V O T O

SÍNTESE DO VOTO

1. O presente voto, ao dispor dos eminentes pares e das partes na íntegra, expressa fundamentação nos termos do inciso IX do art. 93 da Constituição da República Federativa do Brasil, e se contém em aproximadamente 75 páginas. A síntese e a conclusão podem ser apresentadas, sem prejuízo da explicitação no voto contida, à luz do procedimento que se fundamenta nos termos do insculpido no inciso LXXVIII do art. 5º da Constituição Federal de 1988, em cuja abrangência se insere a celeridade de julgamento, mediante sucinta formulação que tem em conta as seguintes premissas e arremate:

1.1. **Premissas**

Primeira: o impacto tecnológico das mudanças porque passa a sociedade reclamam um permanente atualizar do alcance dos direitos e garantias fundamentais.

Segunda: os direitos que as pessoas têm *offline* devem também devem ser protegidos *online*. Direitos digitais são direitos fundamentais.

Terceira: a garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet

Quarta: a privacidade é o direito de manter o controle sobre a sua própria informação e de determinar a maneira de construir sua própria esfera pública.

Quinta: A liberdade de expressão tem primazia *prima facie* e constitui condição essencial ao pluralismo de ideias, vetor estruturante do sistema democrático de direito.

Sexta: Na internet, a criptografia e o anonimato são especialmente úteis para o desenvolvimento e compartilhamento de opiniões, o que geralmente ocorre por meio de comunicações online como o e-mail, mensagens de texto e outras interações. A criptografia, em especial, é um meio de se assegurar a proteção de direitos que, em uma sociedade

democrática, são essenciais para a vida pública.

Sétima: É contraditório que em nome da segurança pública deixe-se de promover e buscar uma internet mais segura. Uma internet mais segura é direito de todos e dever do Estado. Medidas que, à luz da melhor evidência científica, trazem insegurança aos usuários somente se justificam se houver certeza comparável aos ganhos obtidos em outras áreas.

1.2. **Base constitucional**: o direito à comunicação (art. 5º, IX, da CRFB), à liberdade de pensamento e de sua expressão (art. 5º, IV, da CRFB) e à privacidade (art. 5º, X, XI, e XII); e **base convencional** (art. 5º, § 2º, da CRFB): a liberdade de opinião e de expressão (artigo 19 do Pacto Internacional de Direitos Civis e Políticos e artigo 13 do Pacto de São José da Costa) e o direito à privacidade (artigo 17 do Pacto Internacional de Direitos Civis e Políticos e artigo 11 do Pacto de São José da Costa Rica).

1.3. **Base em precedentes:** o voto se estriba em precedentes que formam jurisprudência deste Tribunal, do Conselho de Direitos Humanos das Nações Unidas, da Corte Europeia de Direitos Humanos e do Comitê de Direitos Humanos.

1.4. **Base doutrinária:** o voto faz referência ao Relatório *The Effect of Encryption on Lawful Access to Communication and Data* de autoria de James A. Lewis, Denis E. Zheng e William A. Carter; ao artigo *On Balancing and Subsumption. A Strucutral Comparison* de autoria de Robert Alexy; às obras de Stéfano Rodotà (*Data Protection as a Fundamental Right*); aos *Comentários ao Pacto Internacional de Direitos Civis e Políticos*, elaborado por Manfred Nowak; ao artigo *Habeas data e autodeterminação informativa: os dois lados da mesma moeda*, de autoria de Laura Schertel Ferreira Mendes; aos *Comentários à Constituição* de João Barbalho; ao texto P*assado, presente e futuro da criptografia forte* de Jacqueline de Souza Abreu; e ao brilhante artigo de Harold Abelson et al. Intitulado *Keys under doormats*.

Conclusão do voto: Julgo procedente a presente arguição de descumprimento de preceito fundamental para declarar a inconstitucionalidade parcial sem redução de texto tanto do inciso II do art. 7º, quanto do inciso III do art. 12 da Lei 12.965/2014, de modo a

afastar qualquer interpretação do dispositivo que autorize ordem judicial que exija acesso excepcional a conteúdo de mensagem criptografada ponta-a-ponta ou que, por qualquer outro meio, enfraqueça a proteção criptográfica de aplicações da internet.

O SENHOR MINISTRO EDSON FACHIN (RELATOR): Principio a presente manifestação pelo registro de genuíno agradecimento aos *amici curiae* e às entidades que participaram da audiência pública realizada no âmbito desta arguição de descumprimento de preceito fundamental e da ação direta de inconstitucionalidade sob Relatoria da e. Ministra Rosa Weber.

Como se verá ao longo dessa manifestação, a contribuição aportada aos autos foi fundamental para elucidar questões complexas sobre o funcionamento do Marco Civil da Internet e dos aplicativos de celular que hoje são ferramentas indispensáveis para o exercício do direito de comunicação.

Antes de examinar os argumentos trazidos no mérito, porém, é preciso afastar as preliminares que foram arguidas pela Procuradoria-Geral da República, pelo Ministério da Justiça e pela Associação dos Magistrados Brasileiros, *amicus curiae* da presente arguição.

Alegações das Partes sobre as Preliminares

Alegações da Procuradoria-Geral da República

A Procuradoria-Geral da República defende, em seu parecer inicial, que o Partido requerente não trouxe aos autos cópia do ato impugnado na presente arguição. Além disso, sustenta que a decisão impugnada, a saber a decisão no âmbito do processo autuado sob n. 201655000183, que tramita perante o Juízo da Vara Criminal da Comarca de Lagarto, foi suspensa pelo Tribunal de Justiça local, o que implicaria a perda de objeto da presente arguição. No que tange ao pedido para que fossem proibidas as decisões judiciais que determinem a suspensão do aplicativo *Whatsapp*,

alega que o Partido não trouxe ato do poder público que justificasse o pedido, razão pela qual, em seu entender seria inepta a petição inicial. Finalmente, alega também não ser possível o conhecimento da ação porquanto o Partido requerente não impugnou todo o complexo normativo.

Alegações do Ministério da Justiça

O Ministério da Justiça suscitou a inépcia da inicial, corroborando os argumentos trazidos pelo Procurador-Geral da República (eDOC 102, p. 14-15).

Alegações do *amicus curiae*

A Associação dos Magistrados Brasileiros questiona o cabimento da ADPF para submeter ao exame direto do Supremo Tribunal Federal a interpretação legal feita por juízes criminais. Afirma, em síntese, que falta à ação o requisito da subsidiariedade, porquanto a decisão poderia, em tese, ser impugnada nas vias processuais ordinárias.

Exame das alegações trazidas

A presente arguição de descumprimento de preceito fundamental merece ser conhecida. Conquanto no parecer final não tenha a Procuradoria aderido à objeção do conhecimento, examino as alegações, para assentar o pleno conhecimento da arguição.

Apesar de não ter havido a juntada da decisão proferida pelo juiz de direito da comarca de Lagarto quando do ajuizamento da ação, as informações prestadas pelo juiz, assim como documentos posteriormente trazidos aos autos dão conta do inteiro teor da decisão objeto da arguição, o que já autorizaria a superação da preliminar. Ademais, cumpre observar, tal como já indicado no relatório e na decisão monocrática proferida pelo Presidente do Supremo Tribunal Federal, o Partido

requerente, em nova manifestação, acrescentou a decisão proferida pelo juízo da Segunda Vara Criminal da Duque de Caxias no Rio de Janeiro, cujas informações também foram prestadas pela referida autoridade. Por isso, deve-se rejeitar a alegação de inépcia ante a ausência de juntada dos documentos.

No que tange ao prejuízo da arguição, é preciso observar que o juízo sobre a constitucionalidade em abstrato no âmbito da presente arguição não recai apenas sobre as decisões, mas sobre as suspensões, por ordem judicial, do funcionamento do aplicativo *Whatsapp*, tal como se depreende do pedido final da arguição (eDOC 1, p. 9):

> "(...) seja julgado o presente pedido de arguição de descumprimento de preceito fundamental, para reconhecer a existência de violação ao preceito fundamental à comunicação, nos termos do art. 5º, inciso IX, com a finalidade de não mais haver suspensão do aplicativo de mensagens WhatsApp por qualquer decisão judicial."

A subsidiar o pedido, o Partido requerente colaciona diversas decisões de juízos que suspenderam o funcionamento do aplicativo de mensagens. Assim, a partir do exame da petição inicial, deve-se reconhecer que a perda de objeto ainda não ocorreu, porquanto ainda possível, em tese, a apreciação do pedido formulado. Ademais, muito embora a decisão de suspensão do aplicativo tenha sido cassada por decisão colegiada em mandado de segurança, o processo no qual a medida cautelar foi proferida ainda não foi encerrado, ao menos do que se tem dos autos. De igual modo, a decisão proferida pelo douto juízo da Segunda Vara Criminal de Duque de Caxias permanece suspensa por força da decisão cautelar proferida pelo e. Ministro Ricardo Lewandowski, no exercício da Presidência deste Tribunal. À luz dos pedidos deduzidos na ADI 5.527, Rel. Ministra Rosa Weber, eventual procedência da ação não atingiria as decisões que foram aqui impugnadas. Por essas razões, não procede a alegação de perda de objeto.

