



SUPERIOR TRIBUNAL DE JUSTIÇA

RECURSO EM MANDADO DE SEGURANÇA Nº 60.531 - RO (2019/0099392-7)

RELATOR : MINISTRO NEFI CORDEIRO
R.P/ACÓRDÃO : MINISTRO RIBEIRO DANTAS
RECORRENTE : WHATSAPP INC
ADVOGADOS : ROCHILMER MELLO DA ROCHA FILHO - RO000635
ADRIELE PINHEIRO REIS AYRES DE BRITTO - DF023490
DAVI DE PAIVA COSTA TANGERINO - SP200793
MARCELO MONTALVAO MACHADO - DF034391
MARCELA TRIGO DE SOUZA - RJ127614
RECORRIDO : MINISTÉRIO PÚBLICO DO ESTADO DE RONDÔNIA

EMENTA

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:

<<https://www.techtudo.com.br/noticias/2019/06/o-que-e-criptografia-de-ponta-a-ponta-entenda-o-recurso-de-privacidade.ghtml>>. 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



SUPERIOR TRIBUNAL DE JUSTIÇA

coletivo sadio e com capacidade prospectiva, nem sempre se contenta com o nexos 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 WhatsApp 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 WhatsApp 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 WhatsApp, para enviá-la a outro usuário, de modo que, mesmo que houvesse a interceptação da mensagem pelo WhatsApp, seria impossível descriptá-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 nexos causal normativo. Entretanto, é importante salientar que a tese contrária à imposição da multa também é prodigiosa em fundamentos jurídicos.

9. Início 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



SUPERIOR TRIBUNAL DE JUSTIÇA

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 absterem-se 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



SUPERIOR TRIBUNAL DE JUSTIÇA

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,



SUPERIOR TRIBUNAL DE JUSTIÇA

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.



SUPERIOR TRIBUNAL DE JUSTIÇA

ACÓRDÃO

Vistos, relatados e discutidos os autos em que são partes as acima indicadas, acordam os Ministros da Terceira Seção do Superior Tribunal de Justiça, após o voto-vista divergente, quanto à fundamentação, do Sr. Ministro Ribeiro Dantas, dando provimento ao recurso ordinário 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, e os votos dos Srs. Ministros Antonio Saldanha Palheiro, Joel Ilan Paciornik, Laurita Vaz, Sebastião Reis Júnior (com ressalva) e Rogerio Schietti Cruz no mesmo sentido, por maioria, dar provimento ao recurso ordinário 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, nos termos do voto do Sr. Ministro Ribeiro Dantas, que lavrará o acórdão. Votou vencido o Sr. Ministro Nefi Cordeiro.

Votaram com o Sr. Ministro Ribeiro Dantas os Srs. Ministros Antonio Saldanha Palheiro, Joel Ilan Paciornik, Laurita Vaz, Sebastião Reis Júnior (com ressalva) e Rogerio Schietti Cruz.

Não participaram do julgamento os Srs. Ministros Felix Fischer e João Otávio de Noronha.

Presidiu o julgamento o Sr. Ministro Reynaldo Soares da Fonseca.

Brasília (DF), 09 de dezembro de 2020 (data do julgamento)

MINISTRO RIBEIRO DANTAS
Relator



SUPERIOR TRIBUNAL DE JUSTIÇA

RECURSO EM MANDADO DE SEGURANÇA Nº 60.531 - RO (2019/0099392-7)

RELATOR : MINISTRO NEFI CORDEIRO

RECORRENTE : WHATSAPP INC

ADVOGADOS : ROCHILMER MELLO DA ROCHA FILHO - RO000635

ADRIELE PINHEIRO REIS AYRES DE BRITTO - DF023490

DAVI DE PAIVA COSTA TANGERINO - SP200793

MARCELO MONTALVAO MACHADO - DF034391

MARCELA TRIGO DE SOUZA - RJ127614

RECORRIDO : MINISTÉRIO PÚBLICO DO ESTADO DE RONDÔNIA

RELATÓRIO

O EXMO. SR. MINISTRO NEFI CORDEIRO (Relator):

Trata-se de recurso ordinário em mandado de segurança interposto por *WhatsApp* inc. em face de acórdão proferido pelo Tribunal de Justiça de Rondônia assim ementado (fls. 401-419):

Mandando de segurança. Multa por descumprimento de ordem judicial. Quebra de sigilo telemático. Aplicativo de mensagens instantâneas. Whatsapp. Possibilidade. Incapacidade técnica não comprovada. Ilegalidade da multa. Proporcionalidade. Suspensão de exequibilidade.

1. O descumprimento de ordem judicial para realização de quebra de sigilo telemático resulta na possibilidade de imposição de multa diária em desfavor da empresa responsável pelos dados requeridos, não subsistindo o argumento de impossibilidade técnica quando existentes informações técnicas de que é possível o cumprimento da ordem judicial pela modalidade de desvio.

2. A proporcionalidade da multa pelo descumprimento das ordens judiciais deve ser aferida pela capacidade econômica do destinatário e, ainda, pela eventual resistência ao cumprimento da ordem, não sendo desproporcional quando demonstrada a recalcitrância e vultosos resultados financeiros do grupo econômico a que pertence.

3. Inexistindo atribuição de efeito suspensivo ou concessão de tutela antecipada nos autos de ações de controle concentrado junto ao STF, não há que se falar em suspensão do feito até que o Supremo profira decisão definitiva sobre a questão da criptografia.

Opostos embargos de declaração, foram rejeitados (fls. 442/452).

Em suas razões recursais, alega a defesa, preliminarmente, que os fundamentos trazidos no presente *mandamus* estão sob discussão perante o Supremo Tribunal Federal, no bojo da ADI 5.527 e da ADPF 403, de modo que as sanções ameaçadas devem ser suspensas até o deslinde da questão. No mérito, aduz, em síntese: (i) inexistência de qualquer obrigação no Marco Civil ou na Lei de Interceptações que imponha ao recorrente o dever de interceptar seus usuários, tampouco para que altere ou enfraqueça seu serviço em detrimento a todos os seus usuários; (ii) incapacidade técnica da empresa de interceptar as informações do seu sistema de criptografia ponta a ponta; (iii) ilegalidade da imposição ou ameaça de



SUPERIOR TRIBUNAL DE JUSTIÇA

imposição de multas pelos descumprimento de uma obrigação impossível, o que caracteriza violação dos arts. 536 e 537 do CPC; (iv) desproporcionalidade da multa imposta, que excede o limite legal imposto pelo art. 77, § 5º, do CPC, ultrapassando o valor de R\$ 90.000.000,00; e (v) impossibilidade de execução de *astreintes* via BACENJUD.

Requer, assim, a reforma do julgado para que sejam revogadas as determinações de aplicação de multa e responsabilidade criminal ou, substancialmente, reduzido seu valor, que não deve exceder o limite previsto no parágrafo 5º do art. 77 do CPC. Subsidiariamente, pugna pela suspensão das referidas ordens judiciais até que o Supremo Tribunal Federal julgue a ADPF n. 403 e a ADI n. 5.527.

Admitido o recurso (fl. 504), manifestou-se o Ministério Público Federal pelo desprovimento do *mandamus* (fls. 539-547).

É o relatório.



SUPERIOR TRIBUNAL DE JUSTIÇA

RECURSO EM MANDADO DE SEGURANÇA Nº 60.531 - RO (2019/0099392-7)

VOTO

O EXMO. SR. MINISTRO NEFI CORDEIRO (Relator):

Consta dos autos que o Juízo da Vara de Delitos de Tóxicos da Comarca de Porto Velho/RO determinou a quebra de sigilo de dados no âmbito do Inquérito n. 0002719-88.2018.8.22.0501, sob pena de aplicação de multa diária no importe de R\$ 300.000,00, limitada ao valor de R\$ 15.000.000,00 e de responsabilização criminal por descumprimento das ordens, nos termos do art. 2º, § 1º, da Lei 12.850/2013 (fls. 56-60).

Irresignada, a defesa impetrou mandado de segurança no Tribunal de origem, que foi, por maioria, parcialmente concedido, apenas para reduzir o valor da multa aplicada.

Destaco, para melhor deslinde da controvérsia, o seguinte trecho do voto condutor do acórdão, que versa sobre a legalidade da imposição de multa na hipótese (fls. 407-413):

3. Ilegalidade da Imposição de Multa e Desproporcionalidade

Diante da alegada impossibilidade de cumprimento das decisões judiciais ora questionadas, o impetrante afirma que a imposição de multas desafia o princípio da legalidade, pois partindo da premissa que o uso da criptografia é incentivado pelo Marco Civil da Internet, não seria ilegal o não cumprimento de decisão judicial que determina a quebra ou enfraquecimento desse mecanismo.

Para defender sua postura, o impetrante sustenta o descumprimento da ordem judicial sob o tripé da adequação, necessidade e proporcionalidade stricto sensu, apontando-os como subprincípios da proporcionalidade lato sensu. Todavia, avaliando os argumentos expostos para cada um desses subprincípios, não encontro justificativas suficientes para afastar a coercibilidade da decisão judicial.

