A (i)legalidade da utilização de *prints* de *Whatsapp* como prova de delito à luz da jurisprudência do Superior Tribunal de Justiça

The (il)legality of using WhatsApp screenshots as evidence of a crime considering the jurisprudence of the Superior Court of Justice.

La (i)legalidad de utilizar capturas de pantalla de WhatsApp como prueba de un delito a la luz de la jurisprudencia de la Corte Superior de Justicia.

DOI: https://doi.org/10.17655/rdct.2025.e0002

Rodrigo Casimiro Reis [1]

ROR Defensoria Pública do Estado do Rio de Janeiro

http://lattes.cnpq.br/3549202502383758

https://orcid.org/0000-0003-0788-6740

1 Defensor público, Mestre em Direito Constitucional (IDP). Chefe de Gabinete de Ministra do Superior Tribunal de Justiça. Defensor Público do Estado do Maranhão. Membro do Comitê Nacional de Inteligência Artificial do Poder Judiciário, instituído pela Portaria CNJ 270/2025. Instrutor interno do Centro de Formação do STJ. Autor de prática exitosa premiada no Prêmio Innovare. Autor do livro "Verdade e Prova Penal: A cadeia de custódia na era digital". Organizador e coautor de obras jurídicas. Ex-Assessor da Presidência do STJ e da Corregedoria Nacional de Justiça | Email: r.casimiro@outlook.com

RESUMO:

A questão sobre a (i)legalidade do uso de *printscreen* de conversas realizadas pelo WhatsApp tem sido objeto de amadurecimento na jurisprudência do Superior Tribunal de Justiça, que tem decidido o assunto considerando as particularidades de cada situação específica.

PALAVRAS-CHAVE:

Cadeia de custódia. *Printscreen*. jurisprudência do STJ.

ABSTRACT:

The question of the (il)legality of using screenshots of WhatsApp conversations has been the subject of a maturing process in the jurisprudence of the Superior Court of Justice, which has been deciding the matter considering the particularities of each specific situation.

KEYWORDS:

Chain of custody. print screen. STJ case law.

RESUMEN:

La cuestión de la (i)legalidad del uso de capturas de pantalla de conversaciones de WhatsApp ha sido objeto de un proceso de maduración en la jurisprudencia del Tribunal Superior de Justicia, que ha decidido el asunto considerando las particularidades de cada situación específica.

PALABRAS CLAVE:

Cadena de custodia. Captura de pantalla, Jurisprudencia del STJ.

1. A cadeia de custódia dos vestígios de prática delitiva

Constatada a prática de uma infração penal, o Estado deve agir, de forma diligente, com o escopo de identificar o autor e preservar os vestígios materiais do delito. Referida providência é essencial para que o direito de punir (*ius puniendi*) seja exercido, ao final do processo criminal, com respeito aos princípios do devido processo legal, do contraditório e da ampla defesa.

Nos casos em que há vestígios (físicos/digitais) do crime, o agente policial, ao chegar ao local da prática delitiva (geralmente denominado pelo legislador de "local de crime" - art. 158-A, §1º, e art. 158-B, II e III, ambos do CPP), tem o dever legal de, nos termos do art. 158-A, §1º, do CPP, resguardar a área até a chegada dos peritos criminais.

E é a partir desse momento que os agentes estatais, incumbidos da investigação, devem adotar todas as cautelas com o escopo de preservar a cadeia de custódia, instituto inserido pela Lei n° 13.964/19 entre os artigos. 158-A e 158-F do CPP [2], dispositivos que preveem procedimentos mínimos que devem ser

-Juiz durante a *persecutio criminis in iudicio*, seja a mesma constrita no momento da suposta prática delitiva ou no curso de medida cautelar de busca e apreensão.

Sobre o conceito de cadeia de custódia, tem-se que a Quinta Turma, no julgamento do AgRg no HC nº 615.321/PR (Brasil, 2020), definiu que "[...] o instituto da quebra da cadeia de custódia diz respeito à idoneidade do 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".

2 O texto dos citados artigos foi inspirado na Portaria nº 82, de 26/2/2014 da SENASP (Secretaria Nacional de Segurança Pública do Ministério da Justiça e da Segurança Pública), que estabelece diretrizes sobre os procedimentos que devem ser observados no tocante à cadeia de custódia de vestígios. Disponível em: https://diariofiscal.com.br/ZpNbw3dk20XgIKXVGacL5NS8haIoH5PqbJKZaawfaDwCm/legislacaofederal/portaria/2014/senasp82.htm.

Conforme registramos em obra específica sobre o tema (Reis, 2025), "[...] a **cadeia de custódia** não tem por escopo obter provas, mas, sim, preservar a autenticidade e a integridade do material probatório relacionado ao delito em questão. A cadeia de custódia configura uma prova sobre a regularidade da prova produzida pelas partes".

Sobre o ônus a preservação da cadeia de custódia, Badaró (2020) assevera que "a documentação da cadeia de custódia é de responsabilidade das pessoas que têm contato com a fonte de prova custodiada".