Também não merece ser acolhida a tese de que o Partido requerente

deixou de impugnar todo o complexo normativo. Como se depreende do teor da petição inicial, o parâmetro invocado é o direito à comunicação, consagrado no art. 5º, IX, da Constituição Federal, e os atos questionados não são, a rigor, leis ordinárias, mas decisões judiciais. Porque essas decisões tomaram por base o Marco Civil da Internet, é à luz de seus dispositivos e de sua fundamentação que se deve examinar eventual incompatibilidade com a Constituição. É de se rejeitar, portanto, também essa alegação.

Relativamente à ausência de subsidiariedade, tal como apontada pelo douto *amicus curiae*, deve-se observar que há precedentes desta Corte que entendem possível o manejo de arguição de descumprimento de preceito fundamental para impugnar diversas decisões de judiciais. É, nesse sentido, o acórdão relatado pela e. Min. Cármen Lúcia, quando do julgamento da ADPF 101:

> "Multiplicidade de ações judiciais, nos diversos graus de jurisdição, nas quais se têm interpretações e decisões divergentes sobre a matéria: situação de insegurança jurídica acrescida da ausência de outro meio processual hábil para solucionar a polêmica pendente: observância do princípio da subsidiariedade. Cabimento da presente ação".

Mais recentemente, também por meio de decisão colegiada, o Tribunal julgou inconstitucional a interpretação feita por um conjunto de decisões judiciais que tinha por constitucionalmente admissíveis a denominada condução coercitiva de acusado (ADPF 444, Rel. Min. Gilmar Mendes, DJe 21.05.2019).

De fato, como há tempos se estabeleceu na jurisprudência desta Corte, o requisito da subsidiariedade, previsto no art. 4º, § 1º, da Lei 9.882, de 1999, consiste na inexistência de outro meio apto para sanar a lesividade apontada. Tal como se observou quando do julgamento da ADPF 33, Rel. Min. Gilmar Mendes, "tendo em vista o caráter enfaticamente objetivo do instituto (o que resulta, inclusive, da legitimação ativa), meio eficaz de sanar a lesão parece ser aquele apto a

solver a controvérsia constitucional relevante de forma **ampla**, **geral** e **imediata**". Sendo esse o sentido da subsidiariedade definido na jurisprudência da Corte, não é difícil ver que as decisões aqui impugnadas, especialmente pela multiplicidade de atores afetados, não poderia ser solucionada a tempo, de forma geral, apenas pelas vias recursais ordinárias. A própria decisão do Tribunal de Justiça do Estado de Sergipe fez observar a necessidade de uma decisão do Supremo Tribunal Federal (eDOC 10, p. 7):

> "Este é um caso em que se vislumbra a necessidade de uma decisão suprema em via de repercussão geral pelo STF, pois normatizaria os serviços de redes sociais em todo o território."

Tampouco se poderia cogitar do cabimento da ação direta, uma vez que ela se destina a impugnar lei ou ato normativo e não, como se aduz da inicial, o conjunto de decisões judiciais. A controvérsia acerca da validade constitucional das normas do Marco Civil que amparam a privacidade e preveem a sanção de suspensão foram colocadas a partir dessas decisões. Noutras palavras, **a presente controvérsia emerge efetivamente a partir de decisões judiciais: trata-se, portanto, de investigar, nos termos do art. 7º, II, do Marco Civil da Internet, os limites da decisão judicial que restringe o direito à privacidade**. Há, portanto, ato do poder público que, de forma geral e ampla, vulnera, ao menos no que alega o Partido, preceito fundamental.

Por fim, embora não tenha sido suscitada, cumpre indicar que a controvérsia judicial não é só aferível por decisões que tenham sido proferidas em diversas unidades da federação, mas também porque, em grau recursal, como se depreende da decisão do Tribunal de Justiça de Sergipe (eDOC 29), há também disputas. Ademais, ainda que seja controverso o sentido de preceito fundamental, é indene de dúvidas, ao menos no âmbito da jurisprudência deste Tribunal, que os direitos fundamentais amoldam-se ao parâmetro de controle para fins de cabimento da arguição.

Rejeito, portanto, a alegação e passo ao exame do mérito da arguição.

Alegações das Partes sobre o Mérito

Alegações do Partido requerente

O Cidadania alega que as decisões judiciais citadas em sua manifestação violam o direito à comunicação, previsto no art. 5º, IX, da CRFB, porquanto aplicam desproporcionalmente a sanção prevista em lei. Aponta que o direito à comunicação é preceito fundamental, razão pela qual, em seu entender, dever-se-ia julgar procedente a arguição, a fim de impedir a suspensão do aplicativo de mensagens *Whatsapp* por qualquer decisão judicial.

A decisão proferida pelo douto Juízo da Comarca de Lagarto, trazida pelo partido como exemplo da violação, foi assim fundamentada (eDOC 23, *sic*):

> "7. Do que se depreende do autos é necessário perquirir, de plano, sobre as razões pelas quais a suspensão por 72h requerida poderia contribuir para o desbaratamento da organização criminosa. A princípio, a simples suspensão poderia ser incompatível com o que se visa, vale dizer, a colheita de elementos de prova a fim de incorporação aos outros já constantes, uma vez que a própria suspensão inviabilizaria a comunicação das mensagens, vídeos ou gravações de voz, entre os componentes daquela organização criminosa;
>
> 8. Numa análise precipitada, pensar-se-ia que este raciocínio encontraria guarida na aparente contradição. Mas o que se pretende, por aquela Autoridade Policial Federal, seria mais uma vez, que medidas de coerção façam com que aquela Empresa respeite o ordenamento jurídico nacional;
>
> 9. Sendo assim, e vencido este primeiro ponto, analisa-se, exaustivamente, o tema apresentado, por dever de ofício e

como sempre feito por este Juiz de Direito.

10. Arremeta-se, de início, que este caso em concreto diz respeito a um enfrentamento entre a Supremacia do Interesse Público frente ao Interesse Privado e os limites daquela, incursionando-se, também, no direito de privacidade, de matriz constitucional;

11. A finalidade da existência estatal não e outra que diversa de si mesma. Pretende-se, através do Princípio basilar do Direito Administrativo da Supremacia do Interesse Público, regrar a própria atividade do Estado;

12. O que se pretende é a tutela dos interesses primários, vale dizer, que deitam berço nos Princípios Fundamentais que são a razão de existir do Estado. Este deve impor ao cidadão, antigamente chamado de 'administrado' e, sob algumas condições, uma limitação da sua atuação. Vale dizer, o interesse público resguarda, na verdade, o interesse privado. Garante-se, então, a ordem social em benefício de uma coletividade;

13. Assim, o interesse privado pode ser mitigado quando o que se pretende é garantir os direitos fundamentais, tendo em vista a garantia da ordem social. Em que pese o direito à privacidade, sabe-se que nenhum dos direitos fundamentais é absoluto, inclusive, o da vida, emc aso de guerra externa declarada, artigo 5º, inciso XLVII, da CF/88;

14. Mas o que se apresenta nesta esfera criminal? Um grupo poderoso e organizado voltado a práticas criminosas de tráfico interestadual de drogas (e competência da Justiça Estadual, e não da Justiça Federal, ainda que o requerimento que se aprecia seja de autoria de um Delegado Federal, o que, por si s´, não desloca competência alguma para aquela), continua a executar suas ações voltadas à macrocriminalidade. Diante disso, foi requerida a suspensão temporária de um serviço de aplicativo oferecido pela representada Facebook de nome 'WhatsApp' por ser utilizado pelos componentes daquela considerando que todas as outras medidas anteriores, no caso presente e cujos autos encontram-se em apenso, não foram cumpridas;

15. É de conhecimento geral os grandes benefícios trazidos ao mundo contemporâneo pela tecnologia da informática, mormente, no caso concreto, aos apreciadores do aplicativo guerreado chamado de 'WhatsApp', ou, para alguns, simplesmente de "zap". Através deste possibilita-se infindáveis comunicações entre pessoas, quer entre físicas ou jurídicas, entre si, por assim dizer. Acredita-se que bilhões de pessoas físicas, ao redor do mundo, desfrutam desta preciosidade criada por mentes privilegiadas e que merecem respeito e admiração. É o ser humano servido do dom da inteligência para se aproximar de tantos outros por diversos e quaisquer motivos, inclusive para praticar atos condenáveis e criminosos;

16. No entanto, não se mostram razoável a rebeldia daquela Empresa em querer impor uma desobediência confessa à legislação nacional. Mantendo-se neste comportamento arredio aloca-se na ilegalidade. Ou seja, encontra-se em território brasileiro atuando ilegalmente, sob os olhares inertes de quem dever/poder de vigilância deveria ser exercido a fim de obstar o desrespeito provocador de uma Empresa que se arvora em descumprir as ordens de diversos Juízos no território brasileiro, levando este Magistrado a determinar a prisão do seu Vice-Presidente para a América Latina, em data muito recente. Aqui, não se atribui ao Facebook a responsabilidade direta por uma organização criminosa, pelo que se apresenta. Mas, diante de sua recalcitrância inconcebível, contribui para tanto, por razões **UNICAMENTE** comerciais e seu desejo, legal, de lucros bilionários. A conhecida 'febre do ouro';

