponibilizem em linguagem natural, compreensível ao ser humano.

Não obstante isso, VAZ (2012, pág. 67) afirma que “a principal característica da prova digital reside no fato de se tratar de objeto imaterial (sequência numérica),

que pode ser facilmente alterado, como também pode ser copiado e difundido, necessitando de um equipamento intermediário para ser acessado.”

E é justamente em razão dessas características típicas que as provas digitais constantemente são passíveis de questionamento em relação à sua confiabilidade e autenticidade, o que levanta a discussão de sua confiabilidade epistêmica.⁷

3 – A CONFIABILIDADE EPISTÊMICA DAS PROVAS DIGITAIS

Uma vez que a prova, no âmbito do direito criminal, conforme assinalado acima, é tudo aquilo que é útil para demonstrar a veracidade de algo e que servirá para justificar a tomada de determinada decisão por parte do julgador, o problema da "verdade" e a possibilidade epistêmica de se atingi-la torna-se incontornável, mormente no contexto de provas cujas características essenciais sejam a de ser facilmente manipuladas e alteradas.

A prova é central no processo judicial como instrumento necessário para a reconstituição dos fatos e para a busca da verdade, objetivos fundamentais para a prolação de decisões justas e legitimadas perante o ordenamento jurídico.

Dessa forma, a prova pode ser concebida também como um elemento com função epistemológica, pois mediatiza o acesso ao conhecimento verdadeiro e confiável sobre determinados acontecimentos, sendo o elo de ligação entre os eventos ocorridos no mundo real (ou virtual) e a aplicação das normas jurídicas.

Ocorre que a produção e valoração da prova é especialmente peculiar no direito, uma vez que as partes a produzem em contextos limitados⁸ – as normas jurídicas estabelecem prazos específicos para a realização de determinadas provas, ao passo que impedem o uso de certas espécies de provas (v.g. ilícitas) etc. –, de

⁷ Conforme LOPES JR., MORAIS DA ROSA e SOUSA (2025), “*diferentemente dos documentos físicos — cuja materialidade e forma possibilitam verificação direta — os dados digitais são marcadamente voláteis e suscetíveis a alterações imperceptíveis, exigindo que um mediador técnico, provido de capacidades de “observar” o que leigos não conseguem: uma abordagem pericial especializada. A análise de vestígios digitais envolve a investigação de metadados, registros de sistema (logs) e a reconstrução cronológica de eventos, sendo que a perda, modificação ou coleta inadequada dessas informações pode comprometer gravemente a busca pela verdade real.*”

⁸ O que não ocorre em outros espaços, como por exemplo na pesquisa acadêmica.

forma que isso amplia ainda mais a complexidade da situação na qual o julgador tomará as decisões, que devem estar conformes aos padrões de justiça estabelecidos pelo ordenamento.

Considerando a prova como um instrumento epistemológico, descortina-se uma clara intersecção entre o direito e a epistemologia – entendida em sentido amplo como o estudo do conhecimento e sua justificação racional –, de modo que a prova assume uma função fundamental, na medida em que permite distinguir o conhecimento verdadeiro dos fatos daquilo que não ocorreu. Por conseguinte, a confiabilidade e a possibilidade de verificação das informações apresentadas são essenciais para uma valoração racional e fundamentada dos fatos.

Isso demonstra a imprescindibilidade da existência de critérios epistemológicos claros e objetivos da atividade probatória, somados a diretrizes jurisprudenciais relativamente estáveis que orientem a admissibilidade, produção e valoração desses eventos.

De forma a contornar esses problemas, a doutrina vem assinalando a necessidade dos denominados *standards* probatórios, os quais indicam o nível de convencimento necessário para se considerar uma hipótese como suficientemente comprovada. Objetiva-se, assim, o estabelecimento de critérios para a valoração racional das provas, os quais devem ser passíveis de controle intersubjetivo. O *standard* probatório tem por finalidade conferir maior confiabilidade às decisões sobre os fatos e afastar os falsos positivos⁹ que eventualmente possam ocorrer no contexto da atividade probatória em processos judiciais.

Como explicam MATIDA e VIEIRA (2019, p. 237), espera-se que um *standard* probatório promova a “*redução dos espaços de decisionismo e de arbitrariedade, além da possibilidade de um controle intersubjetivo sobre o modo como se dá a valoração das provas nas decisões judiciais*”.