A devida documentação da cadeia de custódia dos vestígios garante a autenticidade do material probatório [3] e está intimamente relacionada à **força probatória** do que a evidência busca estabelecer, cabendo ao Estado-acusação, via de regra, o ônus de comprovar a regularidade do citado instituto, até mesmo porque as evidências, na maior parte dos casos, são coletadas em sede de inquérito policial, procedimento administrativo que se desenvolve, via de regra, sem contraditório, e cujo escopo é, nos termos do art. 2º, 1º, da Lei n° 12.830/13 (Brasil, 2013), apurar, preliminarmente, a autoria e a materialidade delitivas, a fim de respaldar ou não o oferecimento de denúncia, nos crimes sujeitos à ação penal de iniciativa pública.

Neste ponto, Prado (2021, p.169) afirma que:

> A integridade e autenticidade do elemento probatório configuram pressuposto para o conhecimento do exame do corpo de delito e sua interpretação crítica pelas partes e pelo juiz.
> A cadeia de custódia como método é a um tempo garantia e condição de procedibilidade do exame de corpo de delito à luz do conjunto de direitos que caracterizam o devido processo legal.

A observância da cadeia de custódia, a um só tempo, assegura a realização do exame pericial à luz do devido processo legal e limita o poder estatal, filtrando eventuais imputações delitivas destituídas de prova material idônea, preservando-se, assim, a higidez do princípio da presunção de não culpabilidade.

3 Manuel Monteiro Guedes Valente preceitua que [...] todo o procedimento da cadeia de custódia da prova está obrigado a respeitar e a promover os princípios constitucionais processuais penais inatos ao instituto da prova, cuja violação vicia a sua utilização no processo [...]. Verificada a ausência de controlo jurisdicional ou de controlo efetivo na tutela e garantia da identidade e autenticidade da prova, [...] estamos perante proibições de produção da prova: inadmissibilidade da prova e, caso seja submetida a julgamento, inadmissibilidade de valoração da prova. VALENTE, Manuel Monteiro Guedes. Cadeia de custódia da prova. 2. ed. Coimbra: Almedina, 2020. P. 52.

Analisando os princípios da perícia criminalística, Renan Saisse afirma que a documentação da cadeia de custódia está intrinsecamente ligada "[...] à necessidade da documentação completa de toda a dinâmica pericial com o intuito de garantir a legalidade e confiabilidade das provas periciais bem como estabelecer um histórico completo destas" (Wendt, 2019, p.127).

Consoante apontado pelo relator Ministro Ribeiro Dantas (Brasil, 2023a):

> A principal finalidade da cadeia de custódia, enquanto decorrência lógica do conceito de corpo de delito (art. 158 do CPP), é garantir que os vestígios deixados no mundo material por uma infração penal correspondem exatamente àqueles arrecadados pela polícia, examinados e apresentados em juízo. Isto é: busca-se assegurar que os vestígios são os mesmos, sem nenhum tipo de adulteração ocorrida durante o período em que permaneceram sob a custódia do Estado.

Na mesma toada, o Ministro Messod Azulay Neto (Brasil, 2024a) afirma que:

> [...] a jurisprudência desta Corte Superior é firme no sentido de que a cadeia de custódia consiste no caminho idôneo a ser percorrido pela prova até sua análise pelo expert, de modo que a ocorrência de qualquer interferência indevida durante sua tramitação probatória pode resultar em sua imprestabilidade para o processo de referência.

A preservação da integridade do vestígio coletado garante que o objeto de prova utilizado pelo Ministério Público, submetido a um processo de contraditório diferido e examinado pelo órgão julgador durante a sentença, seja o mesmo (princípio da mesmidade[4]) que foi reconhecido e coletado pelos peritos criminais ao

Constata-se que quando o **princípio da mesmidade** é observado, o magistrado poderá considerar válida a prova coletada pelo Estado e valorá-la (epistemologia da prova) à luz de outros elementos indiciários e probatórios reunidos

4 Expressão cunhada pelo Tribunal Supremo espanhol, em sentença proferida no dia 03/12/2009: "*En relación a la cadena de custodia el problema que se plantea es garantizar que dado que se recogen los vestigios relacionados con el delito hasta que llegan a concretarse como pruebas en el momento del juicio, aquello sobre lo que recaerá la inmediación, publicidad y contradicción de las partes y el juicio de lo juzgado es lo mismo. Es a través de la cadena de custodia como le satisface la garantía de la "mismidad" de la prueba*". TRIBUNAL SUPREMO. SALA DE LO PENAL. STS 7710/2009. Ponente: Juan Ramon Berdugo Gomez de la Torre. Disponível em: http://www.poderjudicial.es/search/index.jsp#. Referido princípio foi inserido na doutrina brasileira por Geraldo Prado. PRADO, Geraldo. Op. Cit. P. 150.

durante a fase inquisitorial e judicial, qualificando o *standard* probatório adotado pela sentença.

