SUPERIOR TRIBUNAL DE JUSTIÇA

AgRg no RECURSO EM MANDADO DE SEGURANÇA Nº 60237 - RO (2019/0062211-0)

RELATOR	:	**MINISTRO SEBASTIÃO REIS JÚNIOR**
AGRAVANTE	:	MINISTERIO PUBLICO DO ESTADO DE RONDONIA
AGRAVADO	:	W I
ADVOGADOS	:	ROCHILMER MELLO DA ROCHA FILHO - RO000635 DAVI DE PAIVA COSTA TANGERINO - SP200793 MARCELA TRIGO DE SOUZA - RJ127614

EMENTA

AGRAVO REGIMENTAL EM RECURSO EM MANDADO DE SEGURANÇA. DECISÃO MANTIDA POR SEUS PRÓPRIOS FUNDAMENTOS. PENAL. PROCESSO PENAL. INTERCEPTAÇÃO DE DADOS. ASTREINTES. POSSIBILIDADE EM ABSTRATO. CRIPTOGRAFIA DE PONTA A PONTA. IMPOSSIBILIDADE FÁTICA, NO CASO CONCRETO, DE CUMPRIMENTO DA ORDEM JUDICIAL. PRECEDENTES.

1. Não há como abrigar agravo regimental que não logra desconstituir o fundamento da decisão atacada.

2. *É entendimento consolidado no Superior Tribunal de Justiça que a pendência de julgamento no STF de ação em que se discute a constitucionalidade de lei não enseja o sobrestamento dos recursos que tramitam no STJ, salvo determinação expressa da Suprema Corte.* [...] (REsp n. 1.393.421/SE, Ministro Herman Benjamin, Segunda Turma, DJe 24/10/2016).

3. [...] *deve ser afastada a multa aplicada ante a impossibilidade fática decorrente de criptografia intransponível, sendo certo que os benefícios advindos da criptografia de ponta a ponta se sobrepõem às eventuais perdas pela impossibilidade de se coletar os dados das conversas dos usuários da tecnologia (RMS n. 60.531/RO, relator Ministro NEFI CORDEIRO, relator para acórdão Ministro RIBEIRO DANTAS, TERCEIRA SEÇÃO, julgado em 9/12/2020, DJe 17/12/2020)* [...] (AgRg no RMS n. 56.815/RO, relator Ministro Antonio Saldanha Palheiro, Sexta Turma, julgado em 14/9/2021, DJe de 22/9/2021).

4. Agravo regimental improvido.

ACÓRDÃO

Vistos e relatados estes autos em que são partes as acima indicadas, acordam os Ministros da SEXTA TURMA do Superior Tribunal de Justiça, em Sessão Virtual de 18/06/2026 a 24/06/2026, por unanimidade, negar provimento ao recurso, nos termos do voto do Sr. Ministro Relator.

Os Srs. Ministros Rogerio Schietti Cruz, Carlos Pires Brandão, Nilsoni de Freitas (Desembargadora Convocada do TJDFT) e Og Fernandes votaram com o Sr. Ministro Relator.

Presidiu o julgamento o Sr. Ministro Carlos Pires Brandão.

Brasília, 24 de junho de 2026.

Ministro Sebastião Reis Júnior
Relator

Documento eletrônico VDA57993383 assinado eletronicamente nos termos do Art.1º §2º inciso III da Lei 11.419/2006
Signatário(a): SEBASTIÃO REIS JUNIOR Assinado em: 25/06/2026 13:16:05
Publicação no DJEN/CNJ de 29/06/2026. Código de Controle do Documento: e3daaa7b-fcb6-42ec-ad9e-63b43bc15d04

AgRg no RECURSO EM MANDADO DE SEGURANÇA Nº 60237 - RO (2019/0062211-0)

RELATOR	**:**	**MINISTRO SEBASTIÃO REIS JÚNIOR**
AGRAVANTE	:	MINISTERIO PUBLICO DO ESTADO DE RONDONIA
AGRAVADO	:	W I
ADVOGADOS	:	ROCHILMER MELLO DA ROCHA FILHO - RO000635 DAVI DE PAIVA COSTA TANGERINO - SP200793 MARCELA TRIGO DE SOUZA - RJ127614

EMENTA

AGRAVO REGIMENTAL EM RECURSO EM MANDADO DE SEGURANÇA. DECISÃO MANTIDA POR SEUS PRÓPRIOS FUNDAMENTOS. PENAL. PROCESSO PENAL. INTERCEPTAÇÃO DE DADOS. ASTREINTES. POSSIBILIDADE EM ABSTRATO. CRIPTOGRAFIA DE PONTA A PONTA. IMPOSSIBILIDADE FÁTICA, NO CASO CONCRETO, DE CUMPRIMENTO DA ORDEM JUDICIAL. PRECEDENTES.

1. Não há como abrigar agravo regimental que não logra desconstituir o fundamento da decisão atacada.

2. *É entendimento consolidado no Superior Tribunal de Justiça que a pendência de julgamento no STF de ação em que se discute a constitucionalidade de lei não enseja o sobrestamento dos recursos que tramitam no STJ, salvo determinação expressa da Suprema Corte.* [...] (REsp n. 1.393.421/SE, Ministro Herman Benjamin, Segunda Turma, DJe 24/10/2016) .

3. [...] *deve ser afastada a multa aplicada ante a impossibilidade fática decorrente de criptografia intransponível, sendo certo que os benefícios advindos da criptografia de ponta a ponta se sobrepõem às eventuais perdas pela impossibilidade de se coletar os dados das conversas dos usuários da tecnologia (RMS n. 60.531/RO, relator Ministro NEFI CORDEIRO, relator para acórdão Ministro RIBEIRO DANTAS, TERCEIRA SEÇÃO, julgado em 9/12/2020, DJe 17/12/2020)* [...] (AgRg no RMS n. 56.815/RO, relator Ministro Antonio Saldanha Palheiro, Sexta Turma, julgado em 14/9/2021, DJe de 22/9/2021).