Ocorre que a ascensão das provas digitais reflete uma nova dinâmica na produção e valoração das provas, exigindo-se o estabelecimento de critérios valorativos que se atentem para as peculiaridades que são intrínsecos a essa espécie de prova, de forma que as decisões judiciais, afastando-se do puro arbítrio e

⁹ Um falso positivo ocorre quando um teste ou diagnóstico indica a presença de algo (como uma doença ou condição) quando, na realidade, ela não existe.

da mera subjetividade do decisor, estejam amparadas por critérios objetivos de racionalidade e legitimada perante o ordenamento jurídico (MARINONI; ARENHART, 2022).

Diante desta tormentosa questão que é colocada com advento das provas digitais, para além das conjecturas abstratas e teóricas, é na análise dos casos concretos que chegam ao Poder Judiciário que será possível refletir sobre as eventuais soluções que podem ser dadas às questões suscitadas acerca da confiabilidade das provas digitais, o que se fará no tópico a seguir.

4 – A (IN)ADMISSIBILIDADE DE *PRINTS* DE CONVERSAS EM APLICATIVOS NA PERSECUÇÃO PENAL SOB A ÓTICA DA JURISPRUDÊNCIA STJ

Atualmente, uma das formas mais comum e generalizada de comunicação interpessoal, nas mais diversas interações sociais, é feita por meio do uso de aplicativos de mensagens (*app messages*), tais como o WhatsApp, Telegram, Signal, Facebook Messenger, Viber etc. Frequentemente, e para as mais diversas finalidades, os usuários desses mecanismos de comunicação, para preservar o conteúdo de determinado diálogo, capturam a imagem da tela do dispositivo (celular, tablet, computador etc.) onde referido conteúdo está disponível. A este procedimento, dá-se o nome de *print screen*, que basicamente significa “captura ou congelamento de tela”.

Ocorre que, dada a fácil manipulação de dados digitais, há diversos aplicativos (muitos disponíveis gratuitamente) que permitem a criação de *print screen* de conversas, apresentando o *layout* de qualquer aplicativo (*app*) de comunicação, simulando a existência de um conteúdo inexistente.

LOPES JR., MORAIS DA ROSA e SOUSA (2025) explicam que nesses casos:

A imagem é amplamente manipulável, sem metadados (dados sobre dados), nem indicadores de rastreabilidade, servindo de instrumento de manipulação, especialmente aos analfabetos digitais que, desconhecendo a facilidade de manipulação, tendem a aceitá-las acriticamente. É preciso reconhecer que diante da mera imagem, desacompanhada de qualquer

verificação técnica, é grande o risco de se cair numa sedutora armadilha cognitiva com aparência de verdade.

Ocorre que, não obstante isso, atualmente, os *print screen* passaram a ser utilizados como provas criminais, amparando a imposição de restrições à liberdade, prisões cautelares e até mesmo condenações criminais.

Muitos desses casos tem chegado no STJ, o qual, no exercício de sua atribuição constitucional de corte responsável por uniformizar a interpretação da lei federal em todo o país, tem estabelecido parâmetros para a valoração desses elementos probatórios no âmbito do processo penal. Considerando as limitações do presente trabalho, a seguir serão analisados os julgamentos realizados no AgRg no HC nº 828.054/RN, AgRg no HC nº 738.418/SP e HC nº 900.613/MG.

Os julgados acima indicados foram selecionados com base em sua relevância e representatividade no âmbito do Superior Tribunal de Justiça (STJ). Eles são os principais precedentes que atualmente norteiam a interpretação e a aplicação da matéria em questão e refletem a orientação consolidada da Corte sobre o tema. A escolha desses julgados visa assegurar a coerência entre os objetivos propostos pelo trabalho e a realidade jurisprudencial, permitindo uma análise crítica e atualizada da forma como o STJ vem tratando a controvérsia.