Em primeiro ponto, compreendo que a medida é absolutamente adequada porquanto uma vez demonstrada a renitência de determinada instituição em cumprir as decisões judiciais, o ordenamento jurídico permite que sejam adotadas medidas coercitivas, inclusive de ofício em alguns casos, para que a ordem seja cumprida.

Já no ponto que defende o pressuposto da necessidade, o impetrante questiona se a medida ora pleiteada foi a ultima ratio da investigação ora desenvolvida, todavia, cumpre ressaltar que esta tarefa é de competência exclusiva da autoridade judicial, a quem compete analisar o pedido apresentado pela autoridade policial e, diante das peculiaridades de cada caso, deferir-se, ou não, o pedido de interceptação. Ao questionar a imprescindibilidade da medida deferida pelo Juízo impetrado o autor coloca em dúvida a seriedade com que são tratados temas tão sensíveis no Judiciário, porquanto não está se determinando algo simples, mas a mitigação temporária do direito ao sigilo de comunicação.

Ademais, não cabe aos destinatários da ordem judicial, questionar os métodos investigativos desenvolvidos pelas forças de segurança, sendo de rigor apenas que cumpra o que foi determinado, todavia, infelizmente criou-se no Brasil a cultura de descumprimento das ordens judiciais, o que semeia não apenas a insegurança jurídica, mas também o enfraquecimento das instituições.

Em todos os casos ilustrados pelo impetrante em suas razões de recurso, acerca da impossibilidade de cumprimento da decisão judicial, de fato demonstrou-se que não



SUPERIOR TRIBUNAL DE JUSTIÇA

era possível o cumprimento, como no caso de monitoramento prévio de determinados perfis pelo Facebook, contudo, no caso específico dos autos essa impossibilidade absoluta está, pelo menos, duvidosa pelo que se observa do debate técnico -jurídico realizado no âmbito da ADPF 403.

Destaco ainda que a livre iniciativa e livre concorrência não possuem caráter irrestrito, encontrando limites naquilo que o Estado entende como valorativamente superior, como é o caso da segurança pública, inexistindo ainda qualquer disposição constitucional assegurando que a criptografia é um direito fundamental de mais de 120 milhões de "usuários do WhatsApp".

4. Da Suspensão da Ordem de Bloqueio até Julgamento no STF

Neste pedido, o impetrante pede a suspensão das ordens judiciais ora questionadas até que o Supremo Tribunal Federal decida sobre sua Constitucionalidade, algo que pode ocorrer nos autos da ADPF 403 e ADI 5.527, ambos em trâmite naquela Corte. Em que pese este pedido, ressalto que nem na ADI nem na ADPF foi concedida tutela antecipada para suspender o trâmite das ações naquela Corte ou nos demais Tribunais do Brasil.

Sobre esta temática, ressalto que o entendimento do STJ sobre a suspensão já está sedimentado, conforme ementa a seguir:

[...]

Portanto, inexistindo tutela concedendo efeitos suspensivos, não vejo motivos para aguardar a resolução das demandas perante o STF, sobretudo em obediência aos princípios da celeridade processual e razoável duração do processo.

5. Desproporcionalidade do Valor das Multas

Quanto ao ponto que trata da proporcionalidade dos valores das multas aplicadas, vejo que não há irregularidade quanto ao valor arbitrado pela autoridade apontada como coatora, uma vez que, por analogia e como parâmetro seguro, o artigo 12 inciso II do Marco Civil que regula internet estabelece que a multa pode ser fixada até em 10% do faturamento do grupo econômico e não há dúvidas que este grupo ao qual pertence o WhatsApp e é liderado pelo Facebook, possui faturamento compatível com a multa aplicada, porquanto em simples consulta em site de buscas, vários são os resultados que indicam que o Facebook registrou lucro líquido de US\$ 15,9 bilhões em 2017 (<https://economia.uol.com.br/noticias/efe/2018/01/31/facebook-registra-lucro-liquido-de-us-159-bilhoes-em-2017-alta-de-56.html>).

Nesse ponto, o impetrante não trouxe aos autos provas de que o valor arbitrado pelo Juízo de primeiro grau é abusivo, não tendo esclarecido qual é o faturamento para que este colegiado verifique se o valor supera, ou não, o limite da lei. Logo, se a parte não trouxe essas provas nos autos, e quem alega que tem que provar, presumo que esse valor não atinge o limite da lei.

Observo ainda que as ordens expedidas pelo Juízo de primeiro grau foram em continuidade ou complementação da primeira ordem, devendo-se limitar o bloqueio ao teto inicialmente estabelecido de R\$ 15.000.000,00 (quinze milhões), uma vez que não pode o destinatário da ordem ser penalizado pela apresentação incompleta do rol de telefones a serem interceptados.

Com relação ao parágrafo quinto do art. 77 do CPC, argumento trazido aos autos posteriormente em memoriais pelo impetrante, entendo que não se aplica ao caso pois o referido trecho da Lei possui a seguinte redação: "Quando o valor da causa for irrisório ou inestimável a multa poderá ser fixada em até 10 vezes o salário -mínimo". Conforme já destacado, não estamos a tratar de valor irrisório, tampouco de valor inestimável, porquanto existe um valor fixo e certo que a decisão de primeiro grau



SUPERIOR TRIBUNAL DE JUSTIÇA

aponta, então não se aplica o dispositivo mencionado ao caso. Ademais, o STJ já analisou argumento semelhante, indicando que: "Não há que ser falar em afronta ao princípio da proporcionalidade quando demonstradas nos autos a recalcitrância da empresa em cumprir a determinação judicial e o seu poder econômico, conhecida que é como "a maior rede social virtual em todo o mundo", (fonte: <https://pt.wikipedia.org/wiki/Facebook>)" (AgRg no RMS 54.887/RS e AgRg no RMS 56.706/RS).

Ademais é nítido que mesmo com valores que considera exorbitantes, o grupo econômico do impetrante nada faz para cooperar e atender integralmente as determinações judiciais, mantendo sua recalcitrância não apenas perante Juízos deste Tribunal, mas por todo o país, sendo necessária a manutenção do patamar de multa já fixado só pena de ser premiada a desobediência.

6. Da Autoexecutoriedade das Multas Em sua manifestação, a Procuradoria de Justiça manifestou-se pela parcial concessão da ordem para afastar a autoexecutoriedade das multas aplicadas pelo Juízo de primeiro grau, visando evitar o bloqueio de ativos do impetrante e sua controladora. Este colegiado já teve a oportunidade de debater sobre este tema no MS 0004689-11.2017.8.22.0000, cuja ementa transcrevo adiante:

[...]

Compreende-se, portanto, que no decorrer de procedimento de matéria criminal ser estabelecida relação de natureza processual civil, logo, embora o CPP não tenha previsão de imposição de multa cominatória (astreintes), pode-se valer do Código de Processo Civil, que em seu art. 77, IV do CPC/2015 prevê que "são deveres das partes, de seus procuradores e de todos aqueles que de qualquer forma participem do processo: IV - cumprir com exatidão as decisões jurisdicionais, de natureza provisória ou final, e não criar embaraços à sua efetivação".

Este mesmo Código permite ao magistrado, de ofício, fixar multa (art. 77, §2º, 536 e 537 do CPC/2015), o que deixa evidente que a intenção do legislador ao dispor destes métodos foi dotar o Juiz de mecanismos coercitivos para cumprimento de suas decisões, sob pena de total ineficácia das medidas determinadas.

Cito julgado do STJ:

[...]

Portanto, o descumprimento da decisão importa na constituição de um título executivo judicial o que permite a adoção de medidas para seu imediato cumprimento nos próprios autos, pois esta multa possui a natureza de astreintes, permitindo a execução de imediato, inclusive por meio do BACENJUD.

O STJ já decidiu sobre o tema no AgRg no RMS 55.050/SP (Rel.

Ministro Reynaldo Soares da Fonseca, Quinta Turma, julgado em 03/10/2017, DJe 11/10/2017) que:

[...]

Logo, sendo o impetrante destinatário da ordem judicial reiteradamente descumprida, em total violação à Soberania do Estado Brasileiro e ainda com evidente desrespeito ao ordenamento Jurídico Pátrio, pode o juiz fixar medidas pecuniárias de caráter coercitivo e, no bojo dos próprios autos, determinar a execução das medidas, sendo desnecessária a formalização de autos de execução fiscal.

Por estes fundamentos, denego a segurança pretendida pelo impetrante.

Não obstante as diversas teses trazidas no presente *mandamus*, atendo-me à análise



SUPERIOR TRIBUNAL DE JUSTIÇA

da questão específica referente à legalidade da imposição de multa diante do descumprimento de ordem judicial que determinou a quebra de sigilo e interceptação telemática de contas do *Whatsapp* inc.

