RECLAMAÇÃO 49.369 RIO GRANDE DO SUL

RELATOR	**: MIN. RICARDO LEWANDOWSKI**
RECLTE.(S)	: DAVID GUILHERME TOVO
ADV.(A/S)	: FERNANDO DE SOUZA ALVES
RECLDO.(A/S)	: JUIZ FEDERAL DA 5ª VARA FEDERAL DA SEÇÃO JUDICIÁRIA DE CAXIAS DO SUL
ADV.(A/S)	: SEM REPRESENTAÇÃO NOS AUTOS
BENEF.(A/S)	: MINISTÉRIO PÚBLICO FEDERAL
PROC.(A/S)(ES)	: PROCURADOR-GERAL DA REPÚBLICA

Trata-se de reclamação, com pedido de medida liminar, proposta por David Guilherme Tovo, na qual alega a inobservância da Súmula Vinculante 14 pelo Juízo da 5ª Vara Federal de Caxias do Sul/RS.

A defesa técnica afirma que

> "[o] Reclamante foi preso preventivamente no dia 10 de dezembro de 2020, por decisão do insigne Magistrado Federal de Primeiro Grau, constante do evento 10, do Pedido de Prisão Preventiva nº 501298497.2020.4.04.7107, em tramitação na judiciosa Quinta Vara Federal de Caxias do Sul-RS, cujos fundamentos utilizados foram os estabelecidos nos artigos 312 e 313 do CPP, para garantia da ordem pública e por necessidade de aplicação da lei penal.
>
> Os fatos narrados pela equipe de investigação basearam-se, tão somente, em prova digital captada da 'nuvem' das empresas de *network*, sendo que nenhuma prova foi obtida através de mandado de busca e apreensão na posse do Reclamante" (pág. 2 do documento eletrônico 1).

Aduz que

> "[...] o Ministério Público Federal denunciou David como incurso nas sanções previstas nos artigos 33, *caput* (itens III.1, III.2 e III.4), e 35 (item II.1), ambos c/c artigo 40, inciso I, todos da Lei n. 11.343/06, na forma dos artigos 29 e 69, ambos do

Código" (pág. 3 do documento eletrônico 1).

Afirma, ainda, que o reclamante levantou as seguintes preliminares em sua defesa prévia: nulidade da prova digital – quebra da cadeia de custódia – e ausência de materialidade e justa causa do crime de tráfico de drogas.

Assevera que

> "[...] a preliminar de cerceamento de Defesa e nulidade da prova digital fundamentou-se em perícia técnica realizada por profissional da área de T.I. que analisou todo material disponibilizado às Defesas, tendo sido constatado que as conversas de *whatsapp* não estavam acessíveis em detrimento de estarem criptografadas, tudo conforme consta do laudo técnico/pericial que acompanha o presente recurso constitucional.
>
> Em que pese a situação em testilha o douto Magistrado de piso não alterou sua decisão que recebeu a denúncia, estando o feito de origem aguardando a realização da audiência de instrução (a qual ainda não possuí audiência aprazada)" (págs. 7-8 do documento eletrônico 1).

Sustenta que

> "[...] as únicas provas existentes em desfavor de David são estas, as quais a Defesa não conseguiu ter acesso!
>
> Pois bem, tal fato foi devidamente reconhecido pelo Magistrado de Primeiro Grau, no entanto entendeu este que A FALTA DE ACESSO DAS DEFESAS ÀS PROVAS BASILARES DA ACUSAÇÃO NÃO GERAM PREJUÍZOS A ESTAS E TAMPOUCO AO ANDAMENTO DO FEITO [...]" (págs. 9-10 do documento eletrônico 1).

Ao final, requer:

> "a) diante do descumprimento pelo juízo de origem daquilo que decidido por esta Corte de Justiça e estabelecido na Súmula Vinculante nº 14, no que toca ao acesso das Defesas a todos elementos de provas já documentados, o que caracterizou a violação de direitos fundamentais da ampla Defesa e da liberdade, seja suspensa a tramitação do feito de origem até final julgamento do presente recurso, determinando ao Juiz de Primeiro Grau que providencie o acesso das Defesas a todos os elementos de provas documentados, em especial os arquivos das provas digitais relativos as conversas do *Whatsapp* que se encontram criptografados, bem como, frente ao operado excesso de prazo para formação da culpa, revogue a prisão preventiva do Reclamante;
>
> b) Outrossim, quanto ao mérito, requer a ratificação da liminar pleiteada, com o provimento da presente Reclamação Constitucional, anulando o processo referido no preâmbulo, desde o ato de recebimento da denúncia (inclusive a decisão que a recebeu), de sorte a permitir à defesa a prévia consulta à totalidade dos arquivos digitais fornecidos pela Polícia Federal, abrindo-se, a seguir, prazo para apresentação da resposta à acusação e dando-se seguimento aos demais atos processuais" (págs. 14-15 do documento eletrônico 1).

É o relatório. Decido.

Consigno, de início, que não darei vista destes autos à Procuradora-Geral da República (art. 52, parágrafo único, do Regimento Interno do Supremo Tribunal Federal) por entender que esta reclamação reúne todas as condições necessárias para o seu julgamento, encontrando-se, pois, devidamente instruída.

Assinalo, ademais, que o art. 161, parágrafo único, do RISTF faculta ao Relator julgar a reclamação quando a matéria for objeto de jurisprudência consolidada na Corte, como se dá na espécie.

Posto isso, passo ao exame do mérito.

Bem examinados os autos, entendo que não existe afronta ao enunciado da Súmula Vinculante 14, segundo o qual

> "é direito do defensor, no interesse do representado, ter acesso amplo aos elementos de prova que, já documentados em procedimento investigatório realizado por órgão com competência de polícia judiciária, digam respeito ao exercício do direito de defesa".

Transcrevo, por oportuno, o seguinte trecho da decisão reclamada:

> "[...]
> **Nulidade da Prova Digital**
> As defesas sustentam, em síntese, a quebra da cadeia de custódia das provas digitais obtidas por meio de afastamento do sigilo e impossibilidade de vínculo delas com os fatos constantes da denúncia, diante de ausência de verificação de idoneidade dos dados obtidos, circunstâncias que, no seu entendimento, invalidam a prova digital/telemática e, por consequência, todas as dela decorrentes.
> Alegam, ainda, impossibilidade de acesso a arquivos de conversas de *whatsapp* criptografados no *HD* fornecido pela autoridade policial, inviabilizando o pleno conhecimento dos dados armazenados.
> A cadeia de custódia da prova, disciplinada nos arts. 158-A a 158-F do Código de Processo Penal com o advento do 'Pacote Anticrime' (Lei nº 13.964/19), trata do conjunto de procedimentos a serem observados durante a coleta das provas em processo penal, visando à preservação da integridade da prova colhida para fins de garantir a verificação de sua autenticidade pelas partes e pelo Juízo.
> Tratando-se de prova digital, à míngua de especificações técnicas no Código de Processo Penal quanto aos critérios a

serem adotados para garantir sua integridade, há que se verificar se o modo como os dados fornecidos pelas empresas de tecnologia foram recepcionados e gravados indica sua autenticidade ou se há indícios de que foram manipulados.

As defesas fundamentam seu pedido, em síntese, na ausência de códigos de verificação ('código *hashing'*) gerados pelas empresas, capazes de garantir que os arquivos que forneceram as provas digitais que embasaram a denúncia não sofreram qualquer tipo de adulteração, bem como na necessidade de que os dados, recepcionados na forma bruta, sejam 'tratados, acessados e revisados por especialistas para terem validade probatória'.

No caso dos autos, verifico da análise dos autos do Pedido de Quebra de Sigilo nº 5005875-32.2020.4.04.7107 que as provas digitais refutadas pela defesa tratam-se de dados armazenados nos servidores de empresas de tecnologia, que foram obtidos por meio de autorização judicial, recepcionados diretamente pelo Escritório de Análise e Inteligência da Polícia Federal, e, após sua recepção, gravados integralmente, em sua forma bruta, em dispositivo de mídia encaminhado e acautelado no Juízo, para fins de sua preservação, cuja cópia foi disponibilizada às defesas.

A ausência de indicação de código *hash* de todos os arquivos disponibilizados pelas empresas - em que pese se trate da melhor técnica de verificação da autenticidade de arquivos digitais - não implica quebra da cadeia de custódia e nem significa que tenha havido adulteração de arquivos. Vale destacar, no ponto, que não foram apontados pelas defesas quaisquer indícios de manipulação ou adulteração dos arquivos, tampouco há elementos que infirmem a boa-fé dos agentes na recepção e gravação dos dados.

A certeza quanto à integridade dos dados telemáticos fornecidos pelas empresas custodiantes é garantida por outros meios, como, por exemplo, a adoção de procedimentos para documentação do manuseio do material, desde o seu recebimento até eventual descarte, e para o seu

armazenamento.

Outrossim, em se tratando de dados telemáticos obtidos diretamente com o provedor de aplicações de *internet*, e não oriundos de equipamentos eletrônicos e dispositivos de armazenamento lógico porventura apreendidos com os suspeitos ou terceiros, é desnecessário o encaminhamento da prova à perícia, uma vez que, apesar de serem fornecidos de forma bruta pelas empresas requeridas, ou seja, sem tratamento e análise, o acesso e compreensão de seu conteúdo integral - incluindo os arquivos de conversas de *whatsapp* que a defesa alega não ter sido possível acessar, por estarem criptografados - não demanda intervenção de perito em computação forense, bastando para tanto a disponibilidade, pelas defesas dos acusados, de *softwares* capazes de realizar a leitura da íntegra dos arquivos originais constantes no *HD* cuja cópia foi franqueada às defesas.

Em suma, não vislumbro evidências concretas de quebra da cadeia de custódia da prova digital, e nem de alteração, supressão ou inserção de arquivos ou quaisquer outros elementos informativos no material fornecido pelos provedores, razão por que afasto a alegada nulidade da prova digital.

Ainda, não assiste razão à defesa de David Guilherme Tovo no sentido de que os arquivos de mensagens, áudios e figuras foram obtidos pela autoridade policial fora do prazo concedido judicialmente.

Com efeito, não se verifica nos autos circunstanciados elaborados pela autoridade policial elementos obtidos fora dos parâmetros temporais autorizados judicialmente. No que se refere, em especial, à obtenção dos arquivos de dados armazenados nas contas *Apple* e *Google* mantidas pelos investigados, destaco que as decisões que deferiram a quebra de sigilo de dados telefônicos e telemáticos não delimitaram prazo de alcance da referida, tal como ocorre nas interceptações telefônicas, mas apenas o limite temporal dos dados pretéritos armazenados (marco inicial fixado em 01/01/2020).

Além disso, a apresentação, pela autoridade policial, da

> análise dos dados recebidos em auto circunstanciado posterior ao período em que recepcionados os arquivos em nada fere a decisão judicial, notadamente porque necessária, no âmbito da investigação, a identificação e compilação dos elementos de interesse da investigação.
>
> As demais alegações deduzidas pelas defesas no ponto não são passíveis de exame nesta fase processual, porquanto dependem da instrução para que sejam eventualmente confirmadas.
>
> De todo modo, por não vislumbrar prejuízo às partes ou ao andamento do feito, determino a intimação da autoridade policial, com urgência, para que, no prazo de 5 (cinco) dias, esclareça nestes autos todos os procedimentos adotados na recepção e gravação dos dados obtidos através das quebras de sigilo, bem como indique os meios pelos quais as defesas poderão realizar a leitura de todos os arquivos brutos constantes no *HD* fornecido nos autos do procedimento investigativo, em especial os fornecidos pelas empresas *Facebook* Serviços *Online* do Brasil e *Apple Computer* Brasil Ltda.
>
> Com a resposta da autoridade policial, dê-se vista urgente às partes, pelo mesmo prazo.
>
> [...]" (págs. 33-36 do documento eletrônico 7; grifo no original).

Conforme se verifica, não houve negativa de acesso aos autos pela autoridade reclamada, a qual esclareceu que o acesso aos arquivos de conversas de *whatsapp* – que a defesa alega não ter sido possível acessar, por estarem criptografados –, não demandaria intervenção de perito, bastando a utilização de *softwares* capazes de realizar a leitura dos arquivos originais constantes no *HD*, cuja cópia fora franqueada à defesa.

Com efeito, a autoridade reclamada, garantindo a ampla defesa do reclamante, determinou até mesmo a intimação da autoridade policial para que indicasse os meios pelos quais a defesa poderia realizar a leitura de todos os arquivos brutos constantes no *HD* fornecido nos autos da

investigação, em especial os fornecidos pelas empresas *Facebook* e *Apple*.

Aliás, na petição inicial, a defesa reproduziu a resposta dada pela Polícia Federal aos questionamentos feitos pelo Juízo da 5ª Vara Federal de Caxias do Sul/RS, nestes termos:

> "Em atenção ao ofício nº 710013508014, expedido pelo Juízo da 5ª Vara Federal de Caxias do Sul/RS nos autos do PROCEDIMENTO ESPECIAL DA LEI DE ANTITÓXICOS Nº 5001826-11.2021.4.04.7101/RS, requisitando que a Polícia Federal 'esclareça nestes autos todos os procedimentos adotados na recepção e gravação dos dados obtidos através das quebras de sigilo, bem como indique os meios pelos quais as defesas poderão realizar a leitura de todos os arquivos brutos constantes no *HD* fornecido nos autos do procedimento investigativo', temos a informar o que segue:
>
> 1. No que respeita aos procedimentos adotados na recepção e gravação dos dados obtidos através das quebras de sigilo, fornecidos pela empresa de tecnologia *Apple Inc.*, temos a esclarecer que, inicialmente, são fornecidos pela custodiante *links* para *download* dos aquivos e senhas de acesso, os quais são remetidos através de *e-mail*, originado do endereço eletrônico lawenforcement@apple.com, direcionados ao endereço eletrônico de *e-mail* institucional analise.exs@pf.gov.br.
>
> 2. Cada ofício judicial encaminhado à empresa é registrado pela equipe responsável pelo atendimento desse tipo de requisição sob um número de caso (*Case Number*), ao qual a demanda permanece vinculada;
>
> 3. Mediante acesso aos *links* protegidos por senha enviados pelas custodiantes, é realizado o *download* da íntegra dos dados brutos armazenados, os quais são devidamente gravados em mídia para posterior remessa ao Juízo;
>
> 4. Em relação aos procedimentos adotados na recepção e gravação dos dados obtidos através das quebras de sigilo, fornecidos pela empresa de tecnologia *Google LLC*, temos a esclarecer que todos os ofícios judiciais são encaminhados à

custodiante através do portal LERS (*Law Enforcement. Request System* – acesso através do endereço eletrônico http://lers.google.com/signup_v2/landing), sendo que para cada ordem judicial remetida, é gerado um correspondente '*Número de referência do Google*', ao qual a demanda permanece vinculada.

5. O atendimento das demandas se dá através da disponibilização do conteúdo armazenado mesmo portal (LERS – *Law Enforcement Request System*), sendo que após acesso autenticado mediante a inserção de usuário e senha, através de *links* é realizado o *download* da íntegra dos dados brutos armazenados pela custodiante, os quais são devidamente gravados em mídia gravada para posterior remessa ao Juízo;

4. Para acesso e compreensão do conteúdo integral, a Equipe de Investigação utiliza no processamento e categorização dos arquivos brutos recebidos, o aplicativo forense *Cellebrite Physical Analyzer*, que nada mais é do que um programa comercial de computador adquirido pela Polícia Federal, destinado basicamente à leitura, decodificação e categorização de grandes volumes de dados;

5. O aludido aplicativo forense adquirido e utilizado pela Polícia Federal, é amplamente empregado tanto Brasil, quanto no exterior, como solução eficaz diante dessa demanda específica existente no curso das investigações criminais, decorrente da necessidade de análise de grande quantidade de informações disponibilizadas pelas empresas de tecnologia. Importante ressaltar, que o aplicativo *Cellebrite Physical Analyzer* é apenas um, dentre tantos outros *softwares* disponíveis no mercado, que oferece tais funcionalidades, consistentes, basicamente, como já foi dito, na leitura, decodificação e categorização desses dados. A operação do aplicativo não exige grandes habilidades específicas de seu usuário, pois executa rotinas quase que integralmente automatizadas, exigindo mínima intervenção do operador;

6. A grande maioria dos arquivos brutos disponibilizados pelas empresas de tecnologia, em decorrência de demandas

> relacionadas às quebras de sigilo de dados, é acessível através de qualquer computador que funcione integrado aos sistemas operacionais mais comuns (*Windows* e/ou *macOS*), não sendo necessária nenhuma chave e/ou senha adicional para abertura e leitura de dados criptografados eventualmente fornecidos. Conforme já foi pontuado, com o objetivo de facilitar o trabalho de análise desse tipo de conteúdo, a Polícia Federal opta pela utilização desse aplicativo, o qual executa automaticamente a leitura, decodificação e categorização desses dados;
>
> 7. As defesas dos réus tem acesso ao mesmo conteúdo analisado pela Polícia Federal, o qual já foi integralmente remetido ao Juízo em mídia gravada (*HD*). Repisamos que, conforme já foi pontuado, não é necessária nenhuma chave e/ou senha adicional para abertura e leitura de dados criptografados eventualmente fornecidos pelas empresas de tecnologia, bastando para tanto, a utilização de aplicativos pagos destinados a esse fim, os quais não podem ser fornecidos pela Polícia Federal" (pág. 7 do documento eletrônico 1; sem os grifos do original).

Portanto, inexiste violação à Súmula Vinculante 14. O acesso ao material decorrente das quebras de sigilo, conforme esclarecimento da autoridade policial, pode ser realizado por *softwares* disponíveis no mercado, não sendo necessária nenhuma chave ou senha especial para a abertura e leitura de eventuais dados criptografados.

Isso posto, julgo improcedente esta reclamação (art. 161, parágrafo único, do RISTF).

Publique-se.

Brasília, 21 de setembro de 2021.

Ministro **Ricardo Lewandowski**
Relator