RECURSO EM HABEAS CORPUS Nº 186138 - SP (2023/0304725-2)

RELATORA	**:**	**MINISTRA DANIELA TEIXEIRA**
RECORRENTE	:	JOSE MARIO CORREIA CAVALCANTI
ADVOGADOS	:	SÉRGIO SALGADO IVAHY BADARÓ - SP124529
		ROGERIO NEMETI - SP208529
		ZAYRA DOS SANTOS DIAS - DF035372
		CARLOS HUMBERTO FAUAZE FILHO - DF043188
		BARBARA SIQUEIRA FURTADO - SP357824
		BARBARA DO ESPIRITO SANTO PASELLO - SP418891
		DOUGLAS HENRIQUE NORKEVICIUS - SP490782
RECORRIDO	:	MINISTÉRIO PÚBLICO DO ESTADO DE SÃO PAULO
CORRÉU	:	JORGE HADAD SOBRINHO

DECISÃO

Trata-se de recurso em *habeas corpus* com pedido de liminar interposto por JOSÉ MÁRIO CORREIA CAVALCANTI contra acórdão proferido pelo TRIBUNAL DE JUSTIÇA DO ESTADO DE SÃO PAULO (HC 2091516-67.2023.8.26.0000).

O recorrente foi condenado à pena de 1 ano, 8 meses e 16 dias de detenção, em regime aberto, pela prática dos crimes dos artigos 299 do Código Penal, 2º, inciso II, e 12, inciso I da Lei 8.137/1990. Substituiu-se a pena corporal por restritivas de direitos.

O *habeas corpus* impetrado na origem foi denegado em decisão assim ementada (e-STJ, fl. 93):

> *HABEAS CORPUS – Artigo 2º, inciso II c.c. os artigos 11 "caput" e 12, inciso I, da Lei nº 8.137/90, por trinta e quatro vezes – Pleito de declaração de ilicitude da provas obtidas por meio da quebra do sigilo telemático do paciente – Acolhimento – Impossibilidade – Inexistência de exigência legal de cálculo do código "hash" para a validação de arquivos eletrônicos (Lei nº 12.965/2014 – Marco Civil da Internet) – Ausência de apontamento de ilegalidade dos arquivos recebidos e utilizados pelo Ministério Público – Hipótese em que o "Parquet" não participou da colheita da prova e não foi o responsável pela apreensão do computador, tampouco pela extração de mensagens nele constantes – Elementos de prova conhecidos pela Defesa desde o início da ação penal, mas que não foram impugnados oportunamente, nem mesmo sob o procedimento do artigo 145 do CPP – Parte do material, ademais, acessível diretamente ao provedor mediante senha, não havendo sequer de se falar em código "hash" - Inexistência de ilegalidade a ser reconhecida nesta via.*

A defesa alega: a) que "*ao oferecer a peça acusatória, o Parquet, no corpo da denúncia, se utilizou de diversas conversas de e- mails obtidos através*

da quebra do sigilo telemático do Paciente, do corréu JORGE HADAD e de mais oito contas de e-mails que a eles estariam supostamente relacionadas" (e-STJ, fls. 106-107); b) que " *durante a fase de instrução probatória, o Ministério Público não buscou produzir um adminículo de prova sequer que comprovasse a tese acusatória, sendo que ao apresentar suas alegações finais, baseou-se, exclusivamente, no conteúdo das mensagens de e-mails obtidas na ação cautelar de quebra de sigilo telemático - a qual antecedeu o próprio oferecimento da denúncia*" (e-STJ, fl. 1-7); c) que as únicas provas indicadas pelo Parquet para embasar o pedido de condenação foram os referidos e-mails; d) que o recorrente requereu a intimação do Ministério Público para informar o código *hash* do material que recebeu das companhias de e-mail TERRA, YAHII, UOL, MICROSOFT, IG, TEKTRONIK e HOTMAIL, demonstrando sua imprescindibilidade, todavia o requerimento foi indeferido; e) que "*o Ministério Público, espontaneamente, noticiou que "os provedores não forneceram o código hash ao disponibilizarem os e-mails e nem estão obrigados a tanto, conforme Lei nº. 12.965/2014"* (e-STJ, fl. 108); e f) que deve ser reconhecida "*a inadmissibilidade das provas produzidas com a quebra do sigilo telemático do Paciente, tendo em vista os riscos contundentes à sua confiabilidade diante da ausência da documentação referente a cadeia de custódia."* (e-STJ, fl. 112).