Cumpra-se destacar, de início, que não se desconhece os precedentes desta Corte no sentido do cabimento da imposição de multa por descumprimento, ou cumprimento a destempo, de ordem judicial, apesar de não haver disposição expressa a respeito no Código de Processo Penal, aplicando-se, por analogia, o disposto no Código de Processo Civil. Nesse sentido: Inq. 784/DF, Relatora Ministra LAURITA VAZ, CORTE ESPECIAL, DJe 28/8/2013; Agrg no RMS 55.050/SP, Relator Ministro REYNALDO SOARES DA FONSECA, QUINTA TURMA, DJe 11/10/2017; RMS 54.444/RJ, DJe 13/10/2017, Relatora MARIA THEREZA DE ASSIS MOURA.

Ressalto, no entanto, que, por ocasião do julgamento do RMS 54.444/RJ pela Sexta Turma, em 12/9/2017, em hipótese semelhante a que ora se analisa, manifestei posição divergente, em relação à qual proponho nova discussão.

Embora compartilhe da preocupação em seguir os precedentes da Corte, prestigiando, assim, a segurança jurídica, entendo que o tema merece novo debate, porque não vejo como discutirmos em processo penal questão de caracterização de descumprimento de ordem judicial, de proporcionalidade ou de execução provisória de *astreintes*, quando pretende o juiz criminal, a pretexto de analogia, não seguir rito, mas impor penas.

Conforme relatado, as decisões que ora se pretende desconstituir fixaram o pagamento de multa diária, em razão de descumprimento de ordem judicial encartada em procedimento de investigação criminal. Trata-se, portanto, de uma medida coercitiva típica de direito processual civil, de caráter cominatório, deferida na fase inquisitorial.

Com efeito, o Código de Processo Penal, em seu art 3º, admite a interpretação extensiva e a autointegração. Assim, somente sendo omissa a legislação processual penal, é possível a aplicação analógica do Código de Processo Civil (AgRg no HC 256.818/ES, Rel. Ministro MARCO AURÉLIO BELLIZZE, QUINTA TURMA, julgado em 05/02/2013, DJe 15/02/2013; EREsp 287.390/RR, Rel. Ministro ANTÔNIO DE PÁDUA RIBEIRO, CORTE ESPECIAL, julgado em 18/08/2004, DJ 11/10/2004), vedada, contudo, a analogia de norma sancionadora.

Usa-se, por analogia, o art. 3º do CPP, mas o fundamento da medida tem caráter cominatório, estando atrelado ao atraso ou descumprimento de ordem judicial, tratando-se, pois, de *astreintes*, ou seja, multa pecuniária coercitiva típica do âmbito do direito processual civil. Trata-se de multa, portanto, penalidade de natureza patrimonial, somente podendo ser imposta na seara penal mediante prévia cominação legal, não cabendo o uso da analogia *in malam partem*.

Assim, não é possível, a pretexto de cumprimento de ordem judicial, aplicar punição



SUPERIOR TRIBUNAL DE JUSTIÇA

por analogia, sob pena de infligir em um procedimento criminal *astreintes* do Código de Processo Civil.

Desse modo, a imposição de sanção processual por descumprimento de decisão judicial, pelo acórdão recorrido, constitui flagrante ilegalidade, haja vista a ausência de previsão expressa no Código de Processo Penal.

Destaca-se, por oportuno, o seguinte trecho da decisão monocrática proferida no RMS 35.906/MS, da relatoria do Ministro Gilmar Mendes, a respeito da impossibilidade de aplicação de multa cominatória em hipótese de incapacidade ou demora no cumprimento da ordem judicial:

Advirto, porém, que, independentemente dos valores em discussão e dos critérios utilizados para sua fixação, há palpável incompatibilidade entre o instituto processual utilizado e seu manejo pela autoridade coatora.

A multa cominatória, tal como prevista na legislação processual civil, tem como objetivo coagir o devedor ao cumprimento da obrigação mediante a imposição de penalidade pecuniária.

Tal sanção não se autonomiza da providência judicial que visa a efetivar, mas seguirá necessariamente a sorte processual do direito tutelado. Essa incompatibilidade foi muito bem tratada na manifestação da Procuradoria Geral da República, que peço vênia para transcrever:

“Nota-se que, não mais se discutindo a impossibilidade do cumprimento da ordem, as *astreintes* foram ainda assim mantidas, sob o fundamento de que puniriam o apontado atraso na explicação sobre o motivo do não atendimento da ordem. Isso, porém, efetivamente, desnatura a multa cominatória, que se diferencia da aplicação da sanção pelo descumprimento, sem justificativa, de ordem judicial. A multa cominatória visa a compelir quem está sujeito a uma obrigação a cumpri-la. Evidenciado que a obrigação era impossível de ser satisfeita, a multa perde sentido, não podendo se convolar em multa-sanção por não se ter respondido com maior antecedência que a ordem recebida pela empresa era inviável. Se houve na demora assinalada na origem algum comportamento passível de punição, as *astreintes* não se prestam para punir esse comportamento” (fl. 429).

Dessa forma, não se mostra compatível com o nosso ordenamento a aplicação de multa cominatória apenas com o intuito de punir o recorrente pela demora na apresentação de justificativa sobre a impossibilidade de cumprimento da ordem judicial, o que configura o caráter teratológico da decisão a dar ensejo ao provimento do recurso.

Nesse sentido, confira-se o seguinte julgado:

“DIREITO PROCESSUAL CIVIL. AGRAVO INTERNO EM EMBARGOS DECLARATÓRIOS EM AGRAVOS REGIMENTAIS EM RECURSO ORDINÁRIO EM MANDADO DE SEGURANÇA. ATO JUDICIAL. TERATOLOGIA. FUNDAMENTAÇÃO.

1. O mandado de segurança contra ato judicial só tem lugar quando (i) não cabível recurso ou correição (contrário sensu da súm. 267/STF); e (ii) demonstrada a inequívoca teratologia da decisão impugnada (MS 32.772 AgR, Rel. Min. Rosa Weber). 2. Irrecorribilidade do acórdão impugnado reconhecida no julgamento do AI 642.705/STF. Não devidamente fundamentada a ausência de teratologia assentada no acórdão recorrido, notadamente tendo em conta os argumentos deduzidos na peça de interposição do recurso e o valor da multa aplicada. 3. Agravo a que se nega



SUPERIOR TRIBUNAL DE JUSTIÇA

provimento”. (RMS 26769 AgR-AgR-AgR-ED-AgR, Rel. Min. ROBERTO BARROSO, Primeira Turma, DJe 16.11.2017)

Ante o exposto, dou provimento ao recurso ordinário para conceder a segurança pleiteada, declarando a ilegalidade da multa imposta ao impetrante no Recurso Eleitoral 117-92.2013.6.12.0001 (RMS 35.906/MS, Rel. Min. Gilmar Mendes; DJE nº 247, divulgado em 20/11/2018).

É de se aplicar à hipótese o mesmo entendimento desta Corte a respeito da multa por litigância de má-fé, que igualmente configura sanção processual, ou seja, possui natureza de pena, somente podendo ser imposta na seara penal mediante prévia cominação legal, pois vedado em nosso ordenamento o uso da analogia *in malam partem*. A esse respeito:

PROCESSUAL PENAL E PROCESSUAL CIVIL. AGRAVO REGIMENTAL NO RECURSO ORDINÁRIO EM MANDADO DE SEGURANÇA. 1. CABIMENTO DO MANDADO DE SEGURANÇA CONTRA ATO JUDICIAL PASSÍVEL DE RECURSO COM EFEITO SUSPENSIVO: EXCEPCIONALIDADE DIANTE DE MANIFESTA ILEGALIDADE OU TERATOLOGIA. 2. IMPOSIÇÃO DE MULTA POR LITIGÂNCIA DE MÁ-FÉ (ART. 18 DO CPC/1973) NA SEARA PENAL. ILEGALIDADE. ANALOGIA IN MALAM PARTEM.

[...]

3. Pelo menos desde 2009, quando foi levada a julgamento a APn 477/PB, de relatoria da Ministra ELIANA CALMON, a Corte Especial deste Tribunal Superior vem afirmando a impossibilidade de imposição de multa por litigância de má-fé na seara penal, por considerar que sua aplicação constitui analogia in malam partem, sem contar que a imposição de tal multa não prevista expressamente no Processo Penal implicaria prejuízo para o réu na medida em que inibiria a atuação do defensor. Precedentes.

4. É manifestamente ilegal o ato judicial que, em maio/2012, anos após a pacificação do tema pela jurisprudência desta Corte, insiste em impor multa por litigância de má-fé (art. 18, CPC/1973) ao réu, na seara penal, impõe multa por litigância de má-fé, quando tal sanção não encontra amparo na legislação penal e não admite aplicação analógica por caracterizar analogia in malam partem.

5. Agravo regimental do impetrante provido, para dar provimento ao recurso ordinário em mandado de segurança, e, por consequência, conceder a segurança pleiteada, determinando seja excluída a multa por litigância de má-fé imposta no ato judicial apontado como coator. (AgRg no RMS 44.129/PE, Rel. Ministro REYNALDO SOARES DA FONSECA, QUINTA TURMA, julgado em 05/05/2016, DJe 13/05/2016.)