Discorrendo sobre os princípios da mesmidade e da desconfiança, Prado (2021, p.153) afirma que:

> Essa é a razão pela qual as ordens jurídico-processuais que se ajustaram constitucionalmente ao modelo acusatório de processo regulam o procedimento probatório e cuidam não apenas de assegurar a produção do elemento probatório – neste sentido existe pouca diferença em relação ao modelo inquisitorial reformado – mas também as condições para a demonstração de que estes elementos estão preservados para futuro exame, valoração ou perícia.
> Os princípios da mesmidade e da desconfiança são fundamentais para garantir o juízo mediante a redução dos riscos de erro judiciário, consistindo no fundamento lógico e epistemológico da cadeia de custódia das provas [...].

No mesmo sentido, o Ministro Ribeiro Dantas (Brasil, 2022) enuncia que:

> Não presumir o réu como culpado significa, dentre muitas coisas, que não se pode atribuir à narrativa apresentada pelo Estado nenhuma nota de superioridade epistêmica sobre o estado de inocência do acusado. Vigora aqui, contrariamente, um mandamento constitucional e legal de desconfiança: a denúncia não será presumida falsa, claro – o que seria inclusive um contrassenso com seu recebimento –, mas deve ser lida com ceticismo pelo julgador.

Fixadas essas premissas conceituais sobre a cadeia de custódia, verifica-se, contudo, que a recente legislação de regência desse instituto já se mostra, em certo aspecto, ultrapassada, visto que não regulou o tema em relação aos vestígios digitais, dado de importância inquestionável (notadamente em delitos envolvendo a macro criminalidade organizada, objeto das Convenções de Caracas, de Palermo[5]

5 Segundo Nereu Giacomolli e Luiz Eduardo Cani, "A introdução de técnicas especiais de investigação se deve à Convenção de Palermo, por meio da qual os Estados signatários se comprometem a introduzir nos respectivos ordenamentos jurídicos, desde que compatível aos princípios fundamentais, técnicas de entrega vigiada, vigilância eletrônica, operações de infiltração e outras técnicas de vigilância destinadas a "combater eficazmente a criminalidade organizada" (art. 20, item 1, do Decreto 5.015/04). [...] Dito de outro modo, para perseguir crimes circunscritos aos pactos de silêncio (omertà), criaram-se mecanismos para incentivar os investigados a falar (delação premiada e acordo de leniência, v.g.) e estabeleceram-se técnicas de investigação reprodutoras das ações investigadas (dentre as disposições que regulamentam a infiltração de agentes, tem-se a autorização para a prática de alguns crimes, v.g.)." GIACOMOLLI, Nereu; CANI, Luiz Eduardo. O acesso autorizado a aparelhos *smart:* burla ao agente infiltrado digital? Boletim IBCCRIM. V. 30. N. 352. P. 4.

e de Mérida[6]) e que tende a ser mais cada vez mais relevante à medida que avança o processo de virtualização pelo qual vem passando a sociedade.

Demonstrando a relevância dos vestígios digitais para a *persecutio criminis*, a nível internacional, Prado (2024) afirma que "Federico Bueno de Mata, professor da Universidade de Salamanca, sublinha que recente pesquisa apontou para o fato de 85% das atuais provas penais na Espanha envolvem provas digitais".

Sydow (2022), em comentários à Lei nº 13.964/19 (diploma que inseriu os artigos. 158-A a 158-F no CPP), assevera que a citada norma "[...] pecou gravemente ao deixar de dedicar-se ao estudo e regramento das evidências e elementos digitais, que possuem regras mais detalhadas e complexas".

Dissertando sobre a necessidade da observância da cadeia de custódia em relação aos vestígios digitais, Badaró (2020) aduz que "[...] também se poderá pensar na cadeia de custódia nos casos de coleta ou apreensão de elementos imateriais, registrados eletronicamente, [...] sendo necessário a documentação da cadeia de custódia". Nesse diapasão, confira-se: HC nº 796.338/RS, relator Ministro Reynaldo Soares da Fonseca, Quinta Turma, DJe de 18/9/2023.

O conceito de **cadeia de custódia** deve, portanto, ser analisado à luz das inovações tecnológicas que a sociedade contemporânea tem experimentado. A digitalização das informações, o armazenamento em nuvem e a expansão das atividades humanas para além das fronteiras geográficas são fatores relevantes a serem considerados nesse contexto[7].

Conforme apontado por Daniel Costa (2023, p.21-22), "[...] o *Whatsapp* é o aplicativo mais utilizado no Brasil e possui o maior número de usuários no mundo,

6 Convenção Interamericana contra a Corrupção, Convenção das Nações Unidas contra o Crime Organizado Transnacional e Convenção das Nações Unidas contra a corrupção, promulgadas, respectivamente, pelos Decretos de n°s 4.410/2002, 5.015/2004, e 5.687/2006.