17 . Apesar dos esforços deste Juízo Criminal, e de outros no Brasil, em fazer com que se cumpram as determinações judiciais, permanece a Empresa Facebook a zombar do Poder Judiciário brasileiro num achincalhe que se perpetua até a presente data e que não conta com qualquer inércia deste Magistrado e nenhum neste território brasileiro. Ao revés, analisa-se novo requerimento, cuja consequência deve ser refletiva em milhões de usuários que são utilizados como 'massa-de-manobra' e como 'escudo' pela Facebook, a qual não

se importa absolutamente com pretenso direito à privacidade absoluta – e que não encontra guarida constitucional – de quem quer que age, mas, apenas e tão-somente, de 'vender' a ideia de que é impossível serem interceptadas as mensagens ou vídeos desfilados em seu aplicativo, já que, assim, resguardaria o valor de suas ações na Nasdaq, principalmente;

18. Após a prisão do sempre lembrado Vice-Presidente da América Latina, por coincidência ou não, agora pretende convencer a todos que aqueles estariam protegidos pela criptografia 'end to end', o que impossibilitaria qualquer controle por parte da Empresa e, também, de qualquer Autoridade competente em lograr êxito em investigações criminais;

19. **Segundo documento acostado aos autos, fls. 14/7, pela Autoridade Policial Federal**, "...As investigações policiais... continuam impedidas de prosseguimento, considerando a resistência dos representantes da empresa Facebook... no que tange a interceptação de comunicações entre os alvos investigados... A interceptação de mensagens... em tempo real, devidamente descriptografas, se faz essencial para a atuação do estado... dispensando o aprofundamento de maiores comentários sobre o prejuízo que toda a sociedade sofre com tal resistência da empresa Facebook em cumprir as determinações judicias sob os mais variados argumentos, vários deles até mesmo de sinceridade duvidosa... a possibilidade técnica do aplicativo em transmitir tais dados em tempo real para os órgãos de investigação quando instados judicialmente, não resta dúvida de sua possibilidade... foi solicitado o espelhamento de tais mensagens em tempo real... a fim de dar seguimento às investigações, como decorre normalmente uma interceptação de comunicações telefônicas e de mensagens SMS... em nenhum momento foram solicitadas mensagens pretéritas... entre os vários e rasos argumentos amplamente divulgados pela empresa... está a impossibilidade de espelhamento de tais diálogos, o que novamente não condiz com a realidade, basta verificar a ferramenta de envio de

diálogos via email e a opção do Whatsapp Web, onde o usuário do sistema pode ter acesso ao seu aplicativo em um computador da mesma forma que em seu Smartphone. Outra questão muito divulgada pelos representantes do Whatsapp é a impossibilidade encaminhar tais mensagens devidamente descriptografadas, sendo tal argumento novamente desmascarado considerando que foi a própria empresa a responsável em produzir o sistema, não sendo razoável esperar que a criatura supere o criador e se transforme em um sistema autônomo em que a própria empresa desconheça sua engenharia de programação... a legislação nacional é clara... Exemplo do que estamos falando foi o comportamento da empresa detentora do sistema Blackberry, que explora o ramos (...) de comunicações criptografadas... direcionando em tempo real as comunicações de indivíduos investigados... mundialmente conhecido por sua integridade e segurança...";

(...)

22. Mas o que é a criptografia? Nada mais que uma técnica de codificação de informações utilizável entre emissor e receptor para que suas comunicações não sejam captadas por estranhos de modo compreensível, sendo possível reverter com o emprego das chamadas "chaves", conjunto de bit's sob o manto de algoritmos e que possibilita a modificação do próprio algoritmo de encriptação. Vale dizer, não passa de uma forma de alterar transformando as informações, ditas legíveis, em espécies de códigos específicos e que, depois, serão decodificados por outros leitores que são capazes de reconhecer e interpretar esses mesmo códigos. Ademais, a tão invocada criptografia de há muito é utilizada no mundo comercial: serviços bancários, empresas de cartões de créditos, e-commerce, serviços de mensagens e nem por isso as ordens judiciais de entrega de dados quaisquer inviabilizou esses serviços, ao contrário, elevam-se a sua confiança. Portanto, do que se verifica, a Empresa Facebook atesta a possibilidade de disponibilizar o que se exige;

(...)

24. Não se imagina que uma investigação criminal de tráfico interestadual de drogas, abrangente no território nacional em vários Estados, seja impedida de ter a sua continuidade por (ir)responsabilidade de uma bilionária empresa com fins meramente comerciais em detrimento da soberania nacional;

25. Medidas que tais, de suspensão de serviço em que uma coletividade seja atingida, certamente traria em seu bojo o desconforto e a revolta de consumidores. No entanto, e como já dito, conta de modo bastante cômodo a Facebook com a revolta de milhões de brasileiros que seriam atingidos, não necessitando esta de maiores esforços para continuar a descumprir ordens judicias, bastante aguardar, nas sombras, a repercussão do caso e seus supostos admiradores, tudo fruto de uma sociedade extremamente individualizada existente nesta nação brasileira. Este Magistrado determinou a prisão do representante da Facebook no Brasil e arbitrou, anteriormente a isso e para evitá-la, (embora obrigado a isso não estivesse, ao contrário do que entendem alguns operadores do direito, já que os requisitos e pressupostos de uma prisão preventiva, artigo 312 do Código de Processo Penal, não guarda qualquer relação de estipulação de multas, astraintes ou coisa que o valha) multas de até R$ 1.000.000,00 (um milhão) de reais/dia, e que, no momento, foram suspensas por determinação de uma liminar em sede de Mandado de Segurança, cujo mérito também não foi julgado. Ora, efetivamente, tendo sido preso o Vice-Presidente da América Latina (e solto) por pretensa tipificação no artigo 2º, parágrafo 1º, da Lei das Organizações Criminosas (e não por tipificação suspostamente por crime de desobediência, pois se assim entendesse, não teria cabido a decretação de prisão preventiva, já que esta somente pode ser decretada, por assim afirmar, para crimes dolosos cuja pena máxima privativa de liberdade extrapolem o patamar de 04 (quatro anos) e os bloqueios suspensos, além de impedimento de serem arbitradas novas multas com valores acrescidos, em sede de liminar de mandado de segurança, pergunta-se: "E aí"?

Que providência a serem tomadas? Quedar-se na inércia? Compartilhar com a recalcitrância da Facebook e colaborar com os criminosos? Alinhar-se na fila da crise de autoridade vivida neste país?

26. Afirmou-se, em **Decisão recente e extremamente educada, do Tribunal de Justiça do Estado de São Paulo**, em caso notório da Comarca de São Bernardo do Campo/SP, e semelhante a este apreciado, de que seria desproporcional e desarrazoado manter-se a suspensão, pois atingiria milhões de usuários. E que seria possível elevar-se o valor da multa aplicada para conseguir-se o que se ainda é pretendido. Ocorre que, além do caso aqui presente ser impossível elevar-se a multa já arbitrada diante de uma liminar que proíbe qualquer novo bloqueio de novos valores e de estipulação de novas multas, aos olhos deste Juiz de Direito, o desconforto é patrocinado pela própria representada, vale dizer, a Facebook, por não querer se submeter à legislação nacional, zombando, repita-se à exaustão, do Estado brasileiro. Aliás, assim se comporta mundo a fora, até que alguma Instância jurídica superior ou máxima mude seu entendimento em casos que tais, já que, continuando a assim proceder, encontrar-se-ia aquela operando no território nacional de modo ilegal, podendo gerar, inclusive, coações de maior grau em outros Juízos nesse País;

(...)

28. O aplicativo conhecido como 'WhatsApp' (de propriedade da empresa do mesmo nome e de sua controladora mundial, a Facebook Inc. e no Brasil representada pela Facebook Serviços On Line do Brasil Ltda), bem como a própria **Facebook não são sinônimos de Internet.** Internet, como sabido, vai muito, muito mais além. Estas Empresas servem-se, apenas e tão-somente desta para seus objetivos quaisquer que sejam. Por acaso o serviço oferecido pela Facebook e pela WhatsApp são considerados essenciais, pela legislação brasileira? É evidente que não. Nem aqui e nem além-mar. A par do desconforto e do comodismo, nossos serviços essenciais deixariam de ser oferecidos com possível suspensão temporária

ou definitiva de seus serviços?É evidente que não. Estariam a Facebook e a WhatsApp acima da lei? É evidente que não. Portanto, por que quedar-se inerte contribuindo para a perpetuação dos agentes criminosos? Seria razoável e proporcional desrespeitar-se o ordenamento jurídico deste País? É evidente que não;

28. Suposto perigo de dano irreparável para usuários do referido aplicativo seria alegado, certamente, por quem interessa em permanecer descumprindo a lei brasileira. Ora, tese como esta e outras mais que seriam certamente alegadas em sede própria, não mais do que qualificaria o uso que a Facebook faz de seus milhões de usuários neste país, pois lhe é bastante confortável fazê-lo, diante de abalizadas Decisões – até o momento, contrárias aos Juízdos do 1º grau – de Instância superiores do 2º grau. Ou seja, invocar e transformar seus clientes em verdadeiros 'escudos humanos' e que servem de 'cobertores' para seus interesses, diante de uma sociedade individualizada e de pensamento individualista';

(...)