PENAL E PROCESSO PENAL. EMBARGOS DE DECLARAÇÃO NOS ACLARATÓRIOS NOS EMBARGOS DE DECLARAÇÃO NO AGRAVO REGIMENTAL NO AGRAVO EM RECURSO ESPECIAL. RECURSO INFUNDADO. NÍTIDO CARÁTER PROTELATÓRIO. DESVIRTUAMENTO DO CÂNONE DA AMPLA DEFESA. ABUSO DE DIREITO. DETERMINAÇÃO DE BAIXA DOS AUTOS À ORIGEM PARA IMEDIATA EXECUÇÃO DA SENTENÇA CONDENATÓRIA. EMBARGOS NÃO CONHECIDOS.



SUPERIOR TRIBUNAL DE JUSTIÇA

1. A recorribilidade vazia, infundada, como in casu, tão somente com nítido intuito protelatório, configura abuso do direito de recorrer e não é admissível em nosso ordenamento jurídico, notadamente em respeito aos postulados da lealdade e boa fé processual, além de se afigurar desvirtuamento do próprio cânone da ampla defesa.
2. Não obstante na esfera penal não ser viável a fixação de multa por litigância de má-fé, é perfeitamente possível, antes mesmo do trânsito em julgado da condenação, a baixa dos autos, independentemente da publicação do acórdão, para que inicie o cumprimento da pena imposta.
3. Embargos de declaração não conhecidos, com a determinação de imediata baixa dos autos à Vara de origem, para fins de execução da sentença condenatória, independentemente da publicação deste acórdão e da eventual interposição de outro recurso, devendo a Coordenadoria da Sexta Turma certificar o trânsito em julgado. (EInf nos EDcl nos EDcl no AgRg no AREsp 408.256/MG, Rel. Ministra MARIA THEREZA DE ASSIS MOURA, SEXTA TURMA, julgado em 04/02/2014, DJe 18/02/2014.)

Vale também ressaltar precedente da Suprema Corte onde ressaltada a impossibilidade de violação ao princípio da legalidade para imposição de pena:

“AÇÃO DIRETA DE INCONSTITUCIONALIDADE. ARTIGOS 5º, 8º, 9º, 10, 13, § 1º, E 14 DA PORTARIA Nº 113, DE 25.09.97, DO IBAMA. Normas por meio das quais a autarquia, sem lei que o autorizasse, instituiu taxa para registro de pessoas físicas e jurídicas no Cadastro Técnico Federal de Atividades Potencialmente Poluidoras ou Utilizadoras de Recursos Ambientais, e estabeleceu sanções para a hipótese de inobservância de requisitos impostos aos contribuintes, com ofensa ao princípio da legalidade estrita que disciplina, não apenas o direito de exigir tributo, mas também o direito de punir. Plausibilidade dos fundamentos do pedido, aliada à conveniência de pronta suspensão da eficácia dos dispositivos impugnados. Cautelar deferida.”

(ADI 1823 MC, Relator(a): Min. ILMAR GALVÃO, Tribunal Pleno, julgado em 30/04/1998, DJ 16-10-1998 PP-00006 EMENT VOL-01927-01 PP-00053 RTJ VOL-00179-03 PP-01004)

Realmente, não se pode punir com fundamento em analogia, mesmo com bons propósitos. Pena não se sustenta sem lei estrita e prévia e essa situação não se verifica no estatuto processual penal, não podendo ser aplicado o regramento civil sem previsão expressa.

Irrelevante é se a pena encontra-se direcionada a parte processual ou terceiro: pena não se aplica por analogia.

Deste modo, ilegal é a imposição de multa em processo penal sem fundamento legal, ficando prejudicados as demais teses do mandamus.

Ante o exposto, voto por dar provimento ao recurso em mandado de segurança a fim de deconstituir a decisão de primeiro grau que determinou a aplicação ao recorrente de multa por descumprimento de determinação judicial.



SUPERIOR TRIBUNAL DE JUSTIÇA

CERTIDÃO DE JULGAMENTO TERCEIRA SEÇÃO

Número Registro: 2019/0099392-7 **PROCESSO ELETRÔNICO** **RMS 60.531 / RO**
MATÉRIA CRIMINAL

Números Origem: 00027198820188220501 00029229820188220000 27198820188220501
29229820188220000

PAUTA: 11/03/2020

JULGADO: 11/03/2020
SEGREDO DE JUSTIÇA

Relator

Exmo. Sr. Ministro **NEFI CORDEIRO**

Presidente da Sessão

Exmo. Sr. Ministro REYNALDO SOARES DA FONSECA

Subprocuradora-Geral da República

Exma. Sra. Dra. ELA WIECKO VOLKMER DE CASTILHO

Secretário

Bel. GILBERTO FERREIRA COSTA

AUTUAÇÃO

RECORRENTE : WHATSAPP INC
ADVOGADOS : ROCHILMER MELLO DA ROCHA FILHO - RO000635
ADRIELE PINHEIRO REIS AYRES DE BRITTO - DF023490
DAVI DE PAIVA COSTA TANGERINO - SP200793
MARCELO MONTALVAO MACHADO - DF034391
MARCELA TRIGO DE SOUZA - RJ127614
RECORRIDO : MINISTÉRIO PÚBLICO DO ESTADO DE RONDÔNIA

ASSUNTO: DIREITO PROCESSUAL PENAL

SUSTENTAÇÃO ORAL

O Dr. Davi de Paiva Costa Tangerino sustentou oralmente pela parte recorrente: Whatsapp Inc.

CERTIDÃO

Certifico que a egrégia TERCEIRA SEÇÃO, ao apreciar o processo em epígrafe na sessão realizada nesta data, proferiu a seguinte decisão:

Após o voto do Sr. Ministro Relator, dando provimento ao recurso para desconstituir a decisão de primeiro grau que determinou a aplicação ao recorrente de multa por descumprimento de ordem judicial, pediu vista o Sr. Ministro Ribeiro Dantas.

Aguardam os Srs. Ministros Antonio Saldanha Palheiro, Joel Ilan Paciornik, Leopoldo de Arruda Raposo (Desembargador convocado do TJ/PE), Laurita Vaz, Jorge Mussi, Sebastião Reis Júnior e Rogerio Schietti Cruz.

Presidiu o julgamento o Sr. Ministro Reynaldo Soares da Fonseca.



SUPERIOR TRIBUNAL DE JUSTIÇA

CERTIDÃO DE JULGAMENTO TERCEIRA SEÇÃO

Número Registro: 2019/0099392-7 **PROCESSO ELETRÔNICO** **RMS 60.531 / RO**
MATÉRIA CRIMINAL

Números Origem: 00027198820188220501 00029229820188220000 27198820188220501
29229820188220000

PAUTA: 11/03/2020

JULGADO: 12/08/2020
SEGREDO DE JUSTIÇA

Relator

Exmo. Sr. Ministro **NEFI CORDEIRO**

Presidente da Sessão

Exmo. Sr. Ministro REYNALDO SOARES DA FONSECA

Subprocuradora-Geral da República

Exma. Sra. Dra. JULIETA E. FAJARDO C. DE ALBUQUERQUE

Secretário

Bel. GILBERTO FERREIRA COSTA

AUTUAÇÃO

RECORRENTE : WHATSAPP INC
ADVOGADOS : ROCHILMER MELLO DA ROCHA FILHO - RO000635
 ADRIELE PINHEIRO REIS AYRES DE BRITTO - DF023490
 DAVI DE PAIVA COSTA TANGERINO - SP200793
 MARCELO MONTALVAO MACHADO - DF034391
 MARCELA TRIGO DE SOUZA - RJ127614
RECORRIDO : MINISTÉRIO PÚBLICO DO ESTADO DE RONDÔNIA

ASSUNTO: DIREITO PROCESSUAL PENAL

CERTIDÃO

Certifico que a egrégia TERCEIRA SEÇÃO, ao apreciar o processo em epígrafe na sessão realizada nesta data, proferiu a seguinte decisão:

A Terceira Seção, por unanimidade, acolheu a questão de ordem suscitada pelo Sr. Ministro Ribeiro Dantas, para suspender o prazo do pedido de vista por até 90 dias. Presidiu o julgamento o Sr. Ministro Reynaldo Soares da Fonseca.



SUPERIOR TRIBUNAL DE JUSTIÇA

RECURSO EM MANDADO DE SEGURANÇA Nº 60.531 - RO (2019/0099392-7)

RELATOR : **MINISTRO NEFI CORDEIRO**
RECORRENTE : WHATSAPP INC
ADVOGADOS : ROCHILMER MELLO DA ROCHA FILHO - RO000635
ADRIELE PINHEIRO REIS AYRES DE BRITTO - DF023490
DAVI DE PAIVA COSTA TANGERINO - SP200793
MARCELO MONTALVAO MACHADO - DF034391
MARCELA TRIGO DE SOUZA - RJ127614
RECORRIDO : MINISTÉRIO PÚBLICO DO ESTADO DE RONDÔNIA

EMENTA

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:

<<https://www.techtudo.com.br/noticias/2019/06/o-que-e-criptografia-de-ponta-a-ponta-entenda-o-recurso-de-privacidade.ghtml>>. 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



SUPERIOR TRIBUNAL DE JUSTIÇA

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 WhatsApp 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 WhatsApp 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 WhatsApp, para enviá-la a outro usuário, de modo que, mesmo que houvesse a interceptação da mensagem pelo WhatsApp, seria impossível descriptá-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. Início 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



SUPERIOR TRIBUNAL DE JUSTIÇA

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 absterem-se 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 pré-condição do desenvolvimento pessoal autônomo. Seres humanos desenvolvem suas personalidades comunicando-se com os demais.' As consequências da ausência dessa pré-condição 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 reprimida 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



SUPERIOR TRIBUNAL DE JUSTIÇA

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



SUPERIOR TRIBUNAL DE JUSTIÇA

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.