7 Atualmente, já vivemos a era da *internet* das coisas (*internet of things - IOT*), que se refere à conexão de dispositivos e objetos cotidianos à internet, possibilitando que coletem, compartilhem e analisem dados automaticamente, sem precisar de intervenção humana constante. As aplicações da *internet* das coisas englobam residências inteligentes, cidades interligadas, acompanhamento da saúde e administração de fábricas. É fundamental prestar atenção à segurança e à privacidade na IoT, devido ao volume de dados sensíveis que podem ser produzidos e transmitidos. Segundo João Paulo Lordelo, "A *internet* das coisas permite a integração de um vasto número de tecnologias – monitoração de dados biométricos, comunicação instantânea por texto, áudio e vídeo, armazenamento de dados em nuvem, redes sociais, mapas etc – e objetos – smartphones, computadores pessoais*, laptops, smartwatches*, óculos de realidade aumentada, máquinas industriais, GPS etc – em forma de rede, com conexão à *internet"*. LORDELO, João Paulo. Constitucionalismo digital e devido processo legal. São Paulo: Juspodivm, 2022. P. 99-100.

tido pelos especialistas por possuir serviço de mensagem digital seguro, pois dotado de criptografia ponta a ponta. [...] Surpreende, também, a cifra de mensagens diárias entregues (em 2020): mais de 100 bilhões [...]".

É consabido que os processos criminais instaurados a partir de denúncias lastreadas, exclusivamente, em documentos físicos continuarão a existir, mas o grande volume de provas digitais com a qual nos deparamos no âmbito criminal já é uma realidade, com a qual temos que lidar de forma segura.

2. A cadeia de custódia dos vestígios digitais

Nos locais de crimes de informática, os vestígios são imateriais, apresentados na forma de "0" e "1" (sistema binário) e poderão estar contidos (simultaneamente ou não) em sítios da *internet*, serviços de correio eletrônico, plataformas de redes sociais, computadores, aparelhos celulares, *tablets* e em serviços de armazenamento em nuvem, por exemplo.

Em comentário sobre o princípio da simultaneidade no meio digital, Sydow (2022, p.292) afirma que:

> [...] com a lógica da nuvem, isso ganha contornos ainda mais únicos, posto que um provedor brasileiro [...] pode ter sua funcionalidade segmentada em diversos data centers [...] ou, ainda em país algum, como é o caso dos data centers únicos como o da Microsoft, construído no meio do alto mar ou de modo submarino, em terras geopoliticamente de ninguém. [...]
> O surgimento de um metaverso, inclusive, vai destacar ainda mais a situação posto que o(a) usuário (a) estará geograficamente em um local e virtualmente em outro em realidades sobrepostas."

Atento às particularidades dos vestígios digitais, Badaró (2021) aduz que:

> [...] no caso das provas digitais, para que seja minimamente atestada a sua autenticidade e integridade, devem ser seguidos os métodos informáticos de obtenção, registro, armazenamento, análise e apresentação dos elementos de prova digitais que registrem as "*best practices"* nacionais e internacionais. Sua apresentação judicial, para que tenha potencial epistêmico adequado, deve se dar por meio de prova pericial, sendo essencial a completa documentação da cadeia de custódia.

A prova coletada em ambiente eletrônico detém nuances que as diferenciam das provas materiais, razão pela qual é recomendável que os profissionais incumbidos de lidar com essas evidências possuam conhecimento especializado na área, assegurando que a extração e o respectivo acautelamento dos indícios sejam feitos de acordo com métodos científicos reconhecidos, garantindo confiabilidade aos resultados obtidos.

Dissertando sobre a volatilidade dos dados nato-digitais, Badaró (2021b) assevera que:

> No que toca à sua "desmaterialização", não se trata de provas pensáveis como objetos físicos, dotados de uma evidente corporeidade. [...] Há, na prova digital, uma "congênita mutabilidade" ou "fácil alterabilidade". Em suma, trata-se de fonte de prova que pode ser facilmente contaminada, sendo sua gestão muito delicada, por apresentar um alto grau de vulnerabilidade a erros.

Referindo-se aos arts. 158-A e segs. do CPP, o Ministro Rogerio Schietti Cruz, nos autos do AgRg no RHC nº 195.921/MG (Brasil, 2024c), foi categórico ao consignar que "A vigilância sobre a prova digital traz peculiaridades não previstas na ultrapassada legislação de regência, o que exige o cuidado do Judiciário na análise do caso concreto".

De acordo com o Glossário de Ciências Forenses (Brasil, 2016), elaborado pela Diretoria Técnico-Científica da Polícia Federal, o local de crime de informática diz respeito ao local "[...] onde se encontram vestígios em ambientes computacionais que demandam profissionais de perícia especializados para a sua constatação, exame, coleta e preservação".

Ressalto que o Ministério da Justiça e da Segurança Pública (MJSP), em 10/9/2024, publicou Procedimento Operacional Padrão (POP) que contém 10 volumes - sendo um destinado, exclusivamente, à informática forense (Brasil, 2024).