32. Afiance-se que o aplicativo 'WhatsApp' não é o único utilizado neste país. Muitos outros existem e são utilizados tais como 'Viber', 'Hangouts', 'Skyper', 'Kakaotalk', 'Line', 'Kik Messenger', 'Wechat', 'GrupMe', 'Facebook Messenger', 'Telegram'. Todos, com possibilidade, dentro do seu desenvolvimento, de suprirem possível suspensão do 'zap'. O 'WhatsApp' é mais um, não o único. Ainda que fosse, não se mostra razoável que colabore, de modo indireto, com organizações criminosas;

33. Outra análise a ser enfrentada é que a Facebook não seria a responsável pela má utilização do seu aplicativo e, assim, estaria tendo direito violado. Pois bem. Sabe-se que o risco econômico é do empreendedor e cabe a este impedir que seus serviços sejam utilizados para atividades ilegais, e, quando impossível pela própria natureza humana, que sejam levados a curvarem-se diante das leis e a colaborar com as autoridades do País em que deita seus p´s a fim de auferir seus lucros

bilionários;

34. É risível alegar-se violência de privacidade de usuários. Afirma-se isto porquanto para que qualquer pessoa possa utilizar esses dispositivos do mundo virtual, necessário 'clicar' no chamado **'ACEITE'** e que, salvo alguém curioso ao extremo, via de regra ninguém se dispõe a ler as condições impostas. Pois se assim o fizer e não concordar, acesso não terá ao que pretende. Típico caso de pura hipocrisia... essas Empresas, tais como a representada, possuem acesso e sabem em seus arquivos, ainda que os usuários não queiram de fato – e não de direito, embora possua lastro em contrato de adesão –, sobre seus costumes, hábitos, horários de acessos, IP, o que compram, o que vendem, o que os contrariam, seus provedores, navegadores, sistemas operacionais e etc, etc, etc, vendendo essas informações preciosas a tantas outras Empresas e que desenvolvem seus produtos baseado nessas informações, impondo usos e costumes a inúmeras pessoas menos desavisadas, devastando, na verdade, as privacidades e intimidades do alheio, ou seja, seus dados confidenciais;

(...)

40. A Lei do Marco Civil da Internet, em seu artigo 10, cabeça, impõe que:

(...)

42. Logo, três considerações:

A uma, é a auasência de regulamentação de determinados artigos ou parágrafos aqui utilizados para embasar esta Decisão. Em que pese opiniões respeitadas em contrário, a ausência de um regulamento não possui o condão de revogar leis ou mantê-las suspensas quanto a sua vigência e aplicabilidade. Se regulamento não há, aplica-se a lei, tal e qual;

A duas, quis o legislador que, no parágrafo quarto, do artigo 15, da Lei do Marco Civil da Internet, o Poder Judiciário, através de seus Membros melhor Decisão prolatasse, balizada pelos parâmetros anotados legalmente, não havendo sanção previamente estabelecida legalmente expressa;

A três, pretendeu-se a interceptação das mensagens, vale

dizer, tempo real tais como as interceptações telefônicas.

Pois bem.

A Empresa Facebook, através de seu Representante, recusa-se, a não mais caber, a cumprir a legislação brasileira aqui, neste Estado e em todo o território brasileiro, sabe-se lá até quando, em diversas ocasiões, demonstrando seus antecedentes e reincidências.

Arbitradas multas de até R$ 1.000.000,00 (um milhão) de reais/dias, pouco caso fez, mantendo-se em linear e solene silêncio. Decretadas a prisão daquele, permaneceu com a mesma atitude, após este haver sido solto, pois beneficiado de uma liminar em sede de habeas corpus. E até esta data, em seu silêncio permanece, apostando em sua rebeldia. A **natureza e a gravidade** da infração é patente: violação à soberania nacional, desrespeitando todo o ordenamento jurídico do Brasil. O caso se reporta ao tráfico interestadual de drogas, nas espécies de cocaína e maconha, considerando **circunstância agravante** o fato das investigações continuarem impedidas de serem continuadas.

Aufere vantagem econômica, já que mantendo seu comportamento, engrandece a que se destina, multiplicando valores enormes das suas ações em bolsas de valores ao redor do mundo, convencendo – não se sabe até quando – de que seu aplicativo é inviolável, ainda que sob ordens judiciais de um Estado que pretende ser Soberano. Ora, quanto mais alguém acreditar que a sua criptografia, qualquer que seja, é indevassável, maior número conquistado de usuários e, como dito, o próprio valor de suas ações em mercado financeiro seria mantido em patamar elevado e estável.

Finalmente, os danos são, da mesma forma, patentes. De modo indireto, contribui para a criminalidade existente neste País, para somente aqui se referir. É que não há uma pessoa vivia que não saiba que é possível utilizar-se deste aplicativo e desta Empresa para perpetuar o tráfico de drogas, de armas, crimes de pedofilia, extorsões, passaportes falsos, e tantos outros de cujas mazelas ressentem-se as famílias brasileiras e o

sistema de saúde nacional, sob a falsa certeza de que não terão, mesmo em casos ressalvados pela Constituição e legislação inferior, suas intimidades e privacidades mitigadas em benefício de uma coletividade, através de uso criminoso de uma plataforma virtual como aqui se analisa;

43. A Empresa Facebook do Brasil já foi advertida por este Juízo Criminal, processo de interceptação de dados em tempo real, posteriormente houve o arbitramento de multas, primeiramente no montante de R$ 50.000,00 (cinquenta mil reais/dia, após novos descumprimento elevou-se para R$ 1.000.000,00 (um milhão de reais)/dia, al´m da ordem de prisão do seu Representante-mor na América Latina e, portanto, do Brasil (artigo 12, incisos I e II, da lei comentada), obedecendo-se a uma escala de coações permitidas na legislação;

(...)

49. Portanto, por tudo que foi exposto, e não por outras razões, devidamente fundamentado, nos artigos 10, 11, 12, 13 e 15, e seus parágrafos, da Lei 12.965/2014, hei por bem **DEFERIR** a **SUSPENSÃOS** do aplicativo **'WhatsApp'**, de propriedade da WhatsApp e de sua controladora Facebook Inc, no Brasil representada pela Facebook Serviços On Line do Brasil Ltda, sediada em São Paulo/Capital, **pelo prazo de 72h,** ***determinando às Operadoras de Telefonia*** **TIM, VIVO, OI, CLARO, NEXTEL E TELEFÔNICA, que cumpra esta Decisão,** ***suspendendo temporariamente o tráfego de qualquer dado do aplicativo 'WhatsApp' (quer sejam em todos as suas funções de texto, mídia e voz) em seus sistemas de telefonia/internet, também o tráfego de dados por meio dos domínios whatsapp.net e whatspp.com, bem como todosos seus subdomínios e todos os outros domínios que porventura contenham whatsapp.net e whatsapp.com em seus nomes anotados, além de efetuar o bloqueio, logicamente, pelo endereço do whatsApp na rede mundial de computadores de internet para que seja impedida a utilização do citado aplicativo pelas conexões móveis e pelo 'wi fi e, ainda, todos os números de IP que estejam vinculados aos domínios e***

> ***subdomínios, inclusive limpeza de cache daqueles domínios, explicitando-se para que esta Decisão seja cumprida em sua inteireza,*** **sob pena de desobediência e pagamento de multa de R$ 500.000,00 (quinhentos mil reais), cada, por dia de descumprimento."**

Os artigos invocados pelo douto juízo têm o seguinte teor:

> "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 .
>
> § 2º O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7º .
>
> § 3º O disposto no **caput** não impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição.
>
> § 4º As medidas e os procedimentos de segurança e de sigilo devem ser informados pelo responsável pela provisão de serviços de forma clara e atender a padrões definidos em regulamento, respeitado seu direito de confidencialidade quanto a segredos empresariais.
>
> Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de

comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.

§ 1º O disposto no **caput** aplica-se aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil.

§ 2º O disposto no **caput** aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil.

§ 3º Os provedores de conexão e de aplicações de internet deverão prestar, na forma da regulamentação, informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações.

§ 4º Decreto regulamentará o procedimento para apuração de infrações ao disposto neste artigo.

Art. 12. Sem prejuízo das demais sanções cíveis, criminais ou administrativas, as infrações às normas previstas nos arts. 10 e 11 ficam sujeitas, conforme o caso, às seguintes sanções, aplicadas de forma isolada ou cumulativa:

I - advertência, com indicação de prazo para adoção de medidas corretivas;

II - multa de até 10% (dez por cento) do faturamento do grupo econômico no Brasil no seu último exercício, excluídos os tributos, considerados a condição econômica do infrator e o princípio da proporcionalidade entre a gravidade da falta e a intensidade da sanção;

III - suspensão temporária das atividades que envolvam os atos previstos no art. 11; ou

IV - proibição de exercício das atividades que envolvam os atos previstos no art. 11.

Parágrafo único. Tratando-se de empresa estrangeira, responde solidariamente pelo pagamento da multa de que trata o **caput** sua filial, sucursal, escritório ou estabelecimento situado no País.

Art. 13. Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento.

§ 1º A responsabilidade pela manutenção dos registros de conexão não poderá ser transferida a terceiros.

