SUPERIOR TRIBUNAL DE JUSTIÇA

HABEAS CORPUS Nº 1036370 - ES (2025/0358888-0)

RELATOR	:	**MINISTRO JOEL ILAN PACIORNIK**
IMPETRANTE	:	LEDILSON MARTINS DA SILVA PARIZ
ADVOGADOS	:	LEDILSON MARTINS DA SILVA PARIZ - ES018613
		LIDIANE SILVA DOS SANTOS MARTINS - ES040650
IMPETRADO	:	TRIBUNAL DE JUSTIÇA DO ESTADO DO ESPÍRITO SANTO
PACIENTE	:	HELSON MAXIMO DE MOURA JUNIOR (PRESO)
CORRÉU	:	MÁRCIO DA COSTA VIEIRA
CORRÉU	:	MARCOS ANTÔNIO PEREIRA SENA
CORRÉU	:	MARCOS ANTÔNIO DE OLIVEIRA
INTERES.	:	MINISTÉRIO PÚBLICO DO ESTADO DO ESPÍRITO SANTO

DECISÃO

Trata-se de *habeas corpus*, sem pedido liminar, impetrado em benefício de HELSON MAXIMO DE MOURA JUNIOR, contra acórdão proferido pelo TRIBUNAL DE JUSTIÇA DO ESTADO DO ESPÍRITO SANTO no julgamento da Revisão Criminal n. 5001996-75.2025.8.08.0000.

Extrai-se dos autos que o paciente foi condenado à pena de 14 (quatorze) anos, 03 (três) meses e 03 (três) dias de reclusão, além do pagamento de 23 (vinte e três) dias-multa, no regime inicial fechado, pela prática do crime tipificado no art. 157, 2º, incisos II, V e VII e 2º- A, inciso I, do Código Penal - CP.

O Tribunal de origem deu parcial provimento à apelação interposta pelo paciente, redimensionando a pena para 11 (onze) anos e 08 (oito) meses de reclusão e 20 (vinte) dias-multa.

A defesa, posteriormente, ajuizou revisão criminal, alegando a ocorrência de quebra da cadeia de custódia, mas a ação foi julgada improcedente, conforme ementa (fls. 8/9):

> *"Ementa: DIREITO PROCESSUAL PENAL. REVISÃO CRIMINAL. ROUBO QUALIFICADO. ALEGAÇÃO DE ILICITUDE DE PROVA DIGITAL. EXTRAÇÃO DE DADOS DE CELULAR DE CORRÉU. QUEBRA DA CADEIA DE CUSTÓDIA. INOCORRÊNCIA. IMPROCEDÊNCIA.*
>
> *I. CASO EM EXAME*
>
> *1. Revisão criminal ajuizada contra condenação no bojo da ação penal nº 0003739- 57.2021.8.08.0030, na qual o requerente foi condenado pela prática do crime de roubo qualificado (art. 157, §2º, II, e §2º-A, I, do Código*

Penal), à pena de 14 anos, 3 meses e 3 dias de reclusão, além de 23 dias-multa, em regime inicial fechado.

2. O requerente pleiteia a anulação da condenação sob o argumento de ilicitude da prova obtida pela extração de dados do telefone celular de corréu, alegando violação à cadeia de custódia.

II. QUESTÃO EM DISCUSSÃO

A questão em discussão consiste em verificar se a extração de dados do aparelho celular do corréu, sem a certificação do código "hash", caracteriza quebra da cadeia de custódia e implica a ilicitude da prova utilizada para a condenação.

III. RAZÕES DE DECIDIR

4. A extração dos dados do celular do corréu foi devidamente autorizada por decisão judicial fundamentada, em observância às garantias constitucionais dos acusados, especialmente ao disposto no art. 5º, XII, da CF/88.

5. A ausência da certificação do código "hash" não compromete, por si só, a integridade da prova digital, sendo este um elemento de reforço à segurança do material interceptado, mas não um requisito essencial para sua validade, conforme precedentes do TJES (APC 5005830-57.2023.8.08.0000 e APC 0009360-20.2021.8.08.0035).

6. Não há indícios de adulteração da prova digital ou de má-fé na sua obtenção, sendo os dados extraídos devidamente documentados nos autos e submetidos ao contraditório e ampla defesa.