4. Agravo regimental improvido.

RELATÓRIO

Trata-se de agravo regimental interposto pelo MINISTÉRIO PÚBLICO DO ESTADO DE RONDÔNIA contra decisão assim resumida (fl. 970):

> RECURSO EM MANDADO DE SEGURANÇA. INTERCEPTAÇÃO DE DADOS. ASTREINTES. POSSIBILIDADE EM ABSTRATO. CRIPTOGRAFIA DE PONTA A PONTA. IMPOSSIBILIDADE FÁTICA, NO CASO CONCRETO, DE CUMPRIMENTO DA ORDEM JUDICIAL. PRECEDENTES.
> Recurso ordinário em mandado de segurança provido.

Alega o agravante que *a agravada, mesmo antes da suposta impossibilidade técnica pelo uso da criptografia ponta a ponta (que começou a ser utilizada em 5 de abril de 2016), já criava embaraços à Justiça, no que diz respeito ao acesso às comunicações dos usuários, quando havia suspeita do envolvimento destes com a prática de crimes, condição que demonstra, claramente, estar a empresa tentando se sobrepor às determinações judiciais emanadas por autoridade competente, e descumprindo, deliberadamente, a legislação brasileira* (fl. 1.005).

Sustenta que *um aplicativo – sob a pecha da inviolabilidade da intimidade, seja um ambiente seguro àqueles que fazem do crime seu modo de vida e um espaço "sem lei", onde toda a logística criminosa é delineada – não pode se sobrepor à soberania nacional, ao interesse público, à segurança pública, ao combate à criminalidade, por meio das investigações criminais, e à autoridade das decisões judiciais, especialmente, quando devidamente fundamentadas e envolvendo delitos e esquemas deveras graves* (fl. 1.005).

Aduz ser *indevido o afastamento das astreintes, em virtude de suposta impossibilidade técnica da empresa de fornecer o conteúdo das mensagens trocadas entre os usuários do aplicativo, apontada pelo eminente relator, especialmente quando a questão ainda está em pleno debate no Pretório Excelso* (fl. 1.005).

Ao final, busca a reforma da *decisão monocrática, e, consequentemente, desprovido o Recurso Ordinário, no intuito de mantida [sic] as astreintes fixadas. Alternativamente, requer o sobrestamento do feito até o julgamento final da ADPF 403 e da ADI 5527* (fl. 1.006).

Em suas contrarrazões, W I argumenta que *o que se extrai das razões recursais é a mera irresignação do MPRO com o desfecho que lhe fora desfavorável, visto que o próprio reconhece que a jurisprudência desse e. Superior Tribunal de Justiça – das 5ª e 6ª Turmas e da 3ª Seção – é pacífica ao afastamento de astreintes em caso de comprovada impossibilidade técnica de atendimento da ordem em razão da criptografia de ponta-a-ponta* (fl. 1.017).

Diz não ter havido *qualquer alteração do contexto fático desde o julgamento dos referidos precedentes [ADPF 403 e ADI 5527] e, ainda, que as decisões supracitadas e os votos proferidos nas referidas ações constitucionais perante o e. STF caminham no mesmo sentido do entendimento firmado por esse e. STJ, certo é que a r. Decisão deve ser mantida por seus próprios fundamentos, de modo a garantir a segurança jurídica, a estabilidade das decisões e a uniformização da jurisprudência desse e. STJ (art. 926 do CPC)* – (fl. 1.020).

Argumenta que *a impossibilidade técnica de interceptação de mensagens diante da criptografia de ponta-a-ponta não é uma mera "alegação" e, muito menos, "unilateral", mas sim um fato público notório. Nesse sentido, o W trouxe prova pré-constituída robusta suficiente para suportar tal conclusão. Com efeito, a impossibilidade técnica de cumprimento foi corroborada por diferentes especialistas e relatórios independentes, inclusive por perito judicial* (fl. 1.020).

Sustenta que *o argumento do Parquet ignora o fato de que o W cumpriu as Ordens dentro de sua capacidade técnica, fornecendo os dados disponíveis sobre os terminais telefônicos indicados* (fl. 1.022).

Esclarece que o *W prontamente forneceu metadados não criptografados, quais sejam: (i) informações básicas dos usuários, (ii) os registros de acesso (IP Logs), (iii) históricos de mudança de número, (iv) informações sobre grupos e lista de membros de cada um desses grupos, e as agendas de contato dos 8 alvos usuários com contas válidas do WhatsApp, e explicou ser tecnologicamente incapaz de interceptar mensagens sob seu atual sistema de criptografia ponta-a-ponta* (fl. 1.023).

Alega que, *quando o cumprimento de uma determinação é tecnicamente inviável, a multa deixa de ser um meio de pressão e se transforma em uma punição, o que é incompatível com o regime legal das astreintes* (fl. 1.024).

Diz que, *se um provedor de aplicação, dentro dos limites técnicos de seu serviço retém o conteúdo de comunicações privadas, o "caput" do dispositivo impõe proteções à privacidade desses usuários, estabelecendo que "[o] conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7º"* (fl. 1.025).

Aduz que *o W não armazena como regra o conteúdo das mensagens em seus servidores. Portanto, a tese ministerial tenta utilizar uma norma voltada à disponibilização de dados existentes/armazenados para forçar a entrega de dados tecnicamente inacessíveis e inexistentes nos servidores da empresa* (fl. 1.025).