O referido "POP" prevê que os equipamentos eletrônicos apreendidos devem ser acondicionados e lacrados (art. 158-D, § 1, do CPP)(Brasil; Superior Tribunal de Justiça, 2021; Supremo Tribunal Federal, 2021), "[...] incluindo as mídias usadas como destino de dados. Os respectivos lacres e descrição sucinta do material e sua origem devem constar em termo de apreensão." (Brasil, 2024, p.42), sendo recomendável a captura de imagens dos materiais devidamente apreendidos.

Nesse sentido, o volume de informática forense do mencionado “POP” prevê que, havendo possíveis vestígios digitais no local de cumprimento de mandado de busca e apreensão, os agentes devem “Providenciar o isolamento do local para evitar que pessoas estranhas à equipe de perícia criminal tenham acesso físico aos equipamentos de informática presentes. Do mesmo modo, promover o isolamento digital do local, bloqueando os acessos remotos ou as conexões de rede e *internet*, desde que não prejudiquem os exames” (Brasil, 2024, p.38).

Segundo Cláudio Netto (2023, p.267), local de crime de informática preservado “[...] é aquele em que, além do isolamento físico natural, é realizado o isolamento contra acessos remotos, via transmissão de dados, e observados os cuidados inerentes aos aspectos de volatilidade e sensibilidade dos vestígios digitais.”

Nessa toada, Caldeira (2020, p.216) afirma que “[...] o ideal é que as máquinas que estejam desligadas sejam assim mantidas, para evitar alterações de dados”.

Identificadas possíveis fontes de prova digital em equipamento que esteja ligado, é recomendável, ainda, que seja realizada a cópia por espelhamento dos dados e utilizada a função *hash*, que cria um algoritmo alfanumérico capaz de comprovar que a cópia gerada é idêntica à original.

O citado Procedimento Operacional Padrão define que o algoritmo *hash* “[...] gera, a partir de uma entrada de qualquer tamanho, uma saída de tamanho fixo, ou seja, é a transformação de uma grande quantidade de informações em uma pequena sequência de bits (*hash*). Esse *hash* se altera se um único bit da entrada for alterado, acrescentado ou retirado” (Caldeira, 2020, p.21).

A técnica do algoritmo *hash* cria uma espécie de “DNA” da evidência nato-digital coletada, de modo que qualquer adulteração dos dados contidos no equipamento implicará na geração de código diverso.

A produção do mencionado código, por parte da perícia oficial quando da apreensão do equipamento, viabiliza a repetibilidade da evidência digital durante a fase de instrução, providência hábil a comprovar que a imagem dos dados extraídos pela Polícia na etapa pré-processual é a mesma produzida durante o processo (auditabilidade da prova por parte da defesa).

Sobre o tema, Hermeiro (2023, p.38) afirma que:

> Uma das técnicas que é utilizada para garantir a integridade e autenticidade dos dados recolhidos é o hash. O código hash, "é o resultado da aplicação de um procedimento matemático a um conjunto de dados, que podem estar contidos num ficheiro [...], num disco rígido, num DVD etc. O código é o resumo único atribuído ao conjunto de informação sobre a qual se aplicou o algoritmo, obtendo-se um resumo completamente distinto, para o mesmo algoritmo, com a mínima alteração que se produza nos dados originais."

Indispensável mencionar que a Quinta Turma do STJ, nos autos do AgRg no RHC nº 143.169/RJ (Brasil, 2023b), já se pronunciou quanto à indispensabilidade da geração do código *hash* como condição de validade para valoração judicial dos arquivos digitais existentes em equipamentos eletrônicos apreendidos e representativos de prova material de delitos imputados.

No contexto de *digital evidence*, a qualidade epistêmica do vestígio digital será baixa se sua coleta e produção não seguirem as melhores práticas e utilizarem métodos não confiáveis (auditabilidade/justificabilidade).

Nesse sentido, Badaró (2021) aponta que:

> É imprescindível que o método empregado garanta a integridade do dado digital e, com isso, a força *probandi* do conteúdo probatório por ele representado. Normalmente, fazer uma cópia ou espelhamento, obtendo o *bitstream* da imagem do disco rígido ou suporte de memória em que o dado digital está registrado. [...]
> Quanto ao laudo técnico, ele deve conter uma completa e exaustiva descrição dos sistemas informáticos utilizados, um elenco dos instrumentos (*tolls*) utilizados e um detalhado relatório dos resultados obtidos.

Registre-se que, embora o Código de Processo Penal não tenha tratado especificamente dos procedimentos a serem observados pelo Estado com relação à cadeia de custódia dos vestígios digitais, a Norma ABNT ISO/IEC 27037:2013 estabelece diretrizes internacionais, com o escopo de preservar a autenticidade da prova eletrônica[8].

A Quinta Turma do STJ, nos autos do AgRg nos HC nº 828.054/RN (Brasil, 2024b), já teve a oportunidade de examinar a referida normal infralegal, julgamento no qual a ordem foi concedida de ofício para declarar inadmissíveis provas digitais

8 Disponível em: https://academiadeforensedigital.com.br/iso-27037-identificacao-coleta-aquisicao-e-preservacao-de-evidencia/

extraídas de aparelho celular pertencente a acusado e que foram utilizadas para embasar sentença condenatória pela suposta prática do crime tipificado no art. 2°, *caput*, §2°, da Lei nº 12.850/13.

Naquela assentada, o relator Min. Joel Ilan Paciornik destacou que, no trato das evidências digitais, a Norma ABNT ISO/IEC 27037:2013 constitui documento que, "[...] embora não dotado de força obrigatória de lei, constitui relevante guia a ser observado pelos atores da persecução penal, a fim de assegurar, tanto quanto possível, a autenticidade da prova digital" e o resguardo quanto à auditabilidade, repetibilidade, reprodutibilidade e justificabilidade dos métodos empregados para extração dos vestígios imateriais da suposta prática delitiva.

Importante, ainda, mencionar a existência da norma ABNT ISO/IEC 27042:2015 que, embora ainda não tenha sido examinada por julgados proferidos pelo STJ e pelo STF, tampouco traduzida para o português, estabelece diretrizes internacionais que visam preservar a validade, reprodutibilidade e repetibilidade das evidências digitais[9].

Revela-se, portanto, essencial que o método utilizado para extração dos dados digitais assegure a integridade do material coletado e resguarde a idoneidade dos vestígios que subsidiam a acusação.

3. A utilização de provas, consubstanciadas em *prints* de conversas mantidas por meio do *Whatsapp*, à luz da jurisprudência do Superior Tribunal de Justiça

No tocante à fragilidade de evidências coletadas por meio de *printscreen*, Barreto (2022, p.167) afirma que "[...] sua validade é, por vezes, questionada, especialmente pelo fato de não guardar os metadados necessários à comprovação do fato e pelo fato de ser produzido de forma unilateral."

Conforme pontua Atheniense (2024, p.189), "os metadados [...] desempenham um papel crucial na contextualização das evidências digitais. Eles

9 Disponível em: https://www.iso.org/standard/44406.html

são indispensáveis em investigações digitais para autenticidade, identificação de autoria e rastreamento de atividades. Os metadados não apenas fornecem informações detalhadas sobre a origem, criação e modificação dos dados, mas também são instrumentais na construção de uma linha do tempo coerente [...]".

Feitas essas considerações, tem-se que a jurisprudência das Turmas de Direito Penal do STJ vinha, até o ano de 2024, exarando o entendimento de que "prints" de conversas mantidas pelo aplicativo *Whatsapp*, via de regra, não observavam a cadeia de custódia, revelando-se tais elementos destituídos de validade para fins de comprovação da autoria e materialidade delitivas.

Nesse sentido, a Quinta Turma, acompanhando voto proferido pela Relatora Min. Daniela Teixeira nos autos do AgRg no AREsp n. 2.441.511/PR (Brasil, 2024d), concluiu que "[...] a utilização de "prints" de mensagens, mesmo que realizados pela autoridade policial, viola a cadeia de custódia prevista nos artigos 158 e ss. do CPP e é prova ilícita [...]", razão pela qual a ordem foi concedida para reformar decisão de pronúncia lastreada em "prints" de conversa mantida no aplicativo denominado *whatsapp web*. Confira-se, ainda: AgRg no RHC nº 133.430/PE, relator Ministro Nefi Cordeiro, Sexta Turma, DJe de 26/2/2021.

No mesmo diapasão, a Quinta Turma, nos autos do AgRg no EDcl no AREsp nº 2.521.345/RO, deu provimento a recurso da defesa para absolver recorrente que havia sido condenado pela suposta prática do crime tipificado no art. 217-A do Código Penal.

O Relator Min. Ribeiro Dantas considerou que a prova da condenação estava lastreada em *prints* de conversas de *whatsapp*, desacompanhadas da respectiva cadeia de custódia, fato que compromete a integridade dos vestígios apontados pela acusação e que se revela inidôneo a subsidiar a sentença condenatória. Confira-se trecho do voto do Relator, que foi acompanhado pelos Ministros da Quinta Turma:

> Como se sabe, tais imagens podem ser facilmente editadas com softwares de edição de fotos. Ademais, há a possibilidade de criar ou modificar visualmente conversas em aplicativos simuladores, tal como ocorre quando se utiliza a ferramenta "inspecionar", disponível em navegadores web, que permite aos usuários acessarem o HTML e o CSS da página que estão visualizando, possibilitando mudanças temporárias no texto exibido na tela.
> Constato, assim, a absoluta inexistência de comprovação da confiabilidade da aludida prova, o que é ônus da acusação, e não da defesa. Consequentemente, a prova é inapta para fornecer

> conclusões seguras sobre as hipóteses fáticas em discussão no processo, porque não há nenhuma garantia, mínima que seja, sobre seu conteúdo (Brasil, 2024e).

Contudo, a Corte Especial, em sessão realizada no dia 19/2/2025, concluiu, no julgamento do Inq n. 1.658/DF (Brasil, 2025a), que "[...] para que se considere ilícita a prova obtida mediante *print* de *WhatsApp*, é indispensável a comprovação de que houve a quebra da cadeia de custódia [...]".

Referido entendimento foi seguido pela Sexta Turma do STJ, nos autos do RHC n. 218.499/SC (Brasil, 2025g), do AgRg no HC n. 931.683/MS (Brasil, 2025e), do AgRg no AREsp n. 2.600.503/ES(Brasil, 2025c) e do AgRg no AREsp n. 2.833.422/RS (Brasil, 2025b), oportunidades em que esse órgão fracionário adotou a posição de que não havendo demonstração, por parte da defesa, de adulteração, alteração ou interferência na prova (alteração da ordem cronológica das conversas, por exemplo), não há que se falar em prejuízo, tampouco em violação da cadeia de custódia na utilização de *printscreen* de diálogos mantidos por meio do aplicativo *Whatsapp*.

No âmbito da Quinta Turma do STJ, constata-se que a citada orientação foi seguida nos autos do AgRg no AREsp 2.841.690/SP (Brasil, 2025d), fato que demonstra que as Turmas de Direito Penal do STJ têm se inclinado em atribuir à defesa o ônus de comprovar eventual irregularidade na cadeia de custódia dessa espécie de prova, ilegalidade que restou constatada pela Quinta Turma, nos autos do AgRg no HC 943.895/PR (Brasil, 2025f), pois foi detectado que a autoridade policial, antes do encaminhamento do aparelho ao Instituto de Criminalística para extração dos dados com a técnica científica adequada, manuseou o aparelho celular e teria confrontado o proprietário acerca das conversas encontradas.

Verifica-se que a questão em torno da (i)legalidade da utilização de *printscreen* de conversas mantidas por meio do aplicativo *Whatspp* tem sido objeto de amadurecimento por parte da jurisprudência do Tribunal da Cidadania, que vem decidindo a matéria à luz das peculiaridades de cada caso concreto.

4. Conclusão

A cadeia de custódia dos vestígios de prática delitiva detém extrema relevância na aferição da qualidade epistêmica da prova submetida à valoração judicial e sua estrita observância confere lisura e credibilidade à sentença proferida pelo Poder Judiciário, ainda mais em tempos de transição de um Processo Penal analógico para um Processo Penal digital.

Depreende-se que, embora o citado instituto tenha sido inserido em nosso ordenamento com a (ainda) recente entrada em vigor Lei n° 13.964/19, os julgados colacionados neste artigo demonstram que o STJ tem desempenhado papel crucial na interpretação da matéria, contribuindo para a solidificação de um Direito Processual Penal que limite eventuais excessos estatais e que fomente o Estado-acusação a produzir provas íntegras e confiáveis, sob pena de ilicitude (art. 157 do CPP).

CONFLITO DE INTERESSE

Nenhum declarado

REFERÊNCIAS

ATHENIENSE, Alexandre. Provas e golpes digitais. Como o advogado pode vencer um caso sem testemunhas. In: DE LIMA, Ana Paula Canto; CRESPO, Marcelo (orgs). **Crimes digitais**. São Paulo: RT, 2024.

BADARÓ, Gustavo Henrique. **Processo Penal**. 8. ed. São Paulo: Thomson Reuters Brasil, 2020.

BADARÓ, Gustavo. Os standards metodológicos de produção na prova digital e a importância da cadeia de custódia. **Boletim do IBCCRIM**, a.29, n.343, p. 7-9, jun. 2021.

BADARÓ, Gustavo. **A cadeia de custódia da prova digital.** Artigo apresentado no Congresso Internacional de Direito Probatório, Porto Alegre, 2021b.

BARRETO, Alesandro Gonçalves; KUFA, Karina; SILVA, Marcelo Mesquita. **Cibercrimes e seus reflexos no Direito brasileiro**. 3 ed. São Paulo: Juspodivm, 2022.

BRASIL. **Lei n° 12.830, de 20 de junho de 2013**. Dispõe sobre a investigação criminal conduzida pelo delegado de polícia. Brasilia, DF: Presidência da República, 2013.

BRASIL. Ministério da Justiça. Polícia Federal. Diretoria Técnico-científica. **Glossário de ciências forenses**: termos técnicos mais usados pela perícia criminal federal. Brasília: Polícia Federal; Diretoria Técnico-Científica, 2016.

BRASIL. Ministério da Justiça e Segurança Pública. Secretaria Nacional de Segurança Pública. Diretoria do Sistema Único de Segurança Pública. Informática forense. Brasília, DF: SNSP, 2024. (Procedimentos Operacionais Padrão – Perícia, 5). Disponível em: file:///C:/Users/dougl/Downloads/POP%20Per%C3%ADcia%20Criminal%202024%20-%20Inform%C3%A1tica%20Forense%20vol%205.pdf.pdf

BRASIL. Supremo Tribunal Federal. **Reclamação n. 43.007/DF**. 15 set. 2021.

BRASIL. Superior Tribunal de Justiça. **Agravo Regimental no Habeas Corpus n. 615.321/PR**. 12 nov. 2020.

BRASIL. Superior Tribunal de Justiça. **Habeas Corpus n. 653.515/RJ**. 23 nov. 2021.

BRASIL. Superior Tribunal de Justiça. **Agravo em Recurso Especial n.1.936.393/RJ**. 25 out. 2022.

BRASIL. Superior Tribunal de Justiça. **Agravo Regimental no Recurso de Habeas Corpus n.143.169/RJ**. 07 fev. 2023a.

BRASIL. Superior Tribunal de Justiça. **Agravo Regimental no Recurso Ordinário em Habeas Corpus n.143.169/RJ**. 23 mar. 2023b.

BRASIL. Superior Tribunal de Justiça. **Agravo Regimental no Habeas Corpus n. 829.138/RN**. 14 fev. 2024a.

BRASIL. Superior Tribunal de Justiça. **Agravo Regimental no Habeas Corpus n.828.054/RN**. 29 abr. 2024b.

BRASIL. Superior Tribunal de Justiça. **Agravo Regimental no Recurso de Habeas Corpus n.195.921/MG**. 03 jun. 2024c.

BRASIL. Superior Tribunal de Justiça. **Agravo Regimental no Agravo em Recurso Especial n. 2.441.511/PR**. 17 jun. 2024d.

BRASIL. Superior Tribunal De Justiça. **Agravo Regimental nos Embargos de Declaração no Agravo em Recurso Especial n. 2.521.345/RO**. 21 jun 2024e.

BRASIL. Superior Tribunal de Justiça. **Inquérito n. 1.658/DF**. 11 mar. 2025a.

BRASIL. Superior Tribunal de Justiça. **Agravo Regimental no Agravo em Recurso Especial n. 2.833.422/RS**. 14 maio 2025b.

BRASIL. Superior Tribunal de Justiça. **Agravo Regimental no Agravo em Recurso Especial n. 2.600.503/ES**. 25 jun. 2025c.

BRASIL. Superior Tribunal de Justiça. **Agravo Regimental no Agravo em Recurso Especial n. 2.841.690/SP**. 25 jun 2025d.

BRASIL. Superior Tribunal de Justiça. **Agravo Regimental no Habeas Corpus n. 931.683/MS**. 26 jun. 2025e.

BRASIL. Superior Tribunal de Justiça. **Agravo Regimental no Habeas Corpus n. 943.895/PR**. 08 set. 2025f.

BRASIL. Superior Tribunal de Justiça. **Recurso Ordinário em Habeas Corpus n. 218.499/SC**. 16 set. 2025g.

CALDEIRA, Rodrigo de Andrade Figaro. **Pacote Anticrime**: análise crítica à luz da Constituição Federal. São Paulo: Thomson Reuters, 2020.

COSTA, Daniel Tempski Ferreira da. **A prova penal digital dotada de criptografia ponta a ponta [E2EE] e a experiência do direito comparado**. São Paulo: Tirant Lo Blanch, 2023.

HERMEIRO, Andreia Carina Cláudio. **A cadeia de custódia da prova digital**: o uso da tecnologia Blockchain como forma de preservação. Coimbra: Dissertação (Mestrado em ciências jurídico-forenses). 2023.

NETTO, Claudio Saad (coord.). **O direito à prova pericial no processo penal**. São Paulo: Thomson Reuters, 2023.

PRADO, Geraldo. **A cadeia de custódia da prova no processo penal**. 2 ed. São Paulo: Marcial Pons, 2021.

PRADO, Geraldo. **Curso de Processo Penal:** tomo I: fundamentos e sistema. São Paulo: Marcial Pons, 2024.

REIS, Rodrigo Casimiro. **Verdade e Prova Penal**: A cadeia de custódia na era digital. São Paulo: Amanuense, 2025.

SYDOW, Spencer Toth. **Curso de Direito Penal Informático**: partes geral e especial. Salvador: Juspodivm, 2022.

WENDT, Emerson (org.). **Direito e TI**: cibercrimes. Porto Alegre: Livraria do Advogado, 2019.

Correspondence address:

Rodrigo Casimiro Reis
Defensoria Pública do Estado do Rio de Janeiro - Sede Administrativa
Avenida Marechal Câmara, 314 - CEP 20020-080 - Centro, RJ
E-mail: r.casimiro@outlook.com

Enviado para submissão: 21/09/2025

Aceito após revisão: 03/12/2025

Publicado no Fluxo Contínuo 16/12/2025