7. A cadeia de custódia foi observada, com registro formal da apreensão do aparelho, encaminhamento à perícia e extração dos dados, em conformidade com o art. 158 do CPP.

8. O fato de o aplicativo "WhatsApp" não possuir a funcionalidade de edição de mensagens na época dos fatos reforça a confiabilidade da prova colhida.

IV. DISPOSITIVO E TESE

9. Revisão criminal improcedente.

Tese de julgamento:

1. A ausência de certificação do código "hash" não torna a prova digital ilícita, pois se trata de elemento de reforço à segurança da informação, mas não de requisito essencial à sua validade.

2. A extração de dados de aparelho celular, devidamente autorizada por decisão judicial fundamentada e sem indícios de adulteração, não configura violação da cadeia de custódia nem enseja nulidade da prova.

3. A integridade da prova digital pode ser aferida pelo conjunto probatório e pela observância dos registros formais do procedimento pericial."

No presente *writ*, a defesa sustenta que houve quebra da cadeia de custodia, considerando a acusação baseada em fotografias sem acolheita e apresentação dos metadados e código *hash* da prova digital, devendo ser retirada dos autos, bem como todas que as que dela derivam.

Argumenta que após a prisão em flagrante do corréu Marcos Antônio de Oliveira, foi apreendido aparelho celular e posteriormente foi identificada a propriedade do outro corréu Marcos Antônio Pereira Sena.

Aduz que nas informações processuais consta relatório de análise do celular, mas o acesso não seguiu aos procedimentos determinados na cadeia de custódia para a colheita e validação da priva digital.

Afirma que o relatório que foi apresentado pela autoridade policial, apenas com imagens extraídas por meio de *printscreen* de tela do aplicativo WhatsApp.

Defende que o *printscreen* sem a demonstração da regularidade, metadados, integridade e código *hash* não produz efeito probatório.

Com essas razões, por fim, postula pela concessão da ordem de *habeas corpus* para o fim de absolver o paciente, ante a flagrante ilegalidade pela quebra da cadeia de custódia da prova digital.

O Ministério Público Federal opinou pelo não conhecimento da impetração ou pela denegação da ordem (fls. 120/125).

É o relatório.

Decido.

Diante da hipótese de *habeas corpus* substitutivo de recurso próprio, a impetração nem sequer deveria ser conhecida, segundo orientação jurisprudencial do Supremo Tribunal Federal – STF e do próprio Superior Tribunal de Justiça – STJ.

Todavia, considerando as alegações expostas na inicial, mostra-se razoável o processamento do feito para verificar a existência de eventual constrangimento ilegal que autorize a concessão da ordem de oficio.

Conforme relatado, busca-se, no presente *writ*, a declaração de nulidade das provas digitais produzidas, em razão da quebra da cadeia de custodia, com a absolvição do paciente.

Como cediço, o instituto da cadeia de custódia visa a garantir que o tratamento dos elementos probatórios, desde a sua arrecadação até a análise e deliberação pela autoridade judicial, seja idôneo e livre de qualquer interferência que possa macular a confiabilidade da prova. (arts. 158-A e segs. do CPP).

Importante pontuar que, diante da volatilidade dos dados telemáticos e da maior suscetibilidade a alterações, imprescindível se faz a adoção de mecanismos que assegurem a preservação integral dos vestígios probatórios, de forma que seja possível a constatação de eventuais alterações, intencionais ou não, dos elementos inicialmente coletados, demonstrando-se a higidez do caminho percorrido pelo material.

Dessa forma, pode-se dizer que as provas digitais, em razão de sua natureza facilmente - e imperceptivelmente - alterável, demandam ainda maior atenção e cuidado em sua custódia e tratamento, sob pena de ter seu grau de confiabilidade diminuído drasticamente ou até mesmo anulado.