§ 2º A autoridade policial ou administrativa ou o Ministério Público poderá requerer cautelarmente que os registros de conexão sejam guardados por prazo superior ao previsto no **caput.**

§ 3º Na hipótese do § 2º , a autoridade requerente terá o prazo de 60 (sessenta) dias, contados a partir do requerimento, para ingressar com o pedido de autorização judicial de acesso aos registros previstos no **caput.**

§ 4º O provedor responsável pela guarda dos registros deverá manter sigilo em relação ao requerimento previsto no § 2º , que perderá sua eficácia caso o pedido de autorização judicial seja indeferido ou não tenha sido protocolado no prazo previsto no § 3º .

§ 5º Em qualquer hipótese, a disponibilização ao requerente dos registros de que trata este artigo deverá ser precedida de autorização judicial, conforme disposto na Seção IV deste Capítulo.

§ 6º Na aplicação de sanções pelo descumprimento ao disposto neste artigo, serão considerados a natureza e a gravidade da infração, os danos dela resultantes, eventual vantagem auferida pelo infrator, as circunstâncias agravantes, os antecedentes do infrator e a reincidência.

(...)

Art. 15. O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de

> forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento.
>
> § 1º Ordem judicial poderá obrigar, por tempo certo, os provedores de aplicações de internet que não estão sujeitos ao disposto no **caput** a guardarem registros de acesso a aplicações de internet, desde que se trate de registros relativos a fatos específicos em período determinado.
>
> § 2º A autoridade policial ou administrativa ou o Ministério Público poderão requerer cautelarmente a qualquer provedor de aplicações de internet que os registros de acesso a aplicações de internet sejam guardados, inclusive por prazo superior ao previsto no **caput,** observado o disposto nos §§ 3º e 4º do art. 13.
>
> § 3º Em qualquer hipótese, a disponibilização ao requerente dos registros de que trata este artigo deverá ser precedida de autorização judicial, conforme disposto na Seção IV deste Capítulo.
>
> § 4º Na aplicação de sanções pelo descumprimento ao disposto neste artigo, serão considerados a natureza e a gravidade da infração, os danos dela resultantes, eventual vantagem auferida pelo infrator, as circunstâncias agravantes, os antecedentes do infrator e a reincidência."

Em face dessa decisão foi impetrado um mandado de segurança, no qual se alegou teratologia da decisão. Em regime de plantão, a liminar foi indeferida. As razões trazidas para o indeferimento foram as seguintes (eDOC 29):

> "Analisando o conjunto probatório dos autos, não visualizo teratologia ou ilegalidade na decisão combatida. Senão vejamos.
>
> Cuidam os autos sobre irresignação mandamental em face da decisão do Juiz de Direito da Vara Criminal da Comarca de Lagarto que determinou a suspensão do aplicativo

"Whatsapp", de propriedade da Whatsapp e de sua controladora Facebook Inc, pelo prazo de 72 (setenta e duas) horas, com ordem para que as operadoras de telefonia suspendessem temporariamente o tráfego de qualquer dado do referido aplicativo, a fim de impedir a sua utilização por qualquer meio.

Compulsando os autos, verifica-se que a decisão combatida foi prolatada em processo criminal que apura suposta prática de crime de tráfico interestadual de drogas, e a justificativa da medida foi justamente a necessidade de interceptação de comunicações enviadas via Whatsapp, diante da comprovada utilização do aplicativo, oferecido pela representada Facebook, pelos componentes da organização criminosa, consignando que todas as outras medidas anteriores não foram cumpridas.

I – DA ALEGADA DESPROPORCIONALIDADE DA DECISÃO

O primeiro argumento da empresa impetrante é a suposta desproporcionalidade da decisão, pois, no seu entender, a suspensão do serviço utilizado por dezenas de milhões de usuários no Brasil foi motivada pela utilidade prática advinda da interceptação de "apenas 36 números de telefonia celular".

A meu ver, a empresa impetrante vale-se da alegação de que deve resguardar o direito à privacidade dos usuários do aplicativo para refutar a ordem judicial, encobrindo o interesse patrimonial da Empresa Facebook.

Em verdade, o direito à privacidade dos usuários do aplicativo encontra-se em conflito aparente com o direito à segurança pública e à livre atuação da Polícia Federal e do Poder Judiciário na apuração de delitos, em favor de toda a sociedade.

Ora, segundo o art. 144, da Constituição Federal, "a segurança pública, dever do Estado, direito e responsabilidade de todos, é exercida para a preservação da ordem pública e da incolumidade das pessoas e do patrimônio."

(...)

Assim sendo, pode-se concluir, de acordo com o posicionamento do Supremo Tribunal Federal, que a superação de antagonismos existentes entre direitos fundamentais resolve-se, em cada situação ocorrente, pelo método da ponderação concreta de interesses, cabendo ao Poder Judiciário, mediante ponderada avaliação das prerrogativas constitucionais em conflito, definir, em cada situação ocorrente, uma vez configurado esse contexto de tensão dialética, a liberdade que deve prevalecer no caso concreto.

Tendo-se tal preceito em mente, neste primeiro momento, percebo que a impetrante, em verdade, minimiza a importância da investigação criminal de componentes de organização criminosa que utilizam o aplicativo em questão, escamoteando a gravidade do delito supostamente praticado (tráfico interestadual de drogas), sob a pecha de garantir o direito à intimidade de seus usuários.

Ora, o uso do aplicativo por quem quer que seja e para qualquer fim não pode ser tolerado sem ressalvas. Deve, sim, sofrer restrição quando atinge outros direitos constitucionalmente garantidos, como no caso em comento.

(...)

Desse modo, o caso em tela vai muito além do que a interceptação de "apenas 36 números de telefonia celular". Na hipótese dos autos, vejo que está em jogo a ordem social e o direito à segurança de toda uma sociedade.

Convém ressaltar que outras medidas anteriores foram determinadas, visando ao acesso à interceptação da comunicação, em tempo real, pelo aplicativo, entre os investigados, a exemplo da aplicação de multas diárias, posteriormente majoradas, em desfavor da empresa reincidente, culminando com a ordem de prisão do seu Vice-Presidente na América Latina, Sr. Diego Jorge Dzordan, reformada em sede de liminar de habeas corpus, ainda pendente de julgamento definitivo. Porém, todas sem o êxito pretendido.

Assim, está claro que o Poder Judiciário não pode ficar de mãos atadas frente à resistência de empresas internacionais, com atuação no território brasileiro, em cumprir ordens judiciais legitimamente emanadas.

Ademais, é indubitável a relevância do aplicativo para as mais diversas atividades do cotidiano. Porém, repita-se, há direitos e princípios constitucionais que devem ser prestigiados, visando, sempre, ao bem comum.

II – DA ALEGADA AUSÊNCIA DE PREVISÃO LEGAL PARA SUSPENSÃO

Já no tocante à alegação de que inexiste previsão legal apta a autorizar a suspensão do Whatsapp, tenho que não se sustenta.

A Lei nº 12.965, de 23 de abril de 2014, mais conhecida como o "Marco Civil da Internet", foi criada em virtude do crescente aumento das comunicações pela rede e estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil.

O art. 12 prevê a suspensão temporária das atividades que envolvam os atos previstos no art. 11, segundo o qual, "em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros."

Numa interpretação sistemática de seus dispositivos, deve-se admitir a suspensão do serviço não só quando o próprio aplicativo descuida da privacidade das comunicações e dados de quem o utiliza, mas também quando existe risco à segurança de todos os usuários.

Por oportuno, transcrevo dispositivos da referida legislação que autorizam a violabilidade das comunicações, desde que amparadas em ordem judicial, como no caso em testilha:

(...)

Nesse diapasão, tenho que a decisão objurgada não ofende o Marco Civil da Internet. Pelo contrário, a aludida legislação dá suporte à medida imposta.

Inclusive, a Lei de Interceptação Telefônica (nº 9296/96), desde 1996, já previa a possibilidade de se impor a quebra do sigilo das comunicações telefônicas, de informática e de telemática. (art. 1º, e seu parágrafo 1º)

Ora, ao se suspender a comunicação via Whatsapp, força-se a utilização, pelos investigados, de ligações telefônicas, cuja quebra é autorizada para fins de prova em investigação criminal e em instrução processual penal, dependendo de ordem do juiz competente da ação principal, como foi no caso em análise, em que a sua realização mostrou-se necessária à apuração da infração.

Por certo que a decisão ora impugnada vai desagradar a maioria dos brasileiros, que desconhecem os reais motivos de sua prolação. Porém, deve-se considerar que existem inúmeros outros aplicativos com funções semelhantes à do Whatsapp, a exemplo daqueles citados pelo julgador de primeiro grau (Viber, Hangouts, Skype, Kakaotalk Line, Kik Messenger, Wechat, GroupMe, Facebook Messenger, Telegram etc).

Além disso, o juiz não pode decidir contra a ordem jurídica, pensando apenas em agradar a determinados setores da sociedade. Deve, sim, pautar seu ofício no cumprimento do nosso ordenamento, nem que para isso seja preciso adotar medidas, à primeira vista, impopulares.

III – DA IMPOSSIBILIDADE JURÍDICA DE SE DETERMINAR A INTERCEPTAÇÃO DE CONTEÚDO.

Equivoca-se a parte impetrante ao alegar discricionariedade ampla e restrita do juiz para autorizar a quebra de comunicações pela internet.

(...)

Compulsando os autos, nota-se que a decisão refutada foi fundamentada no Estado Democrático de Direito e nos Direitos Fundamentais. Outro equívoco há em mencionar 'quebra

indiscriminada' de sigilo das comunicações.