Sustenta que, mesmo que *se pudesse cogitar que o referido artigo traz deveres ao WhatsApp, o que se admite apenas para fins argumentativos, não há como interpretá-lo como criador de obrigação de inserir vulnerabilidades em seu sistema de criptografia ponta-a-ponta atual para se tornar tecnicamente capaz de cumprir ordens de interceptação. O artigo não traz em seu texto tal obrigação, que tampouco existe nas leis infraconstitucionais que regulam* (fl. 1.027).

É o relatório.

VOTO

A insurgência não merece acolhida.

A decisão impugnada deve ser mantida pelo que nela se contém, tendo em conta que o agravante não logrou desconstituir seu fundamento, motivo pelo qual o trago ao Colegiado para ser confirmado.

Com efeito, de acordo com o afirmado anteriormente, não há falar em ausência de fundamentação no acórdão recorrido, uma vez que o Tribunal *a quo* se pronunciou a respeito dos pontos acerca dos quais deveria ter se manifestado não se podendo atribuir-lhe os defeitos de omisso e contraditório, só porque dispôs contrariamente às pretensões do recorrente.

De outro lado, *é entendimento consolidado no Superior Tribunal de Justiça que* ***a pendência de julgamento no STF de ação em que se discute a constitucionalidade de lei não enseja o sobrestamento dos recursos que tramitam no STJ, salvo determinação expressa da Suprema Corte****. A propósito: AgRg no REsp 1.359.965/RJ, Rel. Ministro Ricardo Villas Bôas Cueva, Terceira Turma, DJe 31.5.2013* (REsp n. 1.393.421/SE, Ministro Herman Benjamin, Segunda Turma, DJe 24/10/2016 – grifo nosso).

Por conseguinte, não há falar em suspensão do presente feito até o julgamento da ADIn n. 5.527 e ADPF n. 403 pelo Supremo Tribunal Federal.

O entendimento consolidado no Superior Tribunal de Justiça é no sentido de ser possível a fixação de astreintes a terceiros não integrantes da relação processual, tais como o W I, F e G, mesmo no âmbito de ação penal.

Inclusive, ***a Terceira Seção desta Corte Superior****, no julgamento do REsp n. 1.568.445/PR (Relator para Acórdão Ministro Ribeiro Dantas, DJe de 20/8/2020) ,* ***reconheceu a possibilidade de aplicação de astreintes no processo penal; [...] a possibilidade de execução das astreintes, no juízo criminal, antes da prolação da sentença; [e] a não aplicação do art. 77, § 5º, do Código de Processo Civil*** (AgRg no REsp n. 1.975.411/SP, Ministro Jesuíno Rissato (Desembargador convocado do TJDFT), Quinta Turma, DJe 30/8/2022 – grifo nosso).

Em reforço:

> AGRAVO REGIMENTAL NO RECURSO EM MANDADO DE SEGURANÇA. POSSIBILIDADE DE BLOQUEIO DE ATIVOS FINANCEIROS VISANDO AO PAGAMENTO DA MULTA VIA BACENJUD. NÃO INCIDÊNCIA DA SÚMULA 410/STJ . AGRAVO DESPROVIDO.
>
> 1. Este Superior Tribunal de Justiça possui entendimento firmado no sentido da possibilidade de aplicação de astreintes a terceiros não integrantes da relação jurídico-processual, como W, F, G, ainda que em sede de processo penal. **Ademais, a Terceira Seção desta Corte Superior já fixou a orientação de que a recorrente - F Brasil - é parte legítima para, no Brasil, representar os interesses do F Inc. Precedentes.**
>
> 2. Na esteira da orientação jurisprudencial desta Corte, não incide a Súmula 410/STJ aos casos de bloqueio de numerário pelo sistema BacenJud para compelir o devedor a cumprir decisão judicial, em razão da natureza cautelar da medida. O referido enunciado atende às hipóteses de aplicação de multa pelo juízo cível em caso de descumprimento de antecipação da tutela em ação cível cujo objeto seja o cumprimento de obrigação de fazer ou não fazer.
>
> 3. Agravo desprovido.
>
> (AgRg no RMS n. 66.496/PE, Ministro Ribeiro Dantas, Quinta Turma, julgado em 14/12/2021, DJe 17/12/2021 – grifo nosso).

No mesmo sentido: AgRg no REsp n. 1.982.698/DF, Ministro Reynaldo Soares da Fonseca, Quinta Turma, DJe 18/3/2022; AgRg no AREsp n. 1.965.578/RS , Ministro Jesuíno Rissato (Desembargador Convocado do TJDFT), Quinta Turma, DJe 17/3/2022; e EDcl no AgRg no RMS n. 65.097/RS, Ministro Antonio Saldanha Palheiro, **Sexta Turma**, DJe 12/11/2021.

Não obstante isso, a Terceira Seção do Superior Tribunal de Justiça também firmou a compreensão de que a obrigação decorrente da fixação das astreintes pode ser afastada quando a empresa responsável pelo cumprimento da determinação judicial **comprovar a impossibilidade técnica de atender à ordem proferida pelo Juízo, notadamente quando envolver a utilização de criptografia ponta a ponta**, como no caso dos autos.

Confira-se:

RECURSO EM MANDADO DE SEGURANÇA. INTERCEPTAÇÃO DE DADOS. ASTREINTES. POSSIBILIDADE EM ABSTRATO. CRIPTOGRAFIA DE PONTA A PONTA. IMPOSSIBILIDADE FÁTICA, NO CASO CONCRETO, DE CUMPRIMENTO DA ORDEM JUDICIAL. RECURSO PROVIDO.

1. A possibilidade de aplicação, em abstrato, da multa cominatória foi reconhecida, por maioria, nesta Terceira Seção(REsp 1.568.445/PR, Rel. Ministro ROGERIO SCHIETTI CRUZ, Rel. p/ Acórdão Ministro RIBEIRO DANTAS, TERCEIRA SEÇÃO, julgado em 24/6/2020, DJe 20/8/2020).

2. No caso concreto, porém, há de se fazer uma distinção ou um distinguishing entre o precedente citado e a situação ora em análise. Diversamente do precedente colacionado, a questão posta nestes autos objeto de controvérsia é a alegação, pela empresa que descumpriu a ordem judicial, da impossibilidade técnica de obedecer à determinação do Juízo, haja vista o emprego da criptografia de ponta a ponta.

3. **Criptografia de ponta a ponta é a proteção dos dados nas duas extremidades do processo, tanto no polo do remetente quanto no outro polo do destinatário.**

Nela, há "dois tipos de chaves são usados para cada ponta da comunicação, uma chave pública e uma chave privada. As chaves públicas estão disponíveis para as ambas as partes e para qualquer outra pessoa, na verdade, porque todos compartilham suas chaves públicas antes da comunicação. Cada pessoa possui um par de chaves, que são complementares. [...] **O conteúdo só poderá ser descriptografado usando essa chave pública [...] junto à chave privada [...]**. **Essa chave privada é o único elemento que torna impossível para qualquer outro agente descriptografar a mensagem, já que ela não precisa ser compartilhada**." (COUTINHO, Mariana. O que é criptografia de ponta a ponta? Entenda o recurso de privacidade. Tectudo. Disponível em: br/noticias/2019/06/o-que-e-criptografia-de-ponta-a-ponta-entenda-o-recurso-de-priv >. Acesso em: 24 mar. 2020).

4. Não obstante a complexidade técnica, a resposta jurídica deve ser simples e direta: sim, é possível a aplicação da multa, inclusive nessa hipótese; ou, por outro lado, não, a realização do impossível, sob pena de sanção, não encontra guarida na ordem jurídica. Note-se que não há espaço hermenêutico para um meio termo.

5. Em determinado aspecto, a solução parece ser pela negativa: ad impossibilia nemo tenetur, ou seja, ninguém pode ser obrigado a fazer o impossível.

6. Porém, o Direito, como fruto do intelecto humano e indispensável ao convívio coletivo sadio e com capacidade prospectiva, nem sempre se contenta com o nexo natural das coisas. Ou seja, a responsabilidade jurídica nem sempre é derivada do raciocínio lógico. Por vezes, faz-se necessário o juízo de valor normativo, a exemplo da figura do garante no Código Penal, que, sem dar causa direta ao resultado típico, responde como se o tivesse (art. 13, §2º, "b", do CP).

7. Conforme relatado pelo em. Min. Edson Fachin, em seu voto, na ADPF 403, a Ciência corrobora a impossibilidade técnica de se interceptar dados criptografados de ponta a ponta. Realizadas audiências públicas para debate público sobre a matéria: "Um dos especialistas acadêmicos convocados para a audiência, o Professor Anderson Nascimento explicou em linhas gerais em que consiste a criptografia, afirmando que seu objetivo é a garantia da integridade, autenticidade e confidencialidade. Segundo ele, o W utiliza a criptografia de chave pública ou assimétrica, onde cada usuário possui duas chaves, uma para cifrar e outra para decifrar. **O objetivo de tais sistemas é criar um túnel criptográfico entre os usuários, sendo que as mensagens enviadas e recebidas passam por um servidor que tem a função de estabelecer protocolos de sinalização, descobrir os endereços IPs das partes, auxiliar na troca de chaves, dentre outros. O Professor esclareceu que não é possível a interceptação de mensagens criptografadas do W devido à adoção de criptografia forte pelo aplicativo.** Explica que esse tipo de criptografia utiliza o Protocolo Signal que, no entendimento da comunidade científica, não possui vulnerabilidade, ou seja, é um protocolo seguro, não podendo ser quebrado. Em relação às alternativas para a

interceptação, discorreu o seguinte. Sobre a possibilidade de espelhamento das conversas travadas no aplicativo para outro smartphone ou computador em face de um usuário específico, indicou que seria preciso, para tal intento, que fosse criado um ponto central de falha, o qual, por sua vez, poderia ser utilizado por parte não autorizadas. **Quanto à desabilitação da criptografia ponta a ponta de um ou mais usuários específicos, seria preciso modificar o protocolo criptográfico. Destacou, ainda, a existência de outros aplicativos de mensagens que não possuem representação no Brasil e que poderiam ser utilizados pelos usuários, inclusive com a possibilidade de facilmente criptografar as mensagens e, posteriormente, colar tal mensagem no W, para enviá-la a outro usuário, de modo que, mesmo que houvesse a interceptação da mensagem pelo W, seria impossível desencriptá-la**. Quanto aos demais instrumentos que podem auxiliar as investigações, aponta a importância da utilização dos metadados e da geolocalização, ressaltando a riqueza de dados a serem explorados pelas autoridades públicas".

8. Com forte apelo lógico, essa argumentação apresenta-se quase que irrefutável, não fossem as razões jurídicas relacionadas aos deveres e às obrigações derivadas do nexo causal normativo. Entretanto, é importante salientar que a tese contrária à imposição da multa também é prodigiosa em fundamentos jurídicos.

9. Inicio dizendo que, ao buscar mecanismos de proteção à liberdade de expressão e comunicação privada, por meio da criptografia de ponta a ponta, as empresas estão protegendo direito fundamental, reconhecido expressamente na Carta Magna. A propósito, confira-se interessante reflexão da em. Min. Relatora Rosa Weber, em seu voto na ADI 5527:

"Considerações sobre o direito às liberdades de expressão e de comunicação (art. 5º, IX, da CF). Integra o pleno exercício das liberdades de expressão e de comunicação a capacidade das pessoas de escolherem livremente as informações que pretendem compartilhar, as ideias que pretendem discutir, o estilo de linguagem empregado e o meio de comunicação. O conhecimento de que a comunicação é monitorada por terceiros interfere em todos esses elementos componentes da liberdade de informação: os cidadãos podem mudar o modo de se expressar ou até mesmo absterense de falar sobre certos assuntos, no que a doutrina designa por efeito inibitório (chilling effect) sobre a liberdade de expressão. Nesse sentido, 'A comunicação desinibida é também uma precondição do desenvolvimento pessoal autônomo. Seres humanos desenvolvem suas personalidades comunicando-se com os demais.' As consequências da ausência dessa precondição em uma sociedade vão desde a desconfiança em relação às instituições sociais, à apatia generalizada e a debilitação da vida intelectual, fazendo de um ambiente em que as atividades de comunicação ocorrem de modo inibido ou tímido, por si só, uma grave restrição à liberdade de expressão. Sob enfoque diverso, considerando que software é linguagem, e como tal, protegido pela liberdade de expressão, indaga-se se compelir o desenvolvimento compulsório de uma aplicação para se implementar a vulnerabilidade desejada, a determinação para a escrita compulsória de um programa de computador não configuraria, ela mesma, uma violação do direito à liberdade de expressão do desenvolvedor? De toda sorte, transformar o Brasil em um país avesso à liberdade de expressão não é o melhor caminho para combater os usos irresponsáveis das ferramentas de comunicação."

10. Ainda nos valendo do valoroso trabalho citado, tem-se a seguinte indagação: de que vale a liberdade de expressão sem o resguardo devido à intimidade privada? A propósito: "Se aos cidadãos não for assegurada uma esfera de intimidade privada, livre de ingerência externa, um lugar onde o pensamento independente e novo possa ser gestado com segurança, de que servirá a liberdade de expressão? O direito à privacidade tem como objeto, na quase poética expressão de Warren e Brandeis, 'a privacidade da vida privada'. O escopo da proteção são os assuntos pessoais, em relação aos quais não se vislumbra interesse público legítimo na sua revelação, e que o indivíduo prefere manter privados. 'É a invasão injustificada da privacidade individual que deve ser repreendida e, tanto quanto possível, prevenida'. Vale observar, ainda, que os maiores desafios contemporâneos à proteção da privacidade nada têm a ver com a imposição de restrições à liberdade de manifestação, enquanto relacionados, isto

sim, aos imperativos da segurança nacional e da eficiência do Estado, à proliferação de sistemas de vigilância e à emergência das mídias sociais, juntamente com a manipulação de dados pessoais em redes computacionais por inúmeros, e frequentemente desconhecidos, agentes públicos e privados. Nesse contexto, pertinente, ainda, a contribuição de Alan Westing à doutrina jurídica da privacidade no mundo contemporâneo, ao caracterizar a estrutura desse direito como controle sobre os usos da informação pessoal. Nesse sentido, a privacidade, afirma, 'é a pretensão de indivíduos, grupos ou instituições de determinarem para si quando, como e em que extensão a informação sobre eles será comunicada a outros'. Tal concepção do direito à privacidade está alinhada com o reconhecimento do seu papel social na própria preservação da personalidade e no desenvolvimento da autonomia individual." (Voto da em. Min. Relatora Rosa Weber na ADI 5527).

11. Complementando os fundamentos expostos até aqui, o em. Ministro Edson Fachin, na Ação de Arguição de Descumprimento de Preceito Fundamental n. 403, traz três balizas necessárias para o exame da questão:

"A precisa definição do objeto da arguição permite, de plano, identificar três premissas que emergem da manifestação dos amici curiae e que orientam a presente manifestação.

A primeira conclusão é a de que, como atestam os participantes da sociedade civil que participaram da audiência, a demanda pela criptografia é especialmente derivada da proteção que se espera ter da liberdade de expressão em uma sociedade democrática. A criptografia é, portanto, um meio de se assegurar a proteção de direitos que, em uma sociedade democrática, são essenciais para a vida pública.

A segunda é a de que todos os órgãos de Estado, assim como a sociedade civil, reconhecem que a criptografia protege os direitos dos usuários da internet, garantindo a privacidade de suas comunicações, e que, portanto, é do interesse do Estado brasileiro encorajar as empresas e as pessoas a utilizarem a criptografia e manter o ambiente digital com a maior segurança possível para os usuários. Essa premissa é evidenciada tanto pela manifestação dos peritos da Polícia Federal que participaram da audiência pública e quanto da Associação de Magistrados Brasileiros: a internet segura é direito de todos.

A terceira é a de que o desafio a esse modelo de proteção da privacidade emerge basicamente de casos como o dos autos, isto é, quando o acesso a mensagens protegidas por criptografia depende da autorização exclusiva do próprio usuário do serviço. Ele também se faz presente na proteção de criptografia que fica disponível para equipamento específicos, como um telefone celular smartphone, ou um computador portátil. Em ambos os casos a preocupação é justificada pelas dificuldades técnicas na apuração de crimes que gravemente violam direitos fundamentais, como, por exemplo, os casos de pornografia infantil e de condutas antidemocráticas, como manifestações xenófobas, racistas e intolerantes, que ameaçam o Estado de Direito. Os órgãos de segurança do Estado ficam, pois, privados de instrumento tido por indispensável – e que é reconhecido como plenamente legítimo em relação às chamadas telefônicas – na solução dessas violações."

12. A partir daí, o Ministro lança a questão: "a partir das premissas aqui indicadas é possível localizar a questão que se afigura chave para enfrentar o mérito desta arguição, qual seja, saber se o risco público representado pelo uso da criptografia justifica a restrição desse direito por meio da imposição de soluções de software, como, por exemplo, a proibição da criptografia ou a criação de canais excepcionais de acesso ou pela diminuição do nível de proteção"?

13. Antes de apresentar sua conclusão, Fachin ressalta a importância do direito à privacidade na internet, cita inclusive, Relatório Especial do Conselho de Direitos Humanos da ONU:

"Na linha inaugurada pela Assembleia Geral das Nações Unidas, o Conselho de Direitos Humanos aprovou o Relatório Especial sobre o Direito à Liberdade de Expressão na Era Digital. Nele, o Relator Especial David Kaye reconhece que o alcance do direito à privacidade na internet é instrumental para a garantia da liberdade de expressão. O receio da exposição que diminui a riqueza do ambiente plural da internet decorre tanto de ingerências governamentais, quanto da possibilidade de manipulação de dados, diminuindo a própria esfera de autonomia

e determinação, ou, nos termos da jurisprudência alemã, diminuindo o direito à autodeterminação informacional".

14. Convém ressaltar que, tanto o Ministro Edson Fachin quanto a Ministra Rosa Weber, ao fim de seus votos, chegam, ambos, à mesma conclusão: **o ordenamento jurídico brasileiro não autoriza, em detrimento da proteção gerada pela criptografia de ponta a ponta, em benefício da liberdade de expressão e do direito à intimidade, sejam os desenvolvedores da tecnologia multados por descumprirem ordem judicial incompatível com encriptação.**

15. Após pedido de vista do em. Min. Alexandre de Moraes, porém, ambas as ações constitucionais foram suspensas, aguardando-se, portanto, a matéria a posição definitiva dos demais membros da Corte.

16. Entretanto, não é mais possível esperar. Diante desse estado de coisas, esta Corte de justiça é posta a decidir sobre o tema: é ou não legal aplicar astreintes ao agente econômico que desenvolve e aplica a criptografia de ponta-a-ponta em seus serviços de comunicação. A vedação ao non liquet, prevista no art. 140 do CPC, nos impede de nos abster. É nosso dever julgar.

17. Por isso, embora chamando atenção para os graves aspectos que neste meu voto inicialmente levantei, curvo-me aos argumentos apresentados pelos em. Ministros Rosa Weber e Edson Fachin, os quais representam, ao menos até a presente altura, o pensamento do Supremo Tribunal Federal na matéria. E, assim, **endosso a ponderação de valores realizada pelos aludidos Ministros, que, em seus votos, concluíram que os benefícios advindos da criptografia de ponta a ponta se sobrepõem às eventuais perdas pela impossibilidade de se coletar os dados das conversas dos usuários da tecnologia.**

18. **Recurso ordinário provido, para afastar a multa aplicada ante a impossibilidade fática, no caso concreto, de cumprimento da ordem judicial, haja vista o emprego da criptografia de ponta-a-ponta**.

(RMS 60.531/RO, Rel. Ministro NEFI CORDEIRO, Rel. p/ Acórdão Ministro RIBEIRO DANTAS, **TERCEIRA SEÇÃO**, julgado em 9/12/2020, DJe 17/12/2020)

Vale destacar do referido julgado importante alerta feito pela Corte Superior de Justiça no sentido de que, *em tese, seria possível juridicamente impor a multa cominatória à empresa,* ***mesmo que se verifique a impossibilidade técnica da quebra de sigilo em razão da criptografia.*** *Isso porque,* ***o defeito do serviço (impossibilidade técnica) decorre da exploração da atividade normalmente desenvolvida pela recorrente. Ademais, os frutos (lucros) da oferta de criptografia de ponta a ponta, por se concentrarem na pessoa jurídica titular ou usuária da tecnologia em benefício de seus clientes, poderiam ser razões a obrigar aquela, juridicamente, a arcar com eventuais ônus decorrentes dessa exploração econômica*** (fl. 27 do voto vencedor – grifo nosso).

Ressaltou-se, ainda, a vedação ao comportamento contraditório, à medida em que, *quando* ***a própria pessoa que se coloca, com finalidade lucrativa, em uma situação de impossibilidade de identificar o conteúdo requisitado pela Justiça — conteúdo este, frise-se, de relevância para solução de crimes e cuja legislação autoriza expressamente a quebra —, seria razoável proibi-la de alegar obstáculo que ela mesma criara****. A* ***máxima venire contra factum proprium, aceita amplamente pelo ordenamento jurídico, pois decorrência do princípio da boa-fé, vedaria tal comportamento*** (fl. 27 op. cit – grifo nosso).

Entretanto, diante da ponderação de valores feita pela Ministra Rosa Weber e Ministro Edson Fachin no julgamento da ADPF n. 403, suspenso em razão de pedido de vista do Ministro Alexandre de Moraes, o Ministro Ribeiro Dantas, relator para o acórdão do citado RMS n. 60.531/RO, concluiu que ***os benefícios advindos da criptografia de ponta a ponta se sobrepõem às eventuais perdas pela impossibilidade de se coletar os dados das conversas dos usuários da tecnologia*** (fl. 38 op. cit – grifo nosso).

Por oportuno, diante da relevância da controvérsia em análise, **que envolve investigação de *organização criminosa voltada à prática do crime de tráfico de drogas, associação para o tráfico, lavagem de capitais e outros correlatos*** (fl. 301), anoto os seguintes trechos do referido voto condutor (fl. 28 op. cit – grifo nosso):

> [...]
> Note-se, portanto, que o engajamento na solução do conflito fático entre a criptografia de ponta a ponta, de um lado, e a obrigatoriedade de se cumprir as decisões judiciais – sob pena de multa, inclusive –, de outro, é algo que refoge à competência do Poder Judiciário. A este cabe apenas reconhecer se existe ou não a obrigação de fornecer os dados. Se essa obrigação existe, é possível aplicar multa para que seja cumprida a determinação.
> A Lei n. 13.709/18, Lei Geral de Proteção de Dados Pessoais (LGPD), traz balizas a serem observadas na proteção dos direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (art. 1º). Logo no art. 4º, ela diz ser possível a quebra do sigilo, nas investigações penais, afastando a regra geral do sigilo de dados [...].
> Portanto, percebe-se que o próprio legislador traça limites a serem observados na proteção ao sigilo de dados. Essa proteção não é absoluta. Vê-se uma espécie de ponderação, prima facie. Para melhor visualização, confira-se o art. 6 º:
> "Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
> I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
> II - **adequação**: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
> III - **necessidade**: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, **proporcionais e não excessivos em relação às finalidades** do tratamento de dados;" (Grifou-se).
>
> O em. Min. Marco Aurélio Bellizze, em voto no recurso especial n. 1784156/SP, de sua relatoria, traz interessantes e pertinentes considerações:
> [...]
> Com efeito, tão intuitiva quanto a percepção de que os provedores de conexão detêm as portas lógicas, é a compreensão de que os provedores de aplicações também as conhecem – na medida em que são elas que possibilitam a individualização da navegação e que o envio de dados entre dois pontos da comunicação depende intrinsecamente da localização virtual dos dispositivos conectados. Por consequência, é faticamente possível o arquivamento dessas informações, ainda que para tanto fosse necessária adaptação tecnológica dos provedores de aplicações, como bem enfatiza trecho do relatório acima." (Grifou-se).

Dessa forma, mais uma vez, convém dizer, **não se revela absoluto o direito ao sigilo de dados, nem tampouco à livre iniciativa. Além disso, a quebra de dados possui balizamento legal**. Nesse momento, **é importante trazer à reflexão dados fáticos que demonstram a importância de se limitar e restringir o sigilo conferido à troca de mensagens entre usuários de aplicativos de comunicação**. Em várias apurações criminais, os órgãos de repressão ao crime verificam a utilização de vias tecnológicas ocultas para a prática livre e desembaraçada de crimes graves.

[...]

Com efeito, **a ausência de controle das mensagens que trafegam no W poderia ensejar uma nova via livre para a prática de crimes.** É possível ainda especular que mais eficiente até mesmo que a chamada deep web, porque ninguém mais, além dos interlocutores diretos (emitente e destinatário), poderia flagrantear crimes praticados com o uso da criptografia de ponta-a-ponta. Nesse esteio, **revelar-se-ia impróprio afastar a responsabilidade da empresa responsável pela tecnologia em questão**.

Apesar de parecer uma solução audaciosa e inovadora, entendimento muito próximo a esse já foi adotado por esta Corte, por meio de sua 3ª Turma, no REsp 1784156/SP , acima mencionado. Além desse, há precedente no REsp 1.622.483/SP , no qual o em. Min. Paulo de Tarso Sanseverino **anotou que as providências necessárias à identificação (no nosso caso, à própria materialidade delitiva) do autor de ilícitos é ônus da empresa envolvida.**

Nestes termos, seria lícito concluir que as pessoas jurídicas responsáveis pelo desenvolvimento da tecnologia de criptografia de ponta a ponta, por terem se beneficiado com os lucros que a medida as leva a auferir e, indiretamente, terem possibilitado o anonimato a algumas possíveis práticas criminosas, deveriam arcar com os ônus da identificação e também da produção de provas, quando devidamente acionadas pelo Poder Judiciário. A solução quanto à dificuldade ou impossibilidade técnica não seria algo a ser enfrentado pelo Poder Judiciário, mas sim por quem criou voluntariamente essa situação.

Poder-se-ia trabalhar com situações extremas: **imagine-se, por exemplo, uma dupla de indivíduos que, por meio do W , planeja promover um atentado terrorista. Por esta via, fazem mapas, combinam data e modo de agir, bem como as vítimas potenciais**. Aproximando-se o dia planejado, um deles decide conversar com um terceiro para também se associar ao plano. Este terceiro, imediatamente recusa, sem buscar saber de detalhes como lugar, envolvidos etc. **O terceiro noticia o ocorrido às autoridades competentes, mas não ajuda em nada além de identificar um dos envolvidos, o número de celular deste, e informar que o planejamento do crime se dava pelo W . A autoridade policial, então, representa pela interceptação do W daquele que convidou o terceiro agente, antes de mais nada, para evitar várias mortes, danos severos à comunidade e outras consequências nefastas.**

Nessa situação hipotética, indaga-se, equiparar-se-ia a quebra do sigilo de dados à prática da tortura?

Porque a doutrina amplamente majoritária refuta a ponderação de direitos quando se tem de um dos lados a utilização da tortura. Uadi Lammêgo Bulos, nesse sentido, explica que, "salvo hipóteses específicas, como a da proibição à tortura, as liberdades públicas possuem limites, não servindo de substrato para a salvaguarda de práticas ilícitas" (BULOS, Uadi Lammêgo. Curso de Direito Constitucional, 11ª ed. São Paulo: Saraiva, 2018, p. 535). Assim, **indaga-se: obrigar o W a quebrar o sigilo de dados de alguns usuários, em determinados casos concretos, a partir de ordem judicial fundamentada para tanto, merece o mesmo tratamento jurídico que aquele dado à prática da tortura?**

Pois bem, todas essas considerações demonstrariam a **irrefutável e imperativa necessidade de se permitir a imposição de multa diária à empresa que descumpre ordem do Juízo criminal, mesmo que sob o manto argumentativo da impossibilidade fática. Do contrário, permitir-se-ia a criação pelo particular, que deve observância à ordem jurídica do país em que atua, de um ambiente virtual propício à proliferação da prática de crimes**

graves, como o tráfico de drogas em larga escala e outros delitos bárbaros, uma espécie de imunidade absoluta virtual, num ambiente impermeável ao direito e à soberania nacional.

De todo modo, esses argumentos não são mais convincentes do que aqueles apresentados em sentido contrário. **Em verdade, ambos são igualmente ponderáveis.**

[...]

Inicio dizendo que, **ao buscar mecanismos de proteção à liberdade de expressão e comunicação privada, por meio da criptografia de ponta a ponta, as empresas estão protegendo direito fundamental**, reconhecido expressamente na Carta Magna. A propósito, confira-se interessante reflexão da em. Min. Relatora Rosa Weber, em seu voto na ADI 5527 [...].

Ainda nos valendo do valoroso trabalho citado, tem-se a seguinte indagação: de que vale a liberdade de expressão sem o resguardo devido à intimidade privada?

[...]

Complementando os fundamentos expostos até aqui, o em. Ministro Edson Fachin, na Ação de Arguição de Descumprimento de Preceito Fundamental n. 403, traz três balizas necessárias para o exame da questão [...].

Convém ressaltar que, tanto o Ministro Edson Fachin quanto a Ministra Rosa Weber, ao fim de seus votos, chegam, ambos, à mesma conclusão: **o ordenamento jurídico brasileiro não autoriza, em detrimento da proteção gerada pela criptografia de ponta a ponta, em benefício da liberdade de expressão e do direito à intimidade, sejam os desenvolvedores da tecnologia multados por descumprirem ordem judicial incompatível com encriptação.**

[...]

Tal o contexto, sendo o caso dos autos hipótese análoga à do referido julgado, forçoso adotar a mesma solução, em que a impossibilidade fática oriunda da criptografia de ponta a ponta afasta a aplicação da multa pelo descumprimento da decisão judicial, sob pena de incorrer em insegurança jurídica.

Em reforço, confira-se:

PROCESSO PENAL. AGRAVO REGIMENTAL NO RECURSO EM MANDADO DE SEGURANÇA. INTERCEPTAÇÃO DE DADOS. DESCUMPRIMENTO DE ORDEM JUDICIAL. ASTREINTES. CABIMENTO. INVIOLABILIDADE DO SISTEMA DE CRIPTOGRAFIA DE PONTA A PONTA. IMPOSSIBILIDADE FÁTICA DE CUMPRIMENTO DA ORDEM JUDICIAL. AGRAVO DESPROVIDO.

1. A Terceira Seção do STJ, ao ponderar o conflito entre os direitos à privacidade, à inviolabilidade da comunicação privada, o direito à proteção e à segurança dos dados pessoais, firmou o entendimento de que:

a) não há determinação legal ou da Suprema Corte acerca da necessidade de suspensão do feito enquanto se aguarda o julgamento da ADPF n. 403 e ADI n. 5.527 pelo STF;

b) é possível a aplicação, em abstrato, de multa cominatória por descumprimento ou cumprimento a destempo de ordem emanada em processo judicial criminal; e

c) deve ser afastada a multa aplicada ante a impossibilidade fática decorrente de criptografia intransponível, sendo certo que os benefícios advindos da criptografia de ponta a ponta se sobrepõem às eventuais perdas pela impossibilidade de se coletar os dados das conversas dos usuários da tecnologia (RMS n. 60.531/RO, relator Ministro NEFI CORDEIRO, relator para acórdão Ministro RIBEIRO DANTAS, TERCEIRA SEÇÃO, julgado em 9/12/2020, DJe 17/12/2020).

2. Agravo regimental desprovido.

(AgRg no RMS n. 56.815/RO, relator Ministro Antonio Saldanha Palheiro, Sexta Turma, julgado em 14/9/2021, DJe de 22/9/2021 - grifo nosso)

Ante o exposto, **nego provimento** ao agravo regimental.

SUPERIOR TRIBUNAL DE JUSTIÇA

TERMO DE JULGAMENTO
SEXTA TURMA

AgRg no RMS 60.237 / RO

Número Registro: 2019/0062211-0

PROCESSO ELETRÔNICO

MATÉRIA CRIMINAL

Número de Origem:
00001467720188220501 00028216120188220000 1467720188220501 28216120188220000

Sessão Virtual de 18/06/2026 a 24/06/2026

SEGREDO DE JUSTIÇA

Relator do AgRg

Exmo. Sr. Ministro SEBASTIÃO REIS JÚNIOR

Presidente da Sessão

Exmo. Sr. Ministro CARLOS PIRES BRANDÃO

Secretário

Bel. ELISEU AUGUSTO NUNES DE SANTANA

AUTUAÇÃO

RECORRENTE : W I
ADVOGADOS : ROCHILMER MELLO DA ROCHA FILHO - RO000635
DAVI DE PAIVA COSTA TANGERINO - SP200793
MARCELA TRIGO DE SOUZA - RJ127614
RECORRIDO : MINISTERIO PUBLICO DO ESTADO DE RONDONIA

ASSUNTO : DIREITO PROCESSUAL PENAL

AGRAVO REGIMENTAL

AGRAVANTE : MINISTERIO PUBLICO DO ESTADO DE RONDONIA
AGRAVADO : W I
ADVOGADOS : ROCHILMER MELLO DA ROCHA FILHO - RO000635
DAVI DE PAIVA COSTA TANGERINO - SP200793
MARCELA TRIGO DE SOUZA - RJ127614

SUSTENTAÇÃO ORAL

Dr(a). MARCELA TRIGO DE SOUZA, pela parte: AGRAVADO: W I.

TERMO

A SEXTA TURMA do Superior Tribunal de Justiça, em Sessão Virtual de 18/06/2026 a 24/06/2026, por unanimidade, decidiu negar provimento ao recurso, nos termos do voto do Sr. Ministro Relator.

Os Srs. Ministros Rogerio Schietti Cruz, Carlos Pires Brandão, Nilsoni de Freitas (Desembargadora Convocada do TJDFT) e Og Fernandes votaram com o Sr. Ministro Relator. Presidiu o julgamento o Sr. Ministro Carlos Pires Brandão.

Brasília, 24 de junho de 2026