Gustavo Badaró, neste sentido, leciona que:

> *"Evidente que independentemente de qual procedimento técnico empregado, além de adequado segundo as melhores práticas, ele também precisará ser documentado e registrado em todas as suas etapas. Tal exigência é uma garantia de um correto emprego das operating procedures, especialmente por envolver um dado probatório volátil e facilmente sujeito à mutação. Além disso, exatamente pela diferença ontológica da prova digital com relação à prova tradicional, devido àquela não se valer de uma linguagem natural, mas digital, é que, como diz Pittiruti, uma cadeia de custódia detalhada se faz ainda mais necessária"*
>
> *(BADARÓ, Gustavo. A Cadeia de Custódia da Prova Digital. In: OSNA, Gustavo et. al. Direito Probatório. Londrina: Thoth, 2023, p. 179).*

De fato, a prova, enquanto meio de reconstrução histórica dos fatos objeto de apuração, deve ser capaz de revelar, com o máximo de precisão possível, os eventos tais como ocorreram, sob pena de potencialmente conduzir a um temerário distanciamento entre a realidade fática e o pronunciamento jurisdicional.

Diante disso, Badaró visualiza dois cenários em que a inobservância da cadeia de custódia da prova digital, mais do que levar à desconfiança epistemológica sobre o meio de prova (campo da valoração probatória), conduzirá mesmo à sua desconsideração completa enquanto prova (campo da inadmissibilidade probatória). São eles: "*o primeiro, quando não há qualquer documentação da cadeia de custódia; o segundo, quando não seja possível, minimamente, assegurar que o vestígio tenha potencial para o acertamento do fato*" (BADARÓ, p. 183).

Dito isso, mostra-se indispensável que todas as fases do processo de obtenção das provas digitais sejam documentadas, cabendo à polícia, além da adequação de metodologias tecnológicas que garantam a integridade dos elementos extraídos, o devido registro das etapas da cadeia de custódia, de modo que sejam asseguradas a autenticidade e a integralidade dos dados.

A propósito:

> *PENAL E PROCESSUAL PENAL. AGRAVO REGIMENTAL NOS EMBARGOS DE DECLARAÇÃO NO AGRAVO EM RECURSO ESPECIAL. PORNOGRAFIA INFANTIL. ART. 241-B DO ECA. DADOS EXTRAÍDOS DE APARELHOS ELETRÔNICOS SEM O MENOR RIGOR TÉCNICO. QUEBRA DA CADEIA DE CUSTÓDIA. INADMISSIBILIDADE DA PROVA. PRECEDENTE DESTE COLEGIADO. AGRAVO REGIMENTAL DESPROVIDO.*
>
> *1. 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.*
>
> *2. A falta de documentação mínima dos procedimentos adotados pela polícia no tratamento da*

> *prova extraída de aparelhos eletrônicos, bem como a falta de adoção das práticas necessárias para garantir a integridade do conteúdo, torna inadmissível a prova, por quebra da cadeia de custódia. Entendimento adotado por esta Quinta Turma no julgamento do AgRg no RHC 143.169/RJ, de minha relatoria, DJe de 2/3/2023.*
>
> *3.* ***Como decidimos naquela ocasião, "é ônus do Estado comprovar a integridade e confiabilidade das fontes de prova por ele apresentadas. É incabível, aqui, simplesmente presumir a veracidade das alegações estatais, quando descumpridos os procedimentos referentes à cadeia de custódia. No processo penal, a atividade do Estado é o objeto do controle de legalidade, e não o parâmetro do controle; isto é, cabe ao Judiciário controlar a atuação do Estado-acusação a partir do direito, e não a partir de uma autoproclamada confiança que o Estado-acusação deposita em si mesmo".***
>
> *4. Agravo regimental desprovido. (AgRg nos EDcl no AREsp n. 2.342.908/MG, relator Ministro RIBEIRO DANTAS, QUINTA TURMa, DJe de 26/2/2024.)(grifos nossos)*

De outro giro, sob a perspectiva do diálogo das fontes entre processo penal e processo civil, é oportuno ressalvar a pertinência da argumentação delineada pela defesa ao suscitar a inidoneidade de relatório de análise de extração de dados baseado em *print screen* de diálogos entre usuários de Whatsapp.

Ainda que se considere que os atos promovidos por agentes públicos no âmbito de investigação preliminar apresentem legitimidade apriorística, subsiste a disposição do art. 422 do Código de Processo Civil – CPC, pelo qual qualquer reprodução mecânica, como a fotográfica, a cinematográfica, a fonográfica ou de outra espécie, tem aptidão para fazer prova dos fatos ou das coisas representadas, se a sua conformidade com o documento original não for impugnada por aquele contra quem foi produzida.