Requereu liminar para suspender "*o andamento da ação penal originária, uma vez que estão presentes os requisitos necessários à sua concessão"* (e-STJ, fl. 21). No mérito, requer sejam declaradas "*inadmissíveis as provas obtidas a partir da quebra do sigilo telemático do Paciente, do corréu JORGE HADAD e e dos domínios eletrônicos que a eles estariam supostamente vinculados, bem como de todas as provas delas derivadas*" (e-STJ, fl. 23).

O Ministério Público manifestou-se pelo não conhecimento ou, caso conhecido, pelo desprovimento do recurso ordinário (e-STJ fls. 279-284).

É o relatório.

Decido.

Como relatado, pretende o recorrente que seja dado provimento ao recurso para, reconhecendo a quebra da cadeia de custódia, sejam consideradas " *inadmissíveis as provas obtidas a partir da quebra do sigilo telemático do Paciente, do corréu JORGE HADAD e e dos domínios eletrônicos que a eles estariam supostamente vinculados, bem como de todas as provas delas derivadas*" (e-STJ, fl. 23).

Razão assiste ao recorrente.

Conforme jurisprudência dessa Corte, a cadeia de custódia refere-se à *"idoneidade do caminho que deve ser percorrido pela prova até sua análise pelo magistrado, e, uma vez ocorrida qualquer interferência durante o trâmite processual, esta pode resultar na sua imprestabilidade. Não se trata, portanto, de nulidade processual, senão de uma questão relacionada à eficácia da prova, a ser analisada caso a caso"* (RHC n. 158.441/PA, relator Ministro Olindo Menezes, Sexta Turma, DJe de 15/6/2022).

Assim, a finalidade principal da cadeia de custódia, enquanto decorrência lógica do conceito de corpo de delito (art. 158 do CPP), é assegurar que

os vestígios deixados no mundo material por uma infração penal, correspondem exatamente àqueles coletados pela acusação, examinados e apresentados em juízo. Busca-se, desta forma, 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 espécie, a questão relativa à quebra de cadeia de custódia é mais complexa considerando tratar-se de questão relacionada à prova digital e, após análise do conjunto probatório anexado aos presentes autos, vislumbro riscos contundentes à confiabilidade das provas produzidas pela acusação.

Ressalto, ainda, que a tese trazida pelos recorrentes é, apesar da afirmação acima, de compreensão simples e não demanda, ao contrário do alegado pela Corte de origem, aprofundamento no conjunto probatório.

O fato é que os provedores não forneceram o código *hash* ao disponibilizarem as mensagens de e-mails obtidas na ação cautelar de quebra de sigilo telemático que foram usadas pela acusação, para sustentar a inicial acusatória, em suas alegações finais, como provas para requerer a condenação do recorrente e, posteriormente, a prolação da sentença condenatória.

A autoridade responsável pela colheita de dados e informações digitais deve zelar pela sua integridade, especialmente face à volatilidade dos dados que são armazenados digitalmente, a fim de fazer com que seja possível se verificar se algum deles foi alterado, suprimido ou adicionado após a sua coleta inicial.

Aplicando-se a técnica do algoritmo *hash* é possível obter uma assinatura única para cada arquivo, como uma espécie de DNA ou impressão digital. Única. O código *hash* gerado de imagem ou documento apresentaria um valor diferente caso um *bit* de informação fosse alterado em qualquer momento da investigação, quando a fonte de prova já estivesse sob a custódia da polícia ou do órgão acusatório. Mesmo alterações pontuais e mínimas no arquivo resultariam numa *hash* totalmente diferente, pelo que se denomina em tecnologia da informação de efeito avalanche.

No sentido de expor a importância do código *hash,* há manifestação de Gustavo Badaró:

> *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, é necessário fazer uma cópia ou espelhamento, obtendo o bitstream da imagem do disco rígido ou suporte de memória em que o dado digital está registrado. Além disso, por meio do cálculo do algoritmo hash, é possível verificar a perfeita identidade da cópia com o arquivo original. Com isso, de um lado, se preserva o material original e, de outro, se garante a autenticidade e integridade do material que foi examinado pelos peritos. Evidente que todo esse processo técnico precisa ser documentado e registrado em todas as suas etapas. Tal exigência é uma garantia de um correto emprego das operating procedires, especialmente por envolver um dado probatório volátil e sujeito à mutação. Exatamente pela diferença ontológica da prova digital com relação a prova tradicional, bem como devido àquela que não se valer de uma linguagem natural, mas digital, é que uma cadeia de custódia detalhada se faz ainda mais necessária. Realmente, a documentação da cadeia de custódia é essencial no*

caso de análise dos dados digitais, porque permitirá assegurar a autenticidade e integralidade dos elementos de provas e submeter tal atividade investigativa à posterior crítica judiciária das partes, e excluirá que tenha havido alterações indevidas do material digital. (BADARÓ, Gustavo. Os Standards metodológicos de produção na prova digital e a importância da cadeia de custódia. Boletim IBCCRIM, 2021, p.2).

E, ainda, Alexandre Morais da Rosa:

Considerando as características dos dados alvo da prova (volatilidade e fragilidade), a evidência digital pode ser alterada, editada, manipulada ou destruída de modo doloso ou culposo, tanto pelos agentes processuais, como pelos peritos. A E-Evidência constitui-se pelos formatos físico e lógico. Desde o rastreio e obtenção, até o descarte, todo o percurso e tratamento devem ocorrer com a "identificação" dos dispositivos (externa, via dispositivo de armazenamento e, se possível e viável, a interna: os dados), evitando-se sobreposições. Os cuidados com a Cadeia de Custódia Digital (controle de obtenção, movimento e acesso aos dados, com a identificação, histórico de acesso, por tempo, local e motivação, além de eventuais alterações) se potencializam, porque é dever de todos os agentes que participam da obtenção ou tratamento da evidência digital, além de conhecimentos mínimos (p.ex. o programa MD5Summer verifica a integridade dos arquivos transmitidos pela web), a respectiva documentação das condições matérias do rastreamento, identificação, fixação, aquisição (cópia integral e documentada da evidência, observando-se a conformidade: função de Hash), preservação (manutenção do original da evidência intacto), análise, intercorrências, armazenamento e descarte (vide item 9.7). Os "dados" se distinguem entre "voláteis" (p.ex. memória RAM etc.) ou "não voláteis" (p.ex. HD, cards de memória, etc.). Os voláteis podem se perder mais facilmente, motivo pelo qual o modo como eventual Busca e Apreensão é realizada pode destruir ou comprometer o conteúdo.

(...)

A apuração de condutas criminais que se valem do ambiente digital (próprias ou impróprias) exige comprovação adequada por meio da observância de regras, metodologias e procedimentos técnicos. Os prints extraídos de endereços da web ou de smartphones (whatsapp, por exemplo), são qualificados como "imagem", submetidos à demonstração do modo de obtenção e/ou produção. A maleabilidade e a vulnerabilidade dos dados digitais, principalmente pela ampla possibilidade de criação de diálogos falsos (Fakes), por meio de aplicativos disponíveis na rede, reafirma a necessidade de observância da Cadeia de Custódia Digital. Diferentemente do regime do Processo Civil, em que a não impugnação pela parte adversa consolida a validade, no Processo Penal o ônus da prova é da acusação, motivo pelo qual a demonstração da existência, validade e eficácia é atribuída a quem acusa. O print, por si, sem a demonstração da regularidade (metadados, integridade, código Hash, quem, como, onde, atendidas as regras de identificação e coleta), não produz nenhum efeito probatório. Em geral, será preciso a análise do dispositivo, se possível de todos os interlocutores, dada a possibilidade de manipulação.

(ROSA, Alexandre de Morais da. Guia do processo penal estratégico: de acordo com a teoria dos jogos e o MCDA-C / A. Florianópolis, SC : Emais, 2021).

Também há R.W.R. Carvalho:

Função de hash: Algoritmo que 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 altera se um único bit da entrada for alterado, acrescentado ou retirado. [...] Para a coleta de evidências digitais deve ser calculado o hash da mídia, para fins comparativos com o hash calculado na coleta, após manuseio da mesma da evidência e cópias forenses". (CARVALHO, R.W.R. A importância da cadeia de custódia na computação forense. Revista Brasileira de Criminalística, 2020, p. 134-135).

Por fim, há decisão desta Corte:

PENAL E PROCESSUAL PENAL. AGRAVO REGIMENTAL NO RECURSO ORDINÁRIO EM HABEAS CORPUS. OPERAÇÃO OPEN DOORS. FURTO, ORGANIZAÇÃO CRIMINOSA E LAVAGEM DE DINHEIRO. ACESSO A DOCUMENTOS DE COLABORAÇÃO PREMIADA. FALHA NA INSTRUÇÃO DO HABEAS CORPUS. CADEIA DE CUSTÓDIA. INOBSERVÂNCIA DOS PROCEDIMENTOS TÉCNICOS NECESSÁRIOS A GARANTIR A INTEGRIDADE DAS FONTES DE PROVA ARRECADADAS PELA POLÍCIA. FALTA DE DOCUMENTAÇÃO DOS ATOS REALIZADOS NO TRATAMENTO DA PROVA. CONFIABILIDADE COMPROMETIDA. PROVAS INADMISSÍVEIS, EM CONSEQUÊNCIA. AGRAVO REGIMENTAL PARCIALMENTE PROVIDO PARA PROVER TAMBÉM EM PARTE O RECURSO ORDINÁRIO.

1. O habeas corpus não foi adequadamente instruído para comprovar as alegações defensivas referentes ao acesso a documentos da colaboração premiada, o que impede o provimento do recurso no ponto.

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

3. Embora o específico regramento dos arts. 158-A a 158-F do CPP (introduzidos pela Lei 13.964/2019) não retroaja, a necessidade de preservar a cadeia de custódia não surgiu com eles. Afinal, a ideia de cadeia de custódia é logicamente indissociável do próprio conceito de corpo de delito, constante no CPP desde a redação original de seu art. 158. Por isso, mesmo para fatos anteriores a 2019, é necessário avaliar a preservação da cadeia de custódia.

4. 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.

5. Aplicando-se uma técnica de algoritmo hash, é possível obter uma assinatura única para cada arquivo, que 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. 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 modificado.

6. 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.

7. No caso dos autos, a polícia não documentou nenhum dos atos por ela praticados na arrecadação, armazenamento e análise dos computadores apreendidos durante o inquérito, nem se preocupou em apresentar garantias de que seu conteúdo permaneceu íntegro enquanto esteve sob a custódia policial. Como consequência, não há como assegurar que os dados informáticos periciados são íntegros e idênticos aos que existiam nos computadores do réu.

8. Pela quebra da cadeia de custódia, são inadmissíveis as provas extraídas dos computadores do acusado, bem como as provas delas derivadas, em aplicação analógica do art. 157, § 1º, do CPP.

9. Agravo regimental parcialmente provido, para prover também em parte o recurso ordinário em habeas corpus e declarar a inadmissibilidade das provas em questão.

(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.)

Oportuna a colocação do Ministro Ribeiro Dantas ao proferir seu voto no julgado supracitado, ao afirmar que "*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*". Assim, afirmar que os *hashes* não são exigíveis e não necessários, como fez o MPSP "*equivale a dizer que a atuação estatal não é submetida a controle e que, se o Estado-acusação afirmar que atuou corretamente no manejo da prova, isso já bastaria para encampar suas conclusões, dispensando-se a demonstração objetiva da regularidade de seus atos. Nada mais incompatível, certamente, com um processo penal democrático, racional e pautado em comprovações objetivas, para além das impressões pessoais dos agentes públicos que nele atuam".*(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).

No presente caso, o Ministério Público do Estado de São Paulo tinha o dever de informar, nos autos, como se deram os procedimentos de recebimento do material pelos diversos provedores e como os analisou e manuseou. Mais do que isso, é imprescindível a informação de como o material digital fora compartilhado com o órgão acusatório.

No presente caso, a falta dos *hashes* torna impossível a verificação da integridade da prova trazida aos autos, impedindo a confirmação da confiabilidade dos documentos que fundamentaram o decreto condenatório.

De fato, é ônus do Estado demonstrar que os elementos e informações colhidos correspondem exatamente àqueles utilizados na ação penal e, no caso trazido aos autos, nem os provedores, nem a autoridade policial e nem o *Parquet* trouxeram aos autos prova que garantisse a integridade das mensagens de e-mails.

Tendo em vista que "*as irregularidades constantes da cadeia de custódia devem ser sopesadas pelo magistrado com todos os elementos produzidos na instrução, a fim de aferir se a prova é confiável. Assim, à míngua de outras provas capazes de dar sustentação à acusação, deve a pretensão ser julgada improcedente,*

por insuficiência probatória, e o réu ser absolvido" (HC n. 653.515/RJ, relator Ministro Rogerio Schietti Cruz, Sexta Turma, julgado em 23/11/2021, DJe de 1/2/2022), concluo que a quebra da cadeia de custódia trouxe gravíssimo prejuízo à confiabilidade da prova manuseada nos autos da ação penal originária e a ofensa ao art. 158 do CPP.

As mensagens de e-mails utilizadas sem o fornecimento dos respectivos *hashes* são, portanto, inadmissíveis, por falharem num teste de confiabilidade mínima. São inadmissíveis, da mesma forma, as provas delas derivadas, em aplicação analógica do art. 157, § 1º, do CPP.

Pelo exposto, **dou provimento** ao recurso em *habeas corpus*, para declarar inadmissíveis as mensagens de e-mails inseridas nos autos sem os respectivos códigos *hash*, bem como todas as provas delas derivadas.

Caberá ao juízo de primeira instância desentranhar dos autos as provas inadmissíveis e avaliar se (e quais) outras delas decorrem, para que sejam também desentranhadas, retomando-se a instrução do feito sem aquelas.

Comunique-se, **com urgência**, as instâncias ordinárias, em especial o Tribunal de Justiça de São Paulo, onde encontra-se, pendente o julgamento de apelação criminal nos autos n. 1000744-36.2019.8.26.0511 e que deverá remeter, à vara de origem, os autos para as providências aqui determinadas.

Publique-se. Intime-se.

Brasília, 22 de março de 2024.

Ministra Daniela Teixeira
Relatora

Edição nº 0 - Brasília, Publicação: quarta-feira, 03 de abril de 2024
Documento eletrônico VDA40808462 assinado eletronicamente nos termos do Art.1º §2º inciso III da Lei 11.419/2006
Signatário(a): DANIELA RODRIGUES TEIXEIRA Assinado em: 01/04/2024 19:08:24
Publicação no DJe/STJ nº 3837 de 03/04/2024. Código de Controle do Documento: 79fa15e4-40fd-469d-b39a-7e89598fde65