VOTO-VENCEDOR

MINISTRO RIBEIRO DANTAS:

Trata-se de recurso em mandado de segurança interposto pelo **W. I.** contra acórdão do Tribunal de Justiça de Rondônia, que concedeu parcialmente a segurança para, aplicando o voto médio, reduzir de metade o valor da multa diária e também o *quantum* máximo acumulável.

Os embargos de declaração foram rejeitados.

Preliminarmente, o recorrente requer a suspensão das ordens e ameaças de sanções até que o Supremo Tribunal Federal decida sobre a constitucionalidade do sistema de criptografia de ponta a ponta, debatido na ADPF 403.

No mérito, sustenta necessidade de observância ao direito de o Whatsapp conduzir seus negócios sem a interferência do Estado, salvo se proibido por Lei. Alega que a lei brasileira autoriza e incentiva a criptografia.

Argumenta não haver qualquer elemento que demonstre a capacidade técnica de o Whatsapp interceptar conversas criptografadas de ponta a ponta. Assim, assevera que exigir a produção de prova no sentido de sua inaptidão seria exigir prova negativa, o que não se admite no Direito.

A parte recorrente ainda sustenta que impor ou ameaçar impor multa pelo descumprimento de obrigação impossível implica ato ilegal e violador de direito líquido e certo.

Subsidiariamente, requer-se a minoração das multas ameaçadas. Nesse sentido, pleiteia a aplicação do limite do art. 75, §5º, do CPC, ou seja, até 10 salários mínimos.

Argumenta-se também a impossibilidade de executar-se a multa pela via Bacenjud.

Nestes termos, requer a revogação das ameaças de multa e de responsabilização criminal.

O Ministério Público Federal manifestou-se pelo desprovimento do recurso.



SUPERIOR TRIBUNAL DE JUSTIÇA

Por se tratar de questão com repetição de processos, o em. Min. Relator, Néfi Cordeiro, levou à sessão de julgamento da Terceira Seção o presente feito e outros correlatos.

As sustentações orais de todos os processos foram realizadas na sessão do dia 11 de março de 2020.

Após, o em. Min. Relator votou pelo provimento dos recursos, para desconstituir as decisões de primeiro grau que aplicaram multa por descumprimento de determinação judicial, com base no art. 537 do CPC c/c art. 3º do Código de Processo Penal.

Pedi então vista de todos os feitos que tratavam da matéria, tendo já antecipado voto nos demais casos. Restou-se, então, o caso específico da multa aplicada ao agente que alega impossibilidade fática em razão da criptografia de ponta a ponta.

É o relatório.

Primeiramente, destaque-se que a possibilidade de aplicação, em abstrato, da multa cominatória fora reconhecida, por maioria, neste douto Colegiado. A propósito, confira-se a ementa de um dos julgados:

RECURSO ESPECIAL. INTERCEPTAÇÃO DE DADOS. ASTREINTES. AUSÊNCIA DE PREJUDICIALIDADE POR DECISÕES DO STF. APLICABILIDADE SUBSIDIÁRIA DO CPC AO PROCESSO PENAL. MULTA DIÁRIA E PODER GERAL DE CAUTELA. TEORIA DOS PODERES IMPLÍCITOS. MEDIDAS CONSTRITIVAS SOBRE O PATRIMÔNIO DE TERCEIROS. BACEN-JUD E INSCRIÇÃO EM DÍVIDA ATIVA. PRESUNÇÃO RELATIVA DE LIQUIDEZ E CERTEZA. DEVIDO PROCESSO LEGAL. CONTRADITÓRIO POSTERGADO. ANÁLISE ESPECÍFICA DO CASO CONCRETO. CUMPRIMENTO INTEGRAL. NÃO OCORRÊNCIA. PROPORCIONALIDADE DA MULTA APLICADA. RECURSO ESPECIAL DESPROVIDO.

1. Estes autos não cuidam da criptografia de ponta-a-ponta, matéria cuja constitucionalidade encontra-se sob análise do Supremo Tribunal Federal (ADI 5527, de relatoria da Min. Rosa Weber e ADPF 403, do Min. Edson Fachin).

2. O Facebook Brasil é parte legítima para representar, no Brasil, os interesses do WhatsApp Inc, subsidiária integral do Facebook Inc.

"Com o fim de facilitar a comunicação dos atos processuais às pessoas jurídicas estrangeiras no Brasil, o art. 75, X, do CPC prevê que a pessoa jurídica estrangeira é representada em juízo 'pelo gerente, representante ou administrador de sua filial, agência ou sucursal aberta ou instalada no Brasil' e o parágrafo 3º do mesmo artigo estabelece que o 'gerente de filial ou agência presume-se autorizado pela pessoa jurídica estrangeira a receber citação para qualquer processo'. Considerando-se que a finalidade destes dispositivos legais é facilitar a citação da pessoa jurídica estrangeira no Brasil, tem-se que as expressões "filial, agência ou sucursal" não devem ser interpretadas de forma restritiva, de modo que o fato de a pessoa jurídica estrangeira atuar no Brasil por meio de empresa que não tenha sido formalmente constituída como sua filial ou agência não impede que por meio dela seja regularmente efetuada sua citação." (HDE 410/EX, Rel. Ministro BENEDITO GONÇALVES, CORTE ESPECIAL, julgado em 20/11/2019, DJe 26/11/2019). A regras advinda do precedente não deve, no caso concreto, ficar restrita à possibilidade de citação e intimação, sem possibilitar a cominação de multa. Interpretação restritiva tornaria inócua a previsão legal, pois, uma vez intimada, bastaria à representante nada fazer. Portanto, a possibilidade das astreintes revela-se imperiosa até para que se



SUPERIOR TRIBUNAL DE JUSTIÇA

dê sentido ao dispositivo.

3. Conforme amplamente admitido pela doutrina e pela jurisprudência, aplica-se o Código de Processo Civil ao Estatuto processual repressor, quando este for omissivo sobre determinada matéria.

4. "A finalidade da multa é coagir (...) ao cumprimento do fazer ou do não fazer, não tendo caráter punitivo. Constitui forma de pressão sobre a vontade", destinada a convencer o seu destinatário ao cumprimento". (MARINONI, Luiz Guilherme; ARENHART, Sérgio Cruz; e MITIDIERO, Daniel. Novo Código de Processo Civil comentado. 3ª ed. São Paulo: RT, 2017, pp. 684-685).

5. Aplica-se o poder geral de cautela ao processo penal, só havendo restrição a ele, conforme reconhecido pelo Supremo Tribunal Federal, na ADPF 444/DF, no que diz respeito às cautelares pessoais, que de alguma forma restrinjam o direito de ir e vir da pessoa. O princípio do nemo tenetur se detegere e da vedação à analogia in malam partem são garantias em favor da defesa (ao investigado, ao indiciado, ao acusado, ao réu e ao condenado), não se estendendo a quem não esteja submetido à persecução criminal. Até porque, apesar de ocorrer incidentalmente em uma relação jurídico-processual-penal, não existe risco de privação de liberdade de terceiros instados a cumprir a ordem judicial, especialmente no caso dos autos, em que são pessoas jurídicas. Trata-se, pois, de poder conferido ao juiz, inerente à própria natureza cogente das decisões judiciais.

6. A teoria dos poderes implícitos também é fundamento autônomo que, por si só, justifica a aplicação de astreintes pelos magistrados no processo criminal.

7. Sobre a possibilidade do bloqueio de valores por meio do Bacen-Jud ou aplicação de outra medida constritiva sobre o patrimônio do agente, é relevante considerar dois momentos: primeiramente, a determinação judicial de cumprimento, sob pena de imposição de multa e, posteriormente, o bloqueio de bens e constrições patrimoniais. No primeiro, o contraditório é absolutamente descabido. Não se pode presumir que a pessoa jurídica intimada, necessariamente, descumprirá a determinação judicial.

Quando do bloqueio de bens e realização de constrições patrimoniais, o magistrado age em razão do atraso do terceiro que, devendo contribuir com a Justiça, não o faz. Nesse segundo momento, é possível o contraditório, pois, supondo-se que o particular se opõe à ordem do juiz, passa a haver posições antagônicas que o justificam.

8. No caso concreto, o Tribunal local anotou que as informações requisitadas só foram disponibilizadas mais de seis meses após a quebra judicial do sigilo e expedição do primeiro ofício à empresa.

Logo, não se verifica o cumprimento integral da medida.

9. Em relação à proporcionalidade da multa, o parâmetro máximo de R\$ 50.000,00 (cinquenta mil reais) fixado por esta Corte em caso assemelhado, na QO-Inq n. 784/DF, foi observado. Assim, não merece revisão.

10. Recurso especial desprovido."

(REsp 1568445/PR, Rel. Ministro ROGERIO SCHIETTI CRUZ, Rel. p/ Acórdão Ministro RIBEIRO DANTAS, TERCEIRA SEÇÃO, julgado em 24/06/2020, DJe 20/08/2020).

No caso concreto, porém, há de se fazer uma distinção ou um *distinguishing*



SUPERIOR TRIBUNAL DE JUSTIÇA

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.

Aqui, é importante entender que "**criptografia** é o nome dado aos mecanismos que transformam informações que eram transparentes em algo que não possa ser compreendido por um agente externo. Uma chave de criptografia é usada com o algoritmo para embaralhar as mensagens, de modo que seja impossível para um intermediário que tenha acesso a elas compreender o conteúdo. Portanto, as informações são codificadas. Para tornar o texto compreensível novamente, é necessário ter acesso à chave correta. Dessa forma, apenas a pessoa que detém a chave pode ver os dados originais. A chave é uma sequência muito longa de números gerada pelo software, seja um app de mensagens ou um serviço de e-commerce protegendo dados de cartão de crédito. Existem dois tipos de criptografia: a simétrica e a assimétrica. A criptografia de ponta-a-ponta [*sic*] é uma implementação da assimétrica." (COUTINHO, Mariana. O que é criptografia de ponta a ponta? Entenda o recurso de privacidade. **Tectudo**. Disponível em:

<<https://www.techtudo.com.br/noticias/2019/06/o-que-e-criptografia-de-ponta-a-ponta-entenda-o-recurso-de-privacidade.ghtml>>. Acesso em: 24 mar. 2020).

Criptografia de ponta a ponta, por sua vez, 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." (*Idem*).

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.

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

Porém, o Direito, como fruto do intelecto humano e indispensável ao convívio coletivo sadio e com capacidade prospectiva, nem sempre se contenta com o nexu 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).

Assim, passa-se ao exame dos argumentos possíveis. Primeiro, argumentação favorável à aplicação da multa, mesmo diante da impossibilidade técnica.

Como salienta o ex-Ministro da Suprema Corte Eros Grau, em sua obra **A ordem econômica na constituição de 1988**, "Os homens ... não fazem a História como querem, mas sim sob circunstâncias com as quais se defrontam." Assim, o caminho que se revela cabível, no presente litígio, necessariamente perpassa por uma laboriosa operação de ajustes, para que se evite o total desprezo dos direitos envolvidos. Dessa forma, com fulcro no **princípio da concordância prática ou da harmonização**, deve-se buscar a coordenação e combinação dos bens jurídicos em conflito, de modo a evitar o sacrifício total de um deles em favor do outro. (CANOTILHO, J. J. Gomes. Direito Constitucional e teoria da constituição, 3ª ed. p. 1237).



SUPERIOR TRIBUNAL DE JUSTIÇA

Aqui, é importante salientar que, a despeito de a ordem econômica se fundar na livre iniciativa, ela tem por fim assegurar existência digna, conforme os ditames de justiça social. Logo, os agentes econômicos devem se ater também às leis e às diretrizes sociais, de modo a atender a função social de sua atividade e assim poder legitimar o seu exercício. Não se pode deixar de trazer à lume o importante art. 170 da Constituição Federal:

"Art. 170. A ordem econômica, fundada na valorização do trabalho humano e na livre iniciativa, tem por fim assegurar a todos existência digna, conforme os ditames da justiça social, observados os seguintes princípios:

[...]

II - propriedade privada;

III - **função social da propriedade;**

IV - livre concorrência;

V - defesa do consumidor;

VI - defesa do meio ambiente, inclusive mediante tratamento diferenciado conforme o impacto ambiental dos produtos e serviços e de seus processos de elaboração e prestação;

VII - redução das desigualdades regionais e sociais;

VIII - busca do pleno emprego;

IX - tratamento favorecido para as empresas de pequeno porte constituídas sob as leis brasileiras e que tenham sua sede e administração no País." (Grifou-se).

A partir daí, revela-se interessante citar a teoria dos riscos do desenvolvimento. Riscos de desenvolvimento "são os defeitos que - em face do estado da ciência e da técnica à época da colocação em circulação do produto ou serviço eram desconhecidos e imprevisíveis." (BENJAMIN, Antônio Herman de V.; MARQUES, Cláudia Lima; BESSA, Leonardo Roscoe. *Manual de direito do consumidor*, p. 155).

No caso concreto, considera-se defeito do serviço a obstrução de uma medida legítima, reconhecida inclusive pela Constituição da República: fornecimento de dados para persecução penal.

Ainda em sede de responsabilidade civil, a professora Giselda Hironaka, desenvolvedora da tese da responsabilidade pressuposta, nas palavras Flávio Tartuce, diz ser necessário "*buscar, em um primeiro plano, reparar a vítima, para depois verificar-se de quem foi a culpa, ou quem assumiu o risco*. Com isso, o dano assume o papel principal no estudo da responsabilidade civil, deixando de lado a culpa. Ademais, pela tese, *pressupõe-se a responsabilidade do agente pela exposição de outras pessoas a situações de risco ou de perigo, diante de sua atividade (mise en danger)*." (Direito das Obrigações e Responsabilidade Civil. V. 2, 2017, p. 377).

Nessa toada, verifique-se que o ordenamento jurídico como um todo, não só no âmbito do Direito Civil, passou a reconhecer a natureza axiológica da norma jurídica e o papel criativo do julgador. A legalidade estéril deu lugar a uma nova realidade. Pautado pelo princípio da eticidade e sintonizado com o pós-positivismo, que floresce no pós-Guerra, Miguel Reale, responsável pelo projeto do Código Civil de 2002, reconhece a insuficiência e os limites da lei:

"Em nosso projeto não prevalece a crença na plenitude hermética do Direito Positivo, sendo reconhecida a imprescindível eticidade do ordenamento. O código é um sistema, um conjunto harmônico de preceitos que exigem a todo instante recurso à analogia e a princípios gerais, devendo ser valoradas todas as consequências da cláusula rebus sic stantibus. Nesse sentido, é posto o princípio do equilíbrio econômico dos contratos como base ética



SUPERIOR TRIBUNAL DE JUSTIÇA

de todo o Direito Obrigacional.

[...]

Tal reconhecimento vem estabelecer uma função mais criadora por parte da Justiça em consonância com o princípio de eticidade, cujo fulcro fundamental é o valor da pessoa humana como fonte de todos os valores. Como se vê, o novo código abandonou o formalismo técnico-jurídico próprio do individualismo da metade deste século, para assumir um sentido mais aberto e compreensivo, sobretudo numa época em que o desenvolvimento dos meios de informação vem ampliar os vínculos entre os indivíduos e a comunidade." (Disponível em: <<http://www.miguelreale.com.br/artigos/vgpc.htm>>. Acesso em: 24/4/2020).

Assim, 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.

Veja-se 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. Nesse sentido:

"Enunciado 362/CJF. A vedação do comportamento contraditório (*venire contra factum proprium*) funda-se na proteção da confiança, tal como se extrai dos arts. 187 e 422 do Código Civil."

Confirmam-se alguns precedentes desta Corte aplicando a máxima citada:

"PROCESSUAL CIVIL. RECURSO ESPECIAL. [...] COMPORTAMENTO PROCESSUAL CONTRADITÓRIO. *VENIRE CONTRA FACTUM PROPRIUM*. RECURSO MANIFESTAMENTE INFUNDADO. APLICAÇÃO DE MULTA. RECURSO NÃO PROVIDO.

[...]

4. É contrária a dialética processual aceitar determinado procedimento e, diante da prova contrária aos próprios interesses, insurgir-se contra o que foi acordado pelas próprias partes.

5. Agravo regimental não provido, com aplicação de multa." (AgRg no AREsp 269.744/PR, Rel. Ministro LUIS FELIPE SALOMÃO, QUARTA TURMA, julgado em 28/05/2013, DJe 03/06/2013).

"EMBARGOS DE DECLARAÇÃO NO RECURSO ESPECIAL REPRESENTATIVO DE CONTROVÉRSIA (TRIBUTÁRIO. PROCESSO ADMINISTRATIVO FISCAL. PAES. PARCELAMENTO ESPECIAL. [...]



SUPERIOR TRIBUNAL DE JUSTIÇA

PROIBIÇÃO DO COMPORTAMENTO CONTRADITÓRIO (**NEMO POTEST VENIRE CONTRA FACTUM PROPRIUM**). MANIFESTO INTUITO INFRINGENTE. MULTA POR EMBARGOS DE DECLARAÇÃO PROCRASTINATÓRIOS (ARTIGO 538, DO CPC). APLICAÇÃO.

[...]

12. Deveras, o princípio da confiança decorre da cláusula geral de boa-fé objetiva, dever geral de lealdade e confiança recíproca entre as partes, sendo certo que o ordenamento jurídico prevê, implicitamente, deveres de conduta a serem obrigatoriamente observados por ambas as partes da relação obrigacional, os quais se traduzem na ordem genérica de cooperação, proteção e informação mútuos, tutelando-se a dignidade do devedor e o crédito do titular ativo, sem prejuízo da solidariedade que deve existir entre ambos.

13. Assim é que o titular do direito subjetivo que se desvia do sentido teleológico (finalidade ou função social) da norma que lhe ampara (excedendo aos limites do razoável) e, após ter produzido em outrem uma determinada expectativa, contradiz seu próprio comportamento, incorre em abuso de direito encartado na máxima **nemo potest venire contra factum proprium**.

[...]

4. Embargos de declaração rejeitados, com a condenação da embargante ao pagamento de 1% (um por cento) a título de multa, pelo seu caráter procrastinatório (artigo 538, parágrafo único, do CPC)." (EDcl no REsp 1143216/RS, Rel. Ministro LUIZ FUX, PRIMEIRA SEÇÃO, julgado em 09/08/2010, DJe 25/08/2010; grifou-se).

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:

"Art. 4º Esta Lei **não se aplica** ao tratamento de dados pessoais:

[...]

III - realizado para fins exclusivos de:

[...]

d) **atividades de investigação e repressão de infrações penais;**

§ 2º É vedado o tratamento dos dados a que se refere o inciso III do caput deste artigo por pessoa de direito privado, **exceto** em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico à autoridade nacional e que deverão observar a limitação imposta no § 4º deste artigo." (Grifou-se).

No artigo 7º, a Lei traz requisitos para tratamento dos dados pessoais:



SUPERIOR TRIBUNAL DE JUSTIÇA

"Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

[...]

II - para o **cumprimento de obrigação legal** ou regulatória pelo controlador;

[...]

VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;

VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;

[...]

IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais;" (Grifou-se).

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. 6º:

"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:

"As obrigações e a responsabilidade civil de empresas atuantes no ambiente da internet, após tratamento jurisprudencial, teve seus contornos legais delimitados na Lei n. 12.965/2014. O Marco Civil da Internet, além de reconhecer a essencialidade do acesso à internet para o exercício da cidadania, posicionou no vértice principiológico da regulamentação o cuidado com a intimidade e a privacidade.

Decorrente dessa orientação, a necessária proteção aos registros, dados pessoais e comunicações privadas foi disciplinada de modo a restringir sua guarda por provedores de conexão e de acesso a aplicações. **De outro lado, resultante da ponderação de interesses legítimos conflitantes, também se assegurou o acesso aos dados necessários à identificação de autores de crimes ou causadores de danos civis, obrigando-se, pela via judicial, os provedores à eventual disponibilização dos dados por eles guardados.**

É o que se extrai do art. 10 e seu § 1º (sem destaques no original):



SUPERIOR TRIBUNAL DE JUSTIÇA

Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.

§ 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no *caput*, de forma autônoma ou associados a dados pessoais ou a outras informações que possam **contribuir para a identificação do usuário ou do terminal**, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º.

Essa obrigação de guarda de dados do acesso foi ainda repartida entre os provedores de conexão e os provedores de aplicações. Evidenciando a preocupação constante com o respeito à privacidade no ambiente virtual, vedou-se a guarda dos dados de acessos a aplicações aos provedores de conexão. Noutros termos, aos provedores de conexão somente cabe a guarda dos dados de conexão (IP, data e horário), tornando impossível, apenas com esses dados, se conhecer a atividade completa do internauta, enquanto efetivamente conectado à rede mundial (art. 14 da Lei n. 10.965/2014). Do mesmo modo, cada provedor de aplicação somente poderá – e deverá – manter registros de acesso e de cadastro (quando houver) daquele que esteve conectado a sua aplicação, sendo igualmente vedado manter os dados da navegação, salvo consentimento do titular dos dados (art. 16 da Lei n. 10.965/2014).

Isso porque, de tudo quanto foi exposto, não há dúvidas de que o intuito do legislador ao regulamentar os dados que deveriam ser guardados, o sigilo e as hipóteses de seu levantamento, foi o de viabilizar a identificação dos causadores de danos ou, ao menos, dos dispositivos por eles utilizados. Esse é, portanto, o norte para interpretação conjunta dos arts. 15 e 5º, VIII, da Lei n. 12.965/2014.

Noutros termos, ainda que o legislador, ao estabelecer a obrigação de guarda dos dados de acesso à aplicação tenha se referido apenas aos respectivos registros de acesso (art. 15 da Lei n. 12.965/2014), os quais, por sua vez, conforme a definição do art. 5º, VIII, se restringe à data e hora de uso "a partir de um determinado endereço IP", enquanto não se restabelecer a relação de individualidade dos IPs é preciso que se entenda incluída no endereço IP a correspondente porta lógica de origem, em razão da indissociabilidade entre as duas tecnologias para o efetivo acesso individualizado à internet e às aplicações. Do contrário, a adoção da tecnologia paliativa resultaria no esvaziamento da lei, tornando inviável a identificação e responsabilização desses sujeitos.

Acrescenta-se que a questão da identificação de causadores de danos nesse cenário de transição foi objeto de intenso debate pelo Grupo de Trabalho da Agência Nacional de Telecomunicações – Anatel para implantação do protocolo IP Versão 6 nas redes das Prestadoras de Serviços de Telecomunicações. Em seu relatório final, o referido Grupo de Trabalho assinalou a imprescindibilidade do fornecimento das portas lógicas por provedores de aplicações, constatando a necessidade de adaptação tecnológica para armazenagem de todas as informações de acesso, nas quais se inclui a porta lógica, sempre que se tratar de endereço IPv4 (disponível em



SUPERIOR TRIBUNAL DE JUSTIÇA

<<http://www.anatel.gov.br/Portal/verificaDocumentos/documento.asp?numeroPublicacao=325769&assuntoPublicacao=null&caminhoRel=null&filtro=1&documentoPath=325769.pdf>>, acesso em 16/4/2019, p. 14-15):

Tanto no Grupo de Trabalho do NIC.br como no Grupo de Trabalho da ANATEL foi intensamente discutida a questão da identificação unívoca de um determinado usuário que faz uso de um endereço IP compartilhado. Em ambos os Grupos de Trabalho foi consenso que a única forma das prestadoras fornecerem o nome do usuário que faz uso de um IP compartilhado em um determinado instante seria com a informação da “porta lógica de origem da conexão” que estava sendo utilizada durante a conexão. Dessa forma, **os provedores de aplicação devem fornecer não somente o IP de origem utilizado para usufruto do serviço que ele presta, mas também a “porta lógica de origem”**.

.....
Diante do exposto, é importante reforçar que durante o período de utilização da solução paliativa do CG-NAT44, para que o processo de apuração de ilícitos na Internet não fique prejudicado, **é necessário que, não só provedores de acesso, como também provedores de conteúdo e serviços de internet (bancos e sites de comércio eletrônico, por exemplo) adaptem seus sistemas para possibilitar a armazenagem dos registros de aplicação (provedores de aplicação) ou registros de conexão (provedores de acesso) com a informação da “porta lógica de origem” utilizada.**

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.

Observe-se:

"A Polícia Federal deflagrou nesta quarta-feira (5/6) uma ação policial que apura a prática dos **crimes de armazenamento e compartilhamento digital de pornografia infantil**. Um homem, de 30 anos, foi preso em flagrante.

As investigações iniciaram a partir de informações fornecidas por entidades de cooperação internacional, as quais apontaram atividades de pedofilia na internet e na **deep web**, tendo como origem o território nacional. Chegou-se a um suspeito pelos endereços de compartilhamento, que foi posteriormente identificado como local de moradia e trabalho do mesmo." (Disponível em:



SUPERIOR TRIBUNAL DE JUSTIÇA

<<http://www.pf.gov.br/imprensa/noticias/2019/06/pf-combate-o-compartilhamento-de-pornografia-infantil-pela-internet>>. Acesso em: 24 de mar. 2020. Grifou-se).

"O ministro da Justiça, Torquato Jardim, afirmou que criminosos presos por trocar imagens de **pornografia infantil usavam área oculta da internet** para trocar imagens de pornografia infantil. Segundo ele, parte da operação foi viabilizada a partir de investigações na chamada 'deep web' (web profunda), a qual ele classificou como 'perigosíssima.'" (Disponível em:

<<https://g1.globo.com/rio-de-janeiro/noticia/ministro-da-justica-detalha-operacao-de-combate-a-pedofilia-no-pais.ghtml>>. Acesso em: 24 de mar. 2020. Grifou-se).

"O Exército deve entrar em campo para ajudar o Ministério Público de São Paulo e a Polícia Civil a aprimorar seus mecanismos de investigação de crimes cometidos com ajuda da Internet. Na semana que vem haverá uma reunião entre estes órgãos para discutir ferramentas e ações conjuntas que possam prevenir ataques terroristas orquestrados com uso da web – e mais especificamente da **Deep Web**, a Internet que não é indexada por mecanismos de busca tradicionais como o Google. A informação foi confirmada ao EL PAÍS nesta segunda-feira pelo coordenador do Núcleo de Combate aos Crimes Cibernéticos do MP-SP, o procurador Paulo Marcos Ferreira Lima. O anúncio veio dias depois do procurador-geral de Justiça, Gianpaolo Smanio, afirmar que o órgão investiga se os autores do massacre na escola Professor Raul Brasil, em Suzano, teriam orquestrado o ataque com o auxílio de fóruns radicais hospedados na deep web." (Disponível em:

<https://brasil.elpais.com/brasil/2019/03/18/politica/1552945133_746821.html>. Acesso em: 24 de mar. 2020. Grifou-se).

Ainda sobre essa região da internet denominada **deep web**:

"A deep web tem o seu lado "bom", que é a privacidade para troca de conteúdo e informações sigilosas, por exemplo. Mas também tem o lado ruim, **cheio de crimes, pornografia, tráfico de drogas e outras ilegalidades. É a parte da deep web que muitos chamam de dark web.** Superficialmente, **o que parece fazer mais sucesso na dark web é o tráfico de drogas, tanto que existem listas de vendedores recomendados, de acordo com a confiabilidade de cada um.** Mas o **comércio de armas** corre solto, assim como o de contas do PayPal e de produtos roubados - existem lojas específicas para marcas como Apple e Microsoft, por exemplo. Também dá para contratar **assassinos de aluguel** que possuem valores para cada tipo de pessoa (celebridades, políticos etc.), com preços que vão de US\$ 20 mil a US\$ 150 mil.

Cibercriminosos e espíões oferecem seus serviços, e tem gente que garante fazer trabalhos acadêmicos sobre qualquer assunto, sem copiar de lugar algum. **Sites promovem turismo sexual** e, por menos de US\$ 1 mil, prometem buscar o comprador no aeroporto. Outro destaque é a **venda de documentos falsos, com páginas que oferecem até cidadania norte-americana.** O dinheiro é abolido na deep web e poucos negociantes



SUPERIOR TRIBUNAL DE JUSTIÇA

confiam no PayPal, a bola da vez é mesmo a Bitcoin, uma moeda digital que torna as transações mais seguras.

Por meio de fóruns e redes de comunicação, há a **comercialização de todos os tipos de informações que um ataque digital pode ter acesso**. E sempre há um público preparado para aproveitar estas informações. A lista dos tipos de dados que podem ser comprados inclui:

Cartões de crédito roubados com informações detalhadas das vítimas
Dados pessoais, como nome, CPF, RG, placa do carro, chassi
Páginas falsas idênticas às do banco para serem usadas em golpes de phishing, mandando a vítima para um site falso com o objetivo de roubar informações
Malware de ponto de venda, que infectam computadores de empresas para roubar as informações da companhia e dos clientes
Diplomas falsificados

Aluguel de ataques DDoS sem que você precise ter sua própria botnet (rede de computadores infectados). Pague US\$ 10 por uma hora, US\$ 50 por dia ou US\$ 400 por mês para derrubar algum serviço ou site online.

Mas se o vendedor e o comprador são obviamente criminosos, como um estabelece a confiança no outro para que haja o pagamento e a entrega da "mercadoria"? Para isso, há algumas ferramentas.

O dono do fórum normalmente age como mediador das transações, levando uma comissão no caminho. Ele recebe o dinheiro do comprador e só o libera para o vendedor depois de haver a confirmação de que tudo aconteceu de acordo com o combinado. Por isso também são comuns os casos de sites que subitamente desaparecem levando todo o dinheiro de transações que ainda não haviam sido completadas.

Nestes fóruns também normalmente há rankings de confiança, não muito diferentes dos fóruns da "surface web" que normalmente exibem um índice de reputação por usuário. Se a pessoa é um negociante "honesto" (muitas aspas aqui), ele tende a receber uma boa avaliação para continuar exercendo mais tranquilamente sua atividade." (Deep Web: o que é, como entrar e o que acontece na parte sombria da internet. **Olhar digital**. Disponível em:

<https://olhardigital.com.br/fique_seguro/noticia/deep-web-saiba-o-que-acontece-na-parte-obscura-da-internet/31120> Acesso em: 24 de mar. 2020. Grifou-se).

Com efeito, a ausência de controle das mensagens que trafegam no *WhatsApp* 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 (emissor 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. Confira:

"De outra parte, quanto aos custos do armazenamento dos logs dos usuários, correto o entendimento do Tribunal no sentido de que se trata de



SUPERIOR TRIBUNAL DE JUSTIÇA

'providência inerente ao risco do próprio negócio', devendo a empresa suportar esse custo.

A alegação de impossibilidade fática, portanto, não obsta o pedido de identificação do usuário."

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 *WhatsApp*, 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 notifica 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 *WhatsApp*. A autoridade policial, então, representa pela interceptação do *WhatsApp* 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 *WhatsApp* 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 descumpra 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.

Com efeito, passa-se à análise, dos fundamentos pela não aplicação da multa cominatória, quando se estiver diante da chamada criptografia de ponta a ponta.

O argumento nuclear dessa segunda corrente é no sentido de que ninguém pode ser obrigado a fazer o impossível (*ad impossibilia nemo tenetur*).

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:



SUPERIOR TRIBUNAL DE JUSTIÇA

“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 WhatsApp 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 WhatsApp 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 46 Cópia ADPF 403 / SE criptografar as mensagens e, posteriormente, colar tal mensagem no WhatsApp, para enviá-la a outro usuário, de modo que, mesmo que houvesse a interceptação da mensagem pelo WhatsApp, seria impossível descriptá-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.”

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

Início 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



SUPERIOR TRIBUNAL DE JUSTIÇA

modo de se expressar ou até mesmo absterem-se 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 pré-condição do desenvolvimento pessoal autônomo. Seres humanos desenvolvem suas personalidades comunicando-se com os demais.”

As consequências da ausência dessa pré-condição 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.

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 reprimida 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)



SUPERIOR TRIBUNAL DE JUSTIÇA

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.” (Grifou-se)

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”?

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:



SUPERIOR TRIBUNAL DE JUSTIÇA

“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.”

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.

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

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.

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.

Com essas considerações, seguindo o voto do em. Ministro Relator, **dou provimento** ao recurso ordinário, 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.

É o voto.



SUPERIOR TRIBUNAL DE JUSTIÇA

CERTIDÃO DE JULGAMENTO TERCEIRA SEÇÃO

Número Registro: 2019/0099392-7 **PROCESSO ELETRÔNICO** **RMS 60.531 / RO**
MATÉRIA CRIMINAL

Números Origem: 00027198820188220501 00029229820188220000 27198820188220501
29229820188220000

PAUTA: 11/03/2020

JULGADO: 09/12/2020
SEGREDO DE JUSTIÇA

Relator

Exmo. Sr. Ministro **NEFI CORDEIRO**

Relator para Acórdão

Exmo. Sr. Ministro **RIBEIRO DANTAS**

Presidente da Sessão

Exmo. Sr. Ministro REYNALDO SOARES DA FONSECA

Subprocuradora-Geral da República

Exma. Sra. Dra. JULIETA E. FAJARDO C. DE ALBUQUERQUE

Secretário

Bel. GILBERTO FERREIRA COSTA

AUTUAÇÃO

RECORRENTE : WHATSAPP INC
ADVOGADOS : ROCHILMER MELLO DA ROCHA FILHO - RO000635
ADRIELE PINHEIRO REIS AYRES DE BRITTO - DF023490
DAVI DE PAIVA COSTA TANGERINO - SP200793
MARCELO MONTALVAO MACHADO - DF034391
MARCELA TRIGO DE SOUZA - RJ127614
RECORRIDO : MINISTÉRIO PÚBLICO DO ESTADO DE RONDÔNIA

ASSUNTO: DIREITO PROCESSUAL PENAL

CERTIDÃO

Certifico que a egrégia TERCEIRA SEÇÃO, ao apreciar o processo em epígrafe na sessão realizada nesta data, proferiu a seguinte decisão:

Retomado o julgamento, após o voto-vista divergente, quanto à fundamentação, do Sr. Ministro Ribeiro Dantas, dando provimento ao recurso ordinário 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, e os votos dos Srs. Ministros Antonio Saldanha Palheiro, Joel Ilan Paciornik, Laurita Vaz, Sebastião Reis Júnior (com ressalva) e Rogerio Schietti Cruz no mesmo sentido, a Terceira Seção, por maioria, deu provimento ao recurso ordinário 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, nos termos do voto do Sr. Ministro Ribeiro Dantas, que lavrará o acórdão.

Votou vencido o Sr. Ministro Nefi Cordeiro.



SUPERIOR TRIBUNAL DE JUSTIÇA

Votaram com o Sr. Ministro Ribeiro Dantas os Srs. Ministros Antonio Saldanha Palheiro, Joel Ilan Paciornik, Laurita Vaz, Sebastião Reis Júnior (com ressalva) e Rogerio Schietti Cruz.

Não participaram do julgamento os Srs. Ministros Felix Fischer e João Otávio de Noronha.

Presidiu o julgamento o Sr. Ministro Reynaldo Soares da Fonseca.