Observa-se que a quebra de dados refere-se a usuários estritamente especificados, trinta e seis usuários, para apuração de crimes previstos na Lei Federal nº 11.343/2006 e na Lei Federal nº 12.850/2013.

O impetrante suscitou os incisos X e XII do art. 5º da Constituição Federal espelhados pelos incisos I, II e III do Marco Civil da Internet que tutelam direito à privacidade.

Entretanto, a própria Lei do Marco Civil da Internet traz a possibilidade de o provedor de internet responsável disponibilizar os registros de conexão e acesso, bem como, o conteúdo das comunicações, com previsão nos parágrafos §1º e §2º do art. 10.

Ademais, os princípios constitucionais da intimidade, vida privada, honra, e imagem, bem como, sigilo da correspondência e comunicações, não podem se sobrepor aos objetivos fundamentais da República Federativa do Brasil nem aos seus princípios.

Assim, os direitos individuais não podem servir como salvo-conduto para violação de outros direitos, como o direito à vida, à integridade física, à saúde, e à segurança pública.

A República Federativa do Brasil tem como um dos objetivos construir uma sociedade livre, justa e solidária, possuindo como um dos princípios a prevalência dos direitos humanos.

Dessa forma, como já afirmado, não há que se falar em medida desproporcional ou prejudicial à privacidade, sem fundamento legal, e de caráter antijurídico, uma vez que a supremacia do interesse público na salvaguarda de direitos de toda a sociedade à vida, à liberdade, à segurança pública devem prevalecer.

Não obstante a alegação de que a decisão fere a livre iniciativa constitucional, prevista no art. 170, caput, da CF, obrigando a impetrante mudar seus padrões técnicos de operação, não fez ela prova nesse sentido Se a própria impetrante cria um sistema de criptografia, não é crível que a

mesma seja incapaz de ter acesso a essas 'chaves', não trazendo fundamento técnico para refutar a decisão combatida.

(...)

IV - DA AD IMPOSSIBILITA NEMO TENETUR

(...)

A decisão combatida é suficientemente clara ao dispor que não se refere a dados pretéritos, mas a dados em tempo real: (...)

A quantidade de usuários dos serviços, aproximadamente 1 bilhão de pessoas, também não é motivo razoável para não cumprimento da ordem judicial, se tal pleito somente refere-se a trinta e seis usuários, estando todos identificados. Refutados, portanto, os argumentos de obrigação de cumprimento impossível.

V – DA ALEGADA INEXISTENCIA DE DESCUMPRIMENTO DE ORDEM JUDICIAL

No tocante à inexistência de descumprimento de ordem judicial, em razão da impetrante jamais ter sido destinatária do comando judicial, melhor sorte não amparo o pleito do impetrante.

Como bem se observa do site wikipédia, o Whatsapp é empresa subsididiária do Facebook, juntamente com Oculus, VR, PrivateCore e Instagram.

Estas compõem um poderoso Grupo Econômico Cibernético, sendo responsáveis pelos atos praticados em desconformidade com a legislação brasileira.

Observa-se, no caso, que já era conhecimento da impetrante as ordens judiciais para interceptação de dados telemáticos do Whatsapp, como ocorreu no arbitramento da multa e na prisão do Vice-Presidente do Facebook.

Portanto, não há que se falar em desconhecimento ou ausência de notificação do impetrante, pois as ordens anteriores da autoridade coatora sempre direcionaram em ter acesso a dados telemáticos de determinadas contas.

VI – DA CRIPTOGRAFIA

Por fim, a criptografia também não é empecilho para o cumprimento da ordem judicial prolatada pela autoridade

coatora.

Como já elucidado na decisão combatida, a criptografia seria um conjunto de técnicas para esconder informação de acesso não autorizado.

Ocorre que a criptografia não é justificativa para não fornecer os dados telemáticos requeridos no procedimento criminal.

Isso é o que se extrai das informações técnicas prestadas pela autoridade policial Renato Beni da Silva: (....).

Destarte, observa-se a recalcitrância do Wathsapp em colaborar com as investigações criminais, fatos que já ocorreram com a Google e a Blackberry, mas que foram obrigadas a respeitar as leis brasileiras.

Apesar de toda a argumentação da impetrante sobre sua preocupação na segurança de informações que tramitam em seus aplicativos, através de protocolos de criptografia, valho-me das palavras do magistrado de primeiro grau, que ressaltou: (...).

Outrossim, verifica-se da manifestação da autoridade policial a possibilidade de espelhamento das mensagens expedidas pelos usuários, com a duplicação do número receptor, técnica que possibilitaria que as mensagens chegassem aos celulares dos envolvidos, como também no número duplicado. Isso não resultaria em quebra de criptografia.

Enfim, as possibilidades técnicas são as mais diversas, e há de ressaltar-se que o aplicativo, mesmo diante de um problema de tal magnitude, que já se arrasta desde o ano de 2015, e que podia impactar sobre milhões de usuários como ele mesmo afirma, nunca se sensibilizou em enviar especialistas para discutir com o magistrado e com as autoridades policiais interessadas sobre a viabilidade ou não da execução da medida. Preferiu a inércia, quiçá para causar o caos, e, com isso, pressionar o Judiciário a concordar com a sua vontade em não se submeter à legislação brasileira.

VII – CONCLUSÃO

Desta forma, não vislumbrando a plausibilidade jurídica a

> amparar o deferimento da medida antecipatória perseguida, denego a liminar pleiteada na inicial."

Já a decisão proferida pelo douto Juízo da 2ª Vara Criminal da Comarca de Duque de Caxias assim fundamentou sua decisão (eDOC 35):

> "Trata-se de representação da d. autoridade policial da 62ª DP, ratificada pelo Ministério Público, dando conta de que a determinação deste Juízo para a interceptação telemática das mensagens compartilhadas no aplicativo Whatsapp, pertencente ao Facebook Serviços Online do Brasil, não foi cumprida, requerendo, assim, as medidas legais cabíveis para o efetivo cumprimento da ordem.
>
> Tendo em vista que se trata de procedimento sigiloso, tendo em vista, ainda, que as decisões proferidas recentemente referentes ao aplicativo Whatsapp causaram certa indignação da sociedade, a fim de garantir a todos que serão afetados por este decisum o direito à informação, passo a decidir a questão, analisando em separado os demais pedidos, a äm de que somente a presente possa ser de conhecimento público, permanecendo íntegro o sigilo da presente investigação.
>
> Esta magistrada, no bojo dos autos da investigação criminal em epígrafe, determinou o cumprimento da quebra do sigilo e interceptação telemática das mensagens compartilhadas no aplicativo Whatsapp em relação aos terminais-alvos indicados no ofício encaminhado pela d. autoridade policial ao Facebook do Brasil, sob pena de aplicação de multa coercitiva diária no valor de R$50.000,00, além de eventual configuração de crime de obstrução à Justiça e suspensão dos serviços até cumprimento da ordem judicial.
>
> Aduz a autoridade policial, após a primeira comunicação, que a empresa lhe encaminhou email – a partir do remetente Shannon Kontinos, Shannon@zwillgen.com, – cujo teor foi redigido em inglês e, em suma, revela que o Whatsapp não copia ou arquiva mensagens compartilhadas entre seus usuários e ainda formula cinco perguntas sobre a investigação

de onde partiu a determinação para a quebra, sem cumprir a determinação judicial. Noutra oportunidade, teria informado através de entrevista do criador do sistema criptográfico utilizado para codificação das mensagens acerca da impossibilidade da interceptação telemática dos seus conteúdos.

(...)

Ao ofício assinado por esta magistrada, contendo a ordem de quebra e interceptação telemáticas das mensagens do aplicativo Whatsapp, a referida empresa respondeu através de e-mail redigido em inglês, como se esta fosse a língua oficial deste país, em total desprezo às leis nacionais, inclusive porque se trata de empresa que possui estabelecida filial no Brasil e, portanto, sujeita às leis e à língua nacional, tratando o país como uma "republiqueta" com a qual parece estar acostumada a tratar. Duvida esta magistrada que em seu país de origem uma autoridade judicial, ou qualquer outra autoridade, seja tratada com tal deszelo.

(...)

Ora, a empresa alega, sempre, que não cumpre a ordem judicial por impossibilidades técnicas, no entanto quer ter acesso aos autos e à decisão judicial, tomando ciência dos supostos crimes investigados, da pessoa dos indiciados e demais detalhes da investigação.

O Juízo fica curioso em saber como estas informações auxiliariam os representantes do aplicativo Whatsapp a efetivar o cumprimento de ordem judicial vez que, segundo esta, o motivo dos reiterados descumprimentos, repita-se, são puramente técnicos.

Ao acolhermos o pedido do Whatsapp teríamos que admitir que todas as operadoras de telefonia, provedores e afins, ao receberem ofícios judiciais para cumprimento de determinada ordem de quebra de sigilo, tivessem o mesmo direito garantido de acesso à decisão judicial e aos autos, com conhecimento dos investigados e dos fatos em apuração, isso em processos sigilosos, determinaria, com certeza, o insucesso

de todas as investigações.