Assim, o CPC dispõe, no § 1º do art. 422, que "[*a]s fotografias digitais e as extraídas da rede mundial de computadores fazem prova das imagens que reproduzem, devendo, se impugnadas, ser apresentada a respectiva autenticação eletrônica ou, não sendo possível, realizada perícia*".

Com mais razão, portanto, ao se tratar de investigação criminal, em que a exigência de autenticidade e integridade da potencial evidência digital é maior, o que vai exigir, minimamente, que ***"[a] autoridade policial responsável pela apreensão de um computador (ou outro dispositivo de armazenamento de informações digitais) deve copiar integralmente (bit a bit) o conteúdo do dispositivo, gerando uma imagem dos dados: um arquivo que espelha e representa fielmente o conteúdo original***" (AgRg no RHC n. 143.169/RJ, relator Ministro Messod Azulay Neto, relator para acórdão Ministro Ribeiro Dantas, Quinta Turma, julgado em 7/2/2023, DJe de 2/3/2023).

Na esteira das preocupações com a garantia da autenticidade dos novos meios de prova, a Associação Brasileira de Normas Técnicas, desde o ano de 2013, estabelece na NBR ISO/IEC 2703 7:2013 diretrizes acerca do manuseio inicial

de evidências digitais, o que compreende a sua identificação, coleta, aquisição e preservação.

O referido documento técnico, 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. Recomenda-se, na norma técnica, que o sujeito responsável pela aquisição e tratamento do material de interesse para uma investigação descreva, desde o início, toda a cronologia de movimento e manipulação da potencial evidência digital, convindo que o registro da cadeia de custódia contenha, no mínimo, informações sobre o identificador único da evidência; quem acessou a evidência, com registro de tempo e local; quem checou a evidência interna e externamente nas instalações de preservação da evidência, com respectivo registro de tempo e local; propósito de verificação da evidência; além de quaisquer alterações inevitáveis da potencial evidência digital, assim como o nome do indivíduo responsável para tanto e a justificativa para a introdução da alteração.

Convém, assim, que o material epistemológico digital de interesse à persecução penal seja tratado mediante critérios bem definidos, que possibilitem a sua preservação, na maior medida possível, notadamente com explícita indicação de quem foi responsável pelo seu reconhecimento, coleta, acondicionamento, transporte e processamento, que deverá ser formalizado em laudo produzido por perito, notadamente com indicação da metodologia empregada e das ferramentas eventualmente utilizadas.

A documentação de cada etapa da cadeia de custódia é fundamental, a fim de que o procedimento seja auditável. É dizer, as partes devem ter condições de aferir se o método técnico-científico para a extração dos dados foi devidamente observado (**auditabilidade** da evidência digital). Ainda, faz-se importante que a mesma sequência de etapas sempre redunde nos mesmos resultados, ou seja, que os mesmos procedimentos/instrumentos gerem a mesma conclusão (r**epetibilidade** da evidência digital). Igualmente, ainda que sejam utilizados métodos diversos, os resultados devem ser os mesmos (**reprodutibilidade** da evidência digital). Por fim, os métodos e procedimentos devem ser justificáveis, sob a ótica da melhor técnica (**justificabilidade** da evidência digital).

Assim, pode-se dizer que a auditabilidade, a repetibilidade, a reprodutibilidade e a justificabilidade são quatro aspectos essenciais das evidências digitais, as quais buscam ser garantidas pela utilização da metodologia da ABNT. A ausência de quaisquer deles redunda em um elemento epistemologicamente frágil e deficiente, e, portanto, de valor probatório reduzido ou nulo.

Tudo isso volta-se à tentativa de garantir o princípio da mesmidade, é dizer, 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").

Uma forma de observar o princípio da mesmidade é por meio da utilização da técnica de algoritmo *hash*. Como bem explana o Min. Ribeiro Dantas, em seu voto no AgRg no RHC n. 143.169/RJ:

> *"Aplicando-se uma técnica de algoritmo hash, é possível obter uma assinatura única para cada arquivo - uma espécie de impressão digital ou DNA, por assim dizer, do arquivo. Esse código hash gerado da imagem teria um valor diferente caso um único bit de informação fosse alterado em alguma etapa da investigação, quando a fonte de prova já estivesse sob a custódia da polícia. Mesmo alterações pontuais e mínimas no arquivo resultariam numa hash totalmente diferente, pelo que se denomina em tecnologia da informação de efeito avalanche: [...].*
>
> *Desse modo, comparando as hashes calculadas nos momentos da coleta e da perícia (ou de sua repetição em juízo), é possível detectar se o conteúdo extraído do dispositivo foi alterado, minimamente que seja. Não havendo alteração (isto é, permanecendo íntegro o corpo de delito), as hashes serão idênticas, o que permite atestar com elevadíssimo grau de confiabilidade que a fonte de prova permaneceu intacta."*
>
> *(AgRg no RHC n. 143.169/RJ, relator Ministro Messod Azulay Neto, relator para acórdão Ministro Ribeiro Dantas, Quinta Turma, julgado em 7/2/2023, DJe de 2/3/2023).*

Além da técnica do algoritmo *hash*, também deve ser utilizado um *software* confiável, auditável e amplamente certificado, que possibilite o acesso, a interpretação e a extração dos dados do arquivo digital. Em outras palavras: 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.

Sobre o que interessa à solução da controvérsia, assim decidiu o Tribunal impetrado (fls. 13/16):

> *“De fato, o entendimento jurisprudencial contemporâneo assenta que “Os dados decorrentes de comunicações realizadas por meio de comunicação telefônica ou pela internet, como mensagens ou caracteres armazenados em aparelhos celulares, são invioláveis, somente podendo ser acessados mediante prévia autorização judicial” (STJ - AgRg no HC n. 567.668/SC, relator Ministro Felix Fischer, Quinta Turma, julgado em 6/10/2020, DJe de 20/10/2020).*
>
> *Todavia, na presente hipótese, verifico que a extração dos dados do aparelho celular do corréu Marcos Antônio Pereira Sena foi devidamente autorizada por decisão judicial fundamentada, havendo observância as garantias constitucionais dos acusados, notadamente a prevista no art. 5º, XII, da CF/88, que exige ordem judicial específica para acesso a dados digitais.*
>
> *Portanto, no caso em tela, os dados extraídos foram devidamente documentados nos autos, com indicação do procedimento técnico utilizado e da autorização judicial que lastreou a medida. Ademais, a defesa não demonstrou a existência de qualquer indício de adulteração da referida*

prova ou de má-fé na sua produção, que pudesse justificar a pretendida ilicitude

A prova, portanto, foi colhida em estrita observância ao devido processo legal, sem vícios que autorizem sua exclusão dos autos.

A ausência da certificação denominada como algoritmo "hash" é questão que já foi decidida por este Colegiado, em julgamento por mim relatado, no qual ficou decidido que a mencionada certificação é elemento de reforço à segurança do material interceptado e não um requisito indispensável à sua produção ou disponibilização às partes (TJES, APC 5005830- 57.2023.8.08.0000. Rel. Desª. Rachel Durão Correia Lima. 1ª Câmara Criminal. Julgado em 13/7/2023).

Referido Acórdão foi utilizado como fundamento de outro julgamento realizado pela Segunda Câmara Criminal, no qual ficou assentado que "O código hash é um elemento de reforço à segurança do material interceptado e não um requisito indispensável à sua produção ou disponibilização às partes (Nesse sentido: TJES, APC 5005830-57.2023.8.08.0000. Rel. Desª. Rachel Durão Correia Lima. 1ª Câmara Criminal. Julgado em 13/7/2023). Sua idoneidade, portanto, pode ser aferida mediante o cotejo de todo material probatório produzido ao longo da instrução processual, não havendo que se falar em nulidade pela mera ausência da referida técnica" (TJES, APC 0009360-20.2021.8.08.0035. Rel. Des. HELIMAR PINTO. 2ª Câmara Criminal. Julgado em 12/Jun/2024).

No mesmo sentido, "tanto no Código de Processo Penal quanto na Lei n° 9.296/96, não há qualquer dispositivo determinando que os arquivos interceptados possuam um determinado código de autenticação. A experiência prática ensina que é comum os dados e os áudios serem certificados com o código hash, que figura como fator corroborador da integridade do acervo obtido pelas interceptações telefônica e ambiental no curso das investigações. Todavia, trata-se de um elemento de reforço à segurança do material interceptado e não um requisito indispensável à sua produção ou disponibilização às partes" (TRF4, ACR 5013041- 90.2021.4.04.7201, SÉTIMA TURMA, Relator DANILO PEREIRA JUNIOR, juntado aos autos em 30/03/2023).

A d. Procuradora de Justiça subscritora do parecer destacou que "o código hash apenas confere certeza de identidade relacionada à cópia realizada, nada interferindo sobre os dados copiados ou seu conteúdo. Isso significa que o código hash não confere certeza de inviolabilidade probatória, justamente porque incide sobre aquilo que foi copiado, ou seja, se tiver havido uma adulteração probatória no celular apreendido, entre o momento de sua apreensão e a extração de dados, a existência ou não de criptografia hash na cópia que foi realizada posteriormente à adulteração, em nada influenciará na verificação de confiabilidade, bem como, não indicará a existência de possível adulteração, em algum momento".

Quanto à alegada quebra da cadeia de custódia, os autos demonstram que o aparelho foi apreendido sob termo de custódia e encaminhado à perícia sem interrupções. A mera ausência do algoritmo "hash", ou de qualquer outro reforço de certificação, consoante já visto, não implica, por si só, em violação à cadeia de custódia,

> *pois a integridade dos dados foi preservada pelos registros formais do procedimento, conforme exigido pelo art. 158 do CPP.*
>
> *Dessa forma, a defesa não se desincumbiu do ônus de apresentar elementos que pudessem comprometer a validade da prova questionada, não havendo qualquer indício de sua adulteração ou manipulação, sendo que os dados extraídos foram realizados por agentes públicos dotados de fé pública."*

No caso dos autos, verifica-se que a equipe policial não se desincumbiu de trazer aos autos registros válidos sobre a extração dos dados, tendo a Corte *a quo* se limitado a afastar a aventada ilegalidade em razão de o procedimento ter sido autorizado judicialmente, ponderando, ainda, não haver proibição de extração de dados do aparelho celular pela polícia judiciaria, concluindo que a simples ausência do algoritmo *hash* não compromete a idoneidade da prova.

De relevo trazer à baila o entendimento majoritário desta Quinta Turma no sentido de que "*é ônus do Estado comprovar a integridade e confiabilidade das fontes de prova por ele apresentadas. É incabível, aqui, simplesmente presumir a veracidade das alegações estatais, quando descumpridos os procedimentos referentes à cadeia de custódia*" (AgRg no RHC n. 143.169/RJ, relator Ministro Messod Azulay Neto, relator para acórdão Ministro Ribeiro Dantas, Quinta Turma, DJe de 2/3/2023).

Nessa mesma esteira, no âmbito doutrinário, Gustavo Badaró pontua que *"[n]ão havendo documentação da cadeia de custódia, e não sendo possível sequer ligar o dado probatório à ocorrência do delito, o mesmo não deverá ser admitido no processo. A parte que pretende a produção de uma prova digital tem o ônus de demonstrar previamente a sua integridade e autenticidade, por meio da documentação da cadeia de custódia. Sem isso, sequer é possível constatar sua relevância probatória*" (BADARÓ, p. 183).

Assim, inafastável a conclusão de que*, in casu*, não houve a adoção de procedimentos que assegurassem a idoneidade e a integridade dos elementos obtidos pela extração dos dados do celular do corréu Marcos Antônio Pereira Sena. Logo, evidentes o prejuízo causado pela quebra da cadeia de custódia e a imprestabilidade da prova digital.

Ante o exposto, com fundamento no art. 34, XX, do Regimento Interno do Superior Tribunal de Justiça, não conheço do presente *mandamus*, mas concedo de ofício a ordem para que sejam declaradas inadmissíveis as provas decorrentes da extração de dados do celular de Marcos Antônio Pereira Sena, bem como as delas decorrentes, devendo o Juízo singular avaliar a existência de demais elementos probatórios que sustentem a manutenção da condenação.

Publique-se.

Intimem-se.

Brasília, 29 de setembro de 2025.

JOEL ILAN PACIORNIK
Relator

Documento eletrônico VDA50900819 assinado eletronicamente nos termos do Art.1º §2º inciso III da Lei 11.419/2006
Signatário(a): JOEL ILAN PACIORNIK Assinado em: 29/09/2025 09:38:35
Publicação no DJEN/CNJ de 01/10/2025. Código de Controle do Documento: 7116e2f5-f3b4-4f1b-afa8-ab2213e4e9bb