No julgamento do AgRg no HC nº 828.054/RN, o STJ foi instado a analisar um caso que envolvia a prisão em flagrante delito de determinado investigado que realizava em via pública a comercialização de cocaína. Na oportunidade, foi apreendido com o investigado um aparelho celular. Após obter autorização judicial para quebra de sigilo dos dados telemáticos das comunicações enviadas e recebidas pelo celular apreendido, o aparelho foi enviado para realização de perícia, a fim de que os dados fossem extraídos: registros de conversas registradas em aplicativos (WhatsApp, Instagra, Telegram etc.) e demais informações que interessassem à investigação. O perito encaminhou ao Delegado relatório de análise do aparelho e informou que a extração dos dados foi feita a partir da técnica de “*print screen*” dos diálogos, tendo em vista que os equipamentos extratores de dados (software Cellebrite¹⁰) não foram capazes de realizar a extração. A partir desses

¹⁰ Cellebrite é um software de extração e análise de dados digitais desenvolvida pela empresa israelense Cellebrite, especializada em tecnologia de perícia digital. Ele é amplamente utilizado por autoridades policiais e

elementos, a polícia descobriu a existência de uma organização criminosa voltada à prática do tráfico de drogas. A partir disso, foi deferida medida cautelar de busca e apreensão na residência dos investigados, os quais, por meio de advogado impetraram *Habeas Corpus* perante o Tribunal de Justiça, aduzindo que os elementos que embasaram a diligência não estavam acompanhados de qualquer elemento capaz de garantir sua integridade, como, por exemplo, o código Hash. Não obstante isso, a ordem denegada pelo Tribunal de Justiça. Não satisfeitos, impetraram novo *Habeas Corpus* ao STJ, insistindo na tese de quebra de cadeia de custódia e pedindo a nulidade das provas. Ressaltaram que o *print screen* é um dado altamente manipulável e pouco confiável, não assegurando a idoneidade de vestígios que é exigido pela cadeia de custódia, conforme dispõe o art. 158-A e seguintes do Código de Processo Penal.

Analisando o caso, o STJ partiu do ponto de que o instituto da cadeia de custódia, tal como disciplinado no nosso ordenamento jurídico¹¹, tem como objetivo garantir a idoneidade do tratamento dos elementos probatórios, desde a coleta até a análise e deliberação pela autoridade judicial, a fim de evitar interferências que possam comprometer a confiabilidade das provas.

Ressaltou que as provas digitais demandam uma maior atenção e cuidado em sua custódia e tratamento, diante da volatilidade dos dados telemáticos e da maior suscetibilidade a alterações, o que requer a adoção de mecanismos que assegurem a preservação integral dos vestígios probatórios, de modo que seja possível constatar eventuais alterações, intencionais ou não, dos elementos inicialmente colhidos, demonstrando-se a higidez do caminho percorrido pelo material.

Após explicitar a necessidade de observação da cadeia de custódia com as provas digitais, respeitando-se as especificidades dela, o Tribunal buscou estabelecer diretrizes técnicas sobre o tratamento das evidências digitais.

Para tanto o Tribunal se valeu das diretrizes estabelecidas por norma técnica expedida pela Associação Brasileira de Normas Técnicas, a NBR ISO/IEC

instituições de investigação para extrair e analisar dados de dispositivos móveis, como celulares e tablets, em casos de investigação criminal.

¹¹ Cf. Art. 158-A e seguintes do Código de Processo Penal, com as alterações feitas pela Lei nº 13.964 de 2019.

27037:2013, a qual estipula diretrizes acerca do manuseio inicial de evidências digitais, compreendendo sua identificação, coleta, aquisição e preservação.

Nesse passo, o STJ estabeleceu que os aspectos essenciais das evidências digitais, os quais, segundo a metodologia da ABNT, asseguram a segurança e confiabilidade epistemológica do objeto são a auditabilidade (a documentação de cada etapa da cadeia de custódia, a fim de que as partes tenham condições de aferir se o método técnico-científico para a extração dos dados foi devidamente observado), a repetibilidade (a mesma sequência de etapas sempre redunde nos mesmos resultados, é dizer, os mesmos procedimentos gerem a mesma conclusão), a reprodutibilidade (ainda que sejam utilizados métodos diversos, os resultados devem ser os mesmos) e a justificabilidade (os métodos e procedimentos devem ser justificáveis, sob a ótica da melhor técnica disponível) (BRASIL, 2024).

O STJ esclareceu que a observância dessas etapas tem por finalidade garantir o denominado princípio da mesmidade, que significa "*a correspondência entre aquilo que foi colhido e aquilo que resultou de todo o processo de extração da prova de seu substrato digital, de forma a assegurar a confiabilidade da prova ("ela é o que pretende ser").*" (BRASIL, 2024).

Portanto, o STJ concluiu que "*os instrumentos utilizados para promover a tradução dos dados digitais para uma linguagem compreensível devem ser conhecidos, confrontados e atestados, sob pena de colocar em risco toda a integridade do conteúdo de prova obtida.*" (BRASIL, 2024).

A partir das diretrizes epistemológicas lançadas, o STJ concluiu que, como a consulta dos dados foi feita diretamente no aparelho, limitando-se na realização de *print screen* – ou seja, a captura de tela (*screenshot*) do dispositivo eletrônico –, não seria possível inferir a idoneidade das provas extraídas pelo acesso direto ao celular apreendido, sem a utilização de ferramenta forense que garantisse a exatidão das evidências, não havendo registros de que os elementos inicialmente coletados são idênticos ao que constavam no relatório de investigação – feito com *print screen* dos dados –, os quais corroboraram a condenação.

O Tribunal concluiu que não houve a adoção de procedimentos que assegurassem a idoneidade e a integridade dos elementos obtidos pela extração dos dados do celular do réu, tornando as provas imprestáveis.

No julgamento do AgRg no HC nº 738.418/SP (BRASIL, 2025), a questão residia na confiabilidade da prova digital colhida - notadamente, mensagens de texto e áudio trocadas pelo aplicativo WhatsApp entre a vítima e o acusado.

No caso, um policial civil foi condenado por corrupção passiva com base em mensagens trocadas via WhatsApp entre ele e a suposta vítima.¹² O celular que continha os diálogos foi entregue voluntariamente por um dos interlocutores (a vítima), sendo que os investigadores da polícia se limitaram a transcrever/degravar as mensagens de texto e os áudios constantes no aparelho. No entanto, não houve a apreensão do aparelho celular do qual provieram referidas provas digitais e nem foi utilizada nenhuma ferramenta de preservação do conteúdo original da prova para posterior confronto, nem realizada qualquer perícia ou espelhamento dos dados, tampouco a adoção de medidas técnicas para garantir a integridade do conteúdo.

O STJ, nessa situação, concluiu que os fatos assinalavam a ausência de medidas para a sua preservação sob a ótica da auditabilidade, repetibilidade, reprodutibilidade e justificabilidade, impedindo qualquer teste de confiabilidade do conteúdo, medida que, mais do que a qualquer das partes, interessa à busca da verdade real. Afirmou que a ausência, no caso concreto, de quaisquer salvaguardas aptas à verificação da higidez da prova digital, colocavam em dúvida a confiabilidade das provas, ante a não evidenciação dos cuidados necessários à preservação da cadeia de custódia, que legalmente recai sobre o Estado, impedindo a realização de qualquer teste de confiabilidade do conteúdo digital apresentado.

Ressaltou que, embora a obtenção da prova tenha sido lícita (pois fornecida pela vítima), era o caso de reconhecer a inviabilidade do uso de tais provas em decorrência da quebra da cadeia de custódia nos momentos subsequentes à coleta da prova.

Na conclusão do julgamento, o STJ reafirmou que a cadeia de custódia deve ser preservada para garantir a confiabilidade das provas digitais e a ausência de medidas para a preservação da cadeia de custódia – que impede a realização

¹² O policial foi condenado como incurso no art. 317, *caput*, do Código Penal (corrupção passiva), a 10 anos de reclusão, em regime inicial fechado, pagamento de 50 (cinquenta) dias-multa e perda do cargo de policial civil. A apelação interposta ao Tribunal de Justiça foi parcialmente provida para redimensionar a pena em 08 (oito) anos de reclusão, regime fechado, mantidos os demais termos da sentença. O condenado impetrou *habeas corpus* no Superior Tribunal de Justiça para sustentar a ausência de preservação da cadeia de custódia, o que tornariam ilícitos os *prints* de conversa de Whatsapp que serviram de lastro para sua condenação.

qualquer teste da confiabilidade do conteúdo digital – torna a prova imprestável (BRASIL, 2025).

No julgamento do *Habeas Corpus* nº 900.613/MG, se tratava de um caso em que os pacientes haviam sido pronunciados pela suposta participação na prática do crime de homicídio qualificado, ocorrido em 3/11/2019. Dentre as provas utilizadas para a pronúncia dos pacientes haviam diversos *prints* de telas de conversas de WhatsApp, os quais não indicavam a data e hora das mensagens apresentadas.

A Defesa havia pleiteado a juntada do Relatório Cellebrite do celular indicado no relatório de investigação, que serviu de base para o pronunciamento. No entanto, o Instituto de Criminalística da Polícia Civil informou que não foi possível acessar o conteúdo das mensagens do celular (o aparelho não ligava, mesmo após longo período de tentativa de carregamento da bateria), o que importou a perda do material a ser periciado.

O STJ, seguindo o entendimento firmado no AgRg no HC n. 828.054/RN (analisado acima), considerou que nesse caso seria impossível aferir a real existência e integridade das mensagens, bem como o exato contexto em que foram enviadas, o que importaria na quebra da cadeia de custódia da prova – inexistência de procedimentos que assegurem a idoneidade e a integridade dos elementos obtidos pela extração dos dados do aparelho celular – e na imprestabilidade da prova digital.¹³

Com efeito, nos casos analisados por este artigo em que os dados das conversas foram externados por meio de *print screen* – AgRg no HC nº 828.054/RN, ArRg no HC nº 738.418/SP e HC nº 900.613/MG – o STJ entendeu que as provas eram imprestáveis em razão do desrespeito à cadeia de custódia na colheita dos dados, porquanto não houve a adoção de salvaguardas técnicas aptas à demonstração da identidade entre a cópia gerada e os vestígios digitais originais (princípio da mesmidade), ou seja, “*sem a preservação adequada e análise pericial, as imagens não possuem valor probatório seguro*” (LOPES JR.; MORAIS DA ROSA; SOUSA, 2025).¹⁴

¹³ Apesar de ter declarado a ilicitude das provas digitais e determinar seu desentranhamento dos autos, o Tribunal manteve a pronúncia dos réus, por considerar que haviam outras provas independentes do conteúdo extraído do celular apreendido que justificavam a pronúncia dos pacientes.

¹⁴ Conforme alertam LOPES JR., MORAIS DA ROSA e SOUSA, “*equivoco comum é a tentativa de suprir tais falhas com a lavratura de ata notarial, metodologia que apenas atesta que determinado conteúdo foi visualizado pelo*

A partir de tais precedentes pode-se notar que o STJ não tem admitido o uso de *print screen* – captura de tela de um dispositivo eletrônico, gerando uma imagem – como método de externalização de conversas em aplicativos de mensagens, sendo tal evidência insuficiente para a demonstração da materialidade de crimes, uma vez que, além de ser uma forma de conservação de informação facilmente manipulável/editável¹⁵, não atende as etapas da cadeia de custódia da prova, segundo a metodologia da ABNT – regulada na NBR ISO/IEC 27037:2013 –, de forma que seja assegurada a segurança e confiabilidade epistemológica da evidência.

No âmbito doutrinário, as conclusões defendidas vão ao encontro do entendimento manifestado pelo Superior Tribunal de Justiça:

(...) o mero "*print screen*" é insuficiente à demonstração da materialidade, por violação da metodologia necessária à existência e à validade do suporte material, por violação dos elementos de "definição" e de "tratamento". É que os documentos nativos do ambiente digital demandam aquisição adequada dos dados, em geral por "imagem" (*no conceito técnico e não do "print screen", por evidente*). Logo, não preenche os atributos de Definição e de Tratamento. (...) O "*print screen*" pode ser manipulado amplamente. Os dados podem ser "montados" por meio de aplicativos disponíveis nas lojas dos smartphone (*google play e apple store*), "espoliados" (*degradação por incidência de calor, umidade, campos magnéticos e/ou elétricos, quedas etc.*) ou "adulterados" (*violada a integridade, mesmidade e auditabilidade*), por aspectos inerentes à diligência de aquisição ou pela interferência de agentes externos. Por isso que agentes profissionais, assim que o dispositivo é apreendido, promovem o desligamento ou a colocação em modo avião (*evitam a adulteração por administradores ou agentes externos*). As operações policiais seguem o procedimento de imediata colocação e "modo avião". Por ser amplamente "manipulável", o "*print screen*" (*conjunto de pixels*), ao contrário do Processo Civil, em que a não contestação do réu, consolida a autenticidade, no domínio do Processo Penal a "materialidade" exige a aquisição adequada, até porque a confissão é insuficiente (MORAIS DA ROSA, 2022).

O que se verifica é que "*a validade está vinculada à garantia de integridade do modo como se capturam os dados de tráfego, de vestígios e dados digitais (inclusive conversas de Whatsapp, Telegram, Facebook, Instagram, sítios online etc.), em atenção à cadeia de custódia*" (MORAIS DA ROSA, 2022).

tabelião naquele momento, não sendo apta a comprovar a origem, a autenticidade técnica ou a ausência de manipulação anterior do material apresentado." **Como criar 'prints' falsos: quando as aparências enganam e a cadeia de custódia dos vestígios digitais.** Consultor Jurídico. 09/05/2025. Disponível em: <<https://www.conjur.com.br/2025-mai-09/como-criar-prints-falsos-quando-as-aparencias-enganam-e-a-cadeia-de-custodia-dos-vestigios-digita>>. Acesso em 24/05/2025.

¹⁵ Os dados podem ser "montados" por meio de vários aplicativos disponíveis nas lojas dos smartphones.

5 – CONCLUSÃO

O presente artigo buscou analisar a (in)admissibilidade e valoração das mensagens obtidas por aplicativos de comunicação (Whatsapp, telegrama, Instagram etc.), através da técnica de *print screen*, na persecução penal, considerando a confiabilidade epistêmica dessas provas no atual contexto do ordenamento jurídico.

Conforme pôde ser verificado, as provas digitais, definidas como "*dados em forma digital constantes de suportes eletrônicos ou transmitidos em rede*", possuem características específicas que as diferenciam das demais provas: imaterialidade, volatilidade, desprendimento do suporte físico, suscetibilidade de clonagem e necessidade de intermediação técnica. Estas características tornam tais provas facilmente manipuláveis, gerando questionamentos sobre sua confiabilidade.

Nesse cenário, foram abordados julgados em que o STJ lidou com a questão da (in)admissibilidade dessas provas no âmbito do processo penal e sua adequada valoração e que são representativos do entendimento atual do Tribunal. Da análise dos julgados é possível concluir que, para o STJ, as conversas por meio de aplicativos de mensagens, para serem admissíveis, devem observar a cadeia de custódia conforme a NBR ISO/IEC 27037:2013, estabelecida pela Associação Brasileira de Normas técnicas (ABNT), assegurando quatro aspectos essenciais: auditabilidade (possibilidade de verificar o método utilizado), repetibilidade (mesmos procedimentos geram mesmos resultados), reprodutibilidade (métodos diversos geram mesmos resultados) e justificabilidade (métodos tecnicamente adequados). Estas exigências visam garantir o “princípio da mesmidade”, onde há a correspondência entre o que foi colhido e o que resultou do processo de extração da prova, assegurando assim a sua confiabilidade epistêmica no processo penal.

Desse modo é possível concluir que o Superior Tribunal de Justiça não admite o uso de *print screen*, enquanto prova criminal, para justificar uma condenação criminal, uma vez que além de ser uma forma de conservação de informação facilmente manipulável – há vários aplicativos nas lojas dos smartphones que montam/editam *print screen* –, ele não atende as etapas da cadeia de custódia

da prova, de forma que seja assegurada a segurança e a confiabilidade epistemológica da evidência.

Justifica-se tal rigor em razão da necessidade de confiabilidade da prova para justificar uma condenação criminal, o que requer um nível de certeza acima de qualquer dúvida razoável (BRASIL, 2017; BRASIL, 2023; BRASIL, 2024), o que não é possível em contextos nos quais há evidências facilmente manipuláveis, ampliando-se o risco de provas fabricadas, colocando em risco a confiabilidade dos julgamentos do Poder Judiciário e, em última instância, sua legitimação perante o ordenamento jurídico e a Constituição.

No entanto, quando a isso, cabe uma última ressalva: embora não tenha sido objeto de análise dos julgados do Superior Tribunal de Justiça, é razoável que nas situações em que o *standard* probatório seja menos rigoroso, como nos casos de imposição de medidas cautelares ou abertura de investigações, tais evidências possam ser consideradas.

REFERÊNCIAS

- ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27037: tecnologia da informação - técnicas de segurança - diretrizes para identificação, coleta, aquisição e preservação de evidência digital. Rio de Janeiro: ABNT, 2013.
- BAUMAN, Zygmunt. Modernidade Líquida. Rio de Janeiro: Jorge Zahar Editor, 2001.
- BRASIL. Código de Processo Penal. Decreto-Lei nº 3.689, de 3 de outubro de 1941. Disponível em: <https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm>. Acessado em 04/05/2025.
- BRASIL. Superior Tribunal de Justiça. AgRg no HC n. 738.418/SP. Relator: Ministro Otávio de Almeida Toledo (Desembargador Convocado do TJSP). Sexta Turma. Julgado em: 11 mar. 2025. DJe: 21 mar. 2025.
- BRASIL. Superior Tribunal de Justiça. AgRg no HC n. 828.054/RN. Relator: Ministro Joel Ilan Paciornik. Quinta Turma. Julgado em: 23 abr. 2024. DJe: 29 abr. 2024.
- BRASIL. Superior Tribunal de Justiça. RHC n. 99.735/SC. Relatora: Ministra Laurita Vaz. Sexta Turma. Julgado em: 27 nov. 2018. DJe: 12 dez. 2018.
- CAVET, Caroline Amadori. Prova digital: créditos de admissibilidade e valoração. 1. ed. -- São Paulo: Thomson Reuters. Brasil, 2024. [livro eletrônico]
- COSTA, Érica Moreira. Sistemas de valoração das provas no processo penal. Consultor Jurídico, 20 mar. 2023. Disponível em: <https://www.conjur.com.br/2023-mar-20/erica-moreira-costa-provas-processo-penal/>. Acesso em: 4 maio 2025.
- LOPES JUNIOR, Aury; MORAIS DA ROSA, Alexandre; SOUSA, Dellano. Como criar 'prints' falsos: quando as aparências enganam e a cadeia de custódia dos vestígios digitais. Consultor Jurídico, 9 maio 2025. Disponível em: <https://www.conjur.com.br/2025-mai-09/como-criar-prints-falsos-quando-as-aparencias-enganam-e-a-cadeia-de-custodia-dos-vestigios-digitais/>. Acesso em: 24 maio 2025.
- MARINONI, Luiz Guilherme; ARENHART, Sérgio Cruz. Prova e convicção. 4. ed. São Paulo: Thomson Reuters Brasil, 2022. E-book.

MATIDA, Janaina; VIEIRA, Antonio. Para além do BARD: uma crítica à crescente adoção do standard de prova “para além de toda a dúvida razoável” no processo penal brasileiro. *Revista Brasileira de Ciências Criminais*, [s.l.], v. 156, p. 221-248, jun. 2019.

MITTERMAIER. C. J. A. *Tratado de Prova em Matéria Criminal*. 5ª Edição. Bookseller, 2008.

MORAIS DA ROSA, Alexandre. O "print screen" é insuficiente à materialidade nos crimes digitais. *Consultor Jurídico*, 17 jun. 2022. Disponível em: <https://www.conjur.com.br/2022-jun-17/limite-penal-print-screen-materialidade-crimes-digitais/>. Acesso em: 5 maio 2025.

SAAD GIMENES, Marta C.; ROSSI, Helena C.; PARTATA, Pedro H. A obtenção das provas digitais no processo penal demanda uma disciplina jurídica própria? Uma análise do conceito, das características e das peculiaridades das provas digitais. *Revista Brasileira de Direito Processual Penal*, v. 10, n. 3, p. e1071, set./dez. 2024. DOI: <https://doi.org/10.22197/rbdpp.v10i3.1071>. Acesso em: 24 maio 2025.

THAMAY, Rennan; TAMER, Maurício. *Provas no direito digital: conceito da prova digital, procedimentos e provas digitais em espécie*. 2. ed. São Paulo: Thomson Reuters Brasil, 2022. E-book.

VAZ, Denise Provasi. *Provas digitais no processo penal: formulação do conceito, definição das características e sistematização do procedimento probatório*. 2012. Tese (Doutorado em Direito) – Faculdade de Direito, Universidade de São Paulo, São Paulo, 2012. DOI: <https://doi.org/10.11606/t.2.2012.tde-28052013-153123>. Acesso em: 5 maio 2025.