Neste sentido, os representantes do aplicativo Whatsapp nada fazem para cumprimento efetivo da ordem judicial, sendo que ordens idênticas já foram determinadas por juízes de diversos Estados deste País, no entanto, aqueles têm comparecido em Juízo e em sede policial pretendendo ter acesso aos autos e à decisão judicial (na forma certificada), em total desrespeito à Justiça, vez que plenamente cientificados de que se trata de processo sigiloso, em relação ao qual nem mesmo a serventia judicial tem acesso!!

Deve-se registrar que o Juízo não solicitou em momento algum o envio de mensagens pretéritas nem o armazenamento de dados, medidas estas que os responsáveis alegam não serem passíveis de cumprimento.

Em verdade, o Juízo requer, apenas, a desabilitação da chave de criptografadas, com a interceptação do fluxo de dados, com o desvio em tempo real em uma das formas sugeridas pelo MP, além do encaminhamento das mensagens já recebidas pelo usuário e ainda não criptografadas, ou seja, as mensagens trocadas deverão ser desviadas em tempo real (na forma que se dá com a interceptação de conversações telefônicas), antes de implementada a criptografia.

Não obstante o descumprimento, esta magistrada determinou que a intimação pessoal do representante empresa Facebook Brasil sediada em São Paulo, tendo sido recebida por funcionário que apôs seu nome e função na cópia do ofício. Embora, o Whatsapp Inc. e o Facebook Brasil, após o recebimento da ordem judicial, terem se manifestado nos autos através de seus departamentos jurídicos, a ordem não foi cumprida. Mesmo depois da terceira determinação, novamente entregue no escritório da citada empresa, não foi acatada a ordem deste Juízo, em razão do que o descumprimento persiste.

Conforme se extrai dos autos, assim, a ordem judicial não foi cumprida, apesar de reiterada por três vezes, ensejando, assim, a adoção das medidas coercitivas determinadas por este

Juízo.

(...)

Ora, se as decisões judiciais não podem efetivamente ser cumpridas e esta informação é sempre rechaçada por peritos da polícia federal e da polícia civil que afirmam ser possível o cumprimento, como foi possível ao Google do Brasil, em determinada ocasião, cumprir as decisões judicias que até então alegava ser impossível, deveremos então concluir que o serviço não poderá mais ser prestado, sob pena de privilegiar inúmeros indivíduos que se utilizam impunemente do aplicativo Whatsapp para prática de crimes diversos, orquestrar execuções, tramar todos os tipos de ilícitos, sempre acobertados pelos responsáveis legais do aplicativo Whatsapp, que insistem em descumprir as decisões judiciais, tornando estas condutas impossíveis de serem alcançadas pela Justiça.

O aplicativo whatsapp possui mais de 1 (um) bilhão de usuários em todo mundo, sendo certo que o "BRASIL é o segundo país com maior número de usuários atrás apenas da África do Sul. Segundo relatório divulgado pela entidade, 76% dos assinantes móveis no Brasil fazem uso regular do Whatsapp, que é o comunicador instantâneo mais popular no País".

Como se conclui, não pode um serviço de comunicação de tamanho alcance, ser oferecido a mais de 100 (cem) milhões de brasileiros sem, no entanto, se submeter às Leis do País, descumprindo decisões judiciais e obstruindo investigações criminais em diversas unidades da Federação.

Qualquer empresa que se instale no País fornecendo determinado serviço, deverá estar apta a cumprir as decisões judiciais que, porventura, recaiam sobre esta, sob pena de cancelamento do próprio serviço, ainda mais, quando se trata de atividade que envolve lucros vultosos, não sendo crível que seus representantes não sejam capazes de se aparelhar para o devido cumprimento das decisões judiciais.

O desembargador Cezário Siqueira Neto, do TJSE, ao indeferir liminar pleiteada pelo Facebook para que o serviço do

aplicativo Whatsapp fosse restabelecido após decisão de suspensão prolatada pelo juiz de Sergipe Marcel Maia Montalvão nos autos do processo nº 201655000183, apontou a inércia da empresa no atendimento das ordens judiciais:

(...)

Neste sentido, a finalidade pública da persecução criminal sempre deverá prevalecer sobre o interesse privado da empresa em preservar a intimidade e privacidade de seus usuários, assim como também deverá prevalecer sobre os interesses desses últimos, sobretudo quando são investigados por praticarem crimes, uma vez que não há direito ou garantia constitucional em nosso ordenamento que se repute absoluta.

(...)

Assim, embora se diga, no âmbito geral, que a suspensão dos serviços do aplicativo Whatsapp causa transtorno aos seus milhões de usuários, é necessário enxergar justamente o oposto, pois as investigações criminais onde atuam a Polícia Judiciária, o Ministério Público e o Poder Judiciário, visam atender, justamente, à população como um todo, tão carente nos dias atuais de uma melhoria na sua qualidade de vida e nos níveis de insegurança social, onde índices de criminalidade vêm crescendo assustadoramente, visando uma diminuição na impunidade que assola nosso País, atendendo, assim, seus reclames por segurança pública e Justiça.

A falta ou a negativa de informação por parte da empresa, deixando de atender a uma determinação judicial, impede aos órgãos de persecução de apurarem os ilícitos e alcançarem os autores dos crimes praticados, constituindo-se a recusa no fornecimento dos dados mera estratégia da empresa a até de procrastinar e até descumprir a ordem judicial, sob o pálio de impossibilidades técnicas.

O prejuízo maior, assim, quando o Facebook do Brasil descumpre uma ordem judicial, é da sociedade, ante a impunidade gerada pela negativa em fornecer informações que serão fundamentais para a consecução das investigações e, posteriormente, para robustecer o processo criminal de provas

que sejam úteis à formação da convicção das partes e do juiz.

Aqueles na sociedade que reclamam a simples ausência de um aplicativo como se não nos fosse mais possível viver sem tal facilidade, como se outros similares não pudessem ser utilizados, como se outros meios de comunicação não existissem, deveriam lembrar que a maior vítima dos crimes ora investigados é a própria Sociedade, sendo certo que a todo o momento novas vítimas são feitas e novos crimes são cometidos sem que a Justiça possa impedir os fatos ou punir os responsáveis.

Ante todo o exposto, deve-se impor ao senhor representante da empresa Facebook, assim, as sanções cominadas na decisão descumprida, a fim de que efetivamente dê atendimento à ordem judicial deste Juízo.

Em se tratando de inquérito policial que apura suposta prática do delito de organização criminosa voltada ao cometimento de diversos crimes, a conduta do senhor representante legal do Facebook Brasil constitui, em tese, crime previsto no artigo 2º, parágrafo 1º, da Lei 12850/2013. Isso posto, considerando o descumprimento de ordem judicial emanada deste Juízo, passo a decidir:

1. Oficie-se à Autoridade Policial, com cópias integrais da presente, a fim de que seja instaurado procedimento contra o senhor representante legal das empresas Facebook Serviços Online do Brasil Ltda, pela suposta prática do crime previsto no artigo 2º, parágrafo 1º, da Lei 12850/2013; 1. Determino a imposição de multa diária no valor de R$50.000,00 (cinquenta mil reais) até o efetivo cumprimento da medida de interceptação do fluxo de dados do Whatsapp (na forma da decisão em separado), com fulcro no artigo 139, IV, do Código de Processo Civil c/c artigo 3º, do Código de Processo Penal. Intime-se para pagamento o senhor representante legal da empresa Facebook Serviços Online do Brasil Ltda;

1. Oficie-se à EMBRATEL, ANATEL, bem como a todas as operadoras de telefonia celular, a fim de que providenciem, imediatamente, a suspensão do serviço do aplicativo Whatsapp

> em todas as operadoras de telefonia, até que a ordem judicial seja efetivamente cumprida pela empresa Facebook, sob as penas da Lei;
>
> 1. As medidas ora cominadas deverão ser cumpridas pela autoridade policial da 62ª DP ou por agentes especialmente designados pela mesma ou pela Chefia da Polícia Civil do Rio de Janeiro; "

Alegações do Ministério da Justiça

O Ministro da Justiça defendeu que as decisões judiciais não descumpriram preceito fundamental. Apontou, inicialmente, que a liberdade de comunicação, integrante da liberdade de expressão, não é absoluta e está sujeita aos limites externos que decorrem do próprio texto constitucional. Um dos limites seria, precisamente, o da investigação de ilícitos penais.

Defendeu, contudo, que o uso do aplicativo *Whatsapp* para a prática de atos ilícitos constitui abuso de direito e que o aplicativo "nada mais é do que um dos suportes tecnológicos disponíveis" para a exteriorização da linguagem (eDOC 102, p. 26). Por isso, em seu entender, a suspensão do aplicativo "envolve não a restrição à liberdade de comunicação, mas sim uma restrição a um suporte tecnológico por intermédio do qual se exercita a faculdade de comunicar-se" (eDOC 102, p. 27).

Sustenta que a guarda dos dados dos usuários é obrigatória, para que estejam disponíveis para fins de detecção e investigação de crimes graves, a exemplo do que ocorre, com a Diretiva n. 2006/24/CE da União Europeia. Aponta que a legislação brasileira deve ser interpretada à luz dessa obrigação e afirma que (eDOC 102, p. 32):

> "(...) a limitação efetuada pela decisão judicial, não só se encontra amparada pelo texto infraconstitucional consubstanciado no Marco Civil da Internet, mas também não desborda dos limites apresentados pela CF de 88, na medida em que à utilização do veículo ou instrumento *WhatsApp* não

> impossibilita a livre manifestação do pensamento e circulação de ideias, porquanto existentes outros meios oferecidos pelas operadores telefônicas, outros aplicativos de comunicação instantânea, de plataformas simples, interativas e igualmente gratuitos".

Por isso, em seu entender, a decisão judicial atacada vai ao encontro do interesse público.

Alegações do Procurador-Geral da República

O Procurador-Geral da República sustenta, no mérito, que, muito embora seja desproporcional a suspensão do funcionamento do aplicativo, é possível que ordem judicial determine a entrega não apenas de metadados, mas também do conteúdo das mensagens. O fundamento, de acordo com o i. Procurador-Geral, está na obrigação de guarda dos dados e da autorização legal de interceptação de comunicações telemáticas.

Alegações dos *Amici Curiae*

O Laboratório de Pesquisa Direito Privado e Internet – LAPIN rememorou o histórico de aprovação do Marco Civil da Internet para sustentar que as decisões que suspenderam o aplicativo fizeram interpretação equivocada dos dispositivos legais (eDOC 48, p.10):

> "26. Nesse contexto, a liberdade e o anonimato na internet receberam defesas efusivas por supostamente constituírem as principais garantias a serem resguardadas, o que significa que não se deveria permitir a autenticação obrigatória ou a associação entre os IPs e os usuários. A tecnologia existente seria relativamente adequada para a identificação dos usuários responsáveis pela prática de crimes virtuais, sem que para tanto fossem armazenados ou utilizados logs de conexão por parte dos provedores.

> 27. Em outra medida, sustentou-se que o registro das informações deveria ser algo voluntário, não devendo constituir uma obrigação de armazenamento por parte dos provedores. As contribuições ainda indicaram que o armazenamento deveria ser temporalmente limitado e aos indivíduos deveriam ser assegurados recursos que lhes permitissem controlar as informações armazenadas nos logs (accountability).
>
> 28. No que tange à responsabilidade pelo armazenamento dos dados, foi sugerida a obrigatoriedade de guarda dos registros pelos provedores de conexão e a faculdade dos provedores de conteúdo de fazê-lo. Por outro lado, tanto os provedores de conteúdo quanto os provedores de conexão deveriam obrigatoriamente armazenar os logs, entretanto bastava que estes logs guardassem a data de utilização e a origem do IP.
>
> 29. Muitas das contribuições, entretanto, demonstravam receio de que o sistema criado pelo poder público para o armazenamento de logs fosse potencialmente perigoso, facilitando a utilização indevida dos dados pessoais para o cometimento de crimes. Assim, em defesa da privacidade, o Estado deveria limitar sua atividade regulatória ao armazenamento de cadastros e não interferir nos logs de acesso, visto que o sigilo das comunicações de dados já era objeto de outras normas.
>
> 30. A partir da análise do relatório de contribuições para o Marco Civil, percebe-se a nítida preocupação com as garantias de autodeterminação informativa e de segurança das informações armazenadas, com frequentes questionamentos no sentido de que a guarda e o registro dos logs deveriam desestimulados para evitar abusos de vigilância em massa por parte dos agentes estatais."

O Facebook Serviços Online do Brasil Ltda., por sua vez, trouxe os seguintes esclarecimentos (eDOC 69, p. 2-3):

> "(i). O Facebook Brasil coopera plenamente com as

> autoridades brasileiras e, especificamente no que tange aos processos em curso perante as comarcas de Lagarto e Duque de Caxias, respondeu a todos os requerimentos dos respectivos juízos, cooperando no limite máximo de sua capacidade material;
>
> (ii). O Facebook Brasil não exerce qualquer controle sobre o aplicativo WhatsApp, que está sob a ingerência de pessoa jurídica independente e que possui representação própria (a WhatsApp Inc.), razão pela qual o Facebook Brasil é materialmente incapaz de cumprir decisões referentes a dados do aplicativo WhatsApp;
>
> (iii). O Facebook Brasil não praticou nenhum ato ilícito ou abusou de sua personalidade jurídica, razão pela qual não há nenhum motivo para que essa seja desconsiderada;
>
> (iv). As diversas esferas do Poder Judiciário Brasileiro vêm reconhecendo a ilegalidade da realização, em contas de titularidade do Facebook Brasil, de bloqueios de valores decorrentes de multa por alegado descumprimento de decisões judiciais em assuntos dessa natureza."

Os argumentos da petição do Instituto de Tecnologia e Sociedade vai ao encontro das informações trazidas pelo LAPIN. Afirma o Instituto que o Marco Civil da Internet pautou-se pela proteção dos dados dos usuários. Por isso, em seu entender, as sanções legalmente previstas somente seriam aplicáveis nos casos de violação do direito à privacidade. Daí porque, de acordo com o *amicus curiae*, "as atividades previstas no artigo 11 são realizadas exclusivamente na camada de conteúdo da internet e nunca na camada de infraestrutura da rede" (eDOC 105, p. 14). Defende que "não existe no texto do Marco Civil da Internet qualquer previsão de que as sanções do artigo 12 possam ser aplicadas em razão de descumprimento de ordem judicial" (eDOC 105, p. 14). Aduz, por fim que:

> "(...) o que está em jogo aqui não é apenas o aplicativo Whatsapp, mas sim a integridade da infraestrutura da internet

brasileira. Uma decisão que determina o bloqueio de um serviço diretamente na infraestrutura da internet impacta em seu funcionamento técnico. Por exemplo, países vizinhos ao Brasil que se interconectam à internet por meio da rede do país são imediatamente afetados. A resposta desses países é então desviar suas conexões para outras rotas não bloqueadas, preferindo se conectar via países como o Panamá ou os Estados Unidos, em vez de passar pelo Brasil, onde o bloqueio foi implementado.

51. Como visto acima, a Internet organiza-se em camadas. A camada de acesso, também conhecida como de aplicações, é onde operam, por exemplo, os intermediários da internet, como o Twitter, o Facebook e o Skype. Essa camada conecta o terminal do usuário ao primeiro terminal do provedor. Uma outra camada é a infraestrutura, que transporta os dados a partir daí até a outra camada de acesso do outro usuário. Interferir no acesso na camada de infraestrutura afeta não só o usuário final, a integridade de toda a rede do país, inclusive no que tange à forma como essa rede é utilizada por outros países.

52. Preservar a "neutralidade" da infraestrutura da internet, isto é, protegê-la contra a interferência desnecessária e desproporcional originada do Estado, quanto do abuso do poder econômico privado foi uma das principais conquistas do Marco Civil da Internet. Admitir o bloqueio de sites e aplicações joga por terra esse princípio essencial da neutralidade da rede. Por outro lado, ainda que se venha a admitir a ocorrência de bloqueios, não através do Marco Civil, mas sim através do exercício do poder geral de cautela do magistrado, conforme previsto na legislação processual civil, é importante destacar que o mesmo poder não deve ser exercido sobre a infraestrutura da rede, mas limitar-se somente à camada de conteúdos.

53. É inconstitucional a decisão que determina o bloqueio na camada de infraestrutura, pois viola direitos fundamentais, elencados como cláusulas pétreas, sem qualquer base constitucional – ou mesmo legal – para tanto. Conforme

> demonstrado anteriormente, o Marco Civil da Internet em nenhum momento permite o bloqueio de aplicativos, tampouco essa medida conforme implementada está em consonância com a Constituição Federal. O Marco Civil da Internet, em seu art. 12, apenas permite a suspensão das atividades do art. 11 e caso ocorra o desrespeito à privacidade dos usuários. Portanto, o bloqueio por descumprimento de ordem judicial é indevido. "

A PROTESTE também corrobora as alegações trazidas pelo Instituto de Tecnologia e Sociedade, no sentido de que não se amolda à previsão legal a sanção de suspensão do serviço de aplicativa. Afirma que, para isso, a outras sanções cabíveis, como, por exemplo, a previsão constante do § 4º do art. 15. Aduz que a proteção à liberdade de expressão é expressa, no âmbito do Marco Civil da Internet, pela neutralidade e inimputabilidade da rede e, por essa razão, devem receber a mesma proteção de preceito fundamental.

A Frente Parlamentar pela Internet Livre e Sem Limites alega que "a tônica preconizada pelo Marco Civil da Internet foi a proteção das liberdades, a guarda da intimidade e da vida privada" (eDOC 130, p. 7). Sustenta que o Marco Civil rejeita a ideia de que os usuários possam se submeter ao constante monitoramento de suas atividades, por isso, em seu entender, a interpretação de que o art. 10 da Lei n. 12.965/2014 exigiria que as empresas de aplicações virtuais guardassem os registros de acesso e conteúdo das mensagens pelos usuários é medida ofensiva a direitos fundamentais. Defende a aplicação dessa interpretação também para as empresas provedoras de aplicações (eDOC 130, p. 12):

> "(...) tanto sob o ponto de vista dos usuários da rede, quanto sob o prisma das empresas provedoras de aplicações virtuais, conclui-se que, perante a ordem constitucional vigente, os registros de conexão e especialmente o conteúdo das mensagens virtuais exigem intensa proteção, não se podendo conceber a existência de ato legislativo que estabeleça armazenamento da substância das comunicações."

A mesma ordem de ideias está na manifestação do Núcleo de Informação e Coordenação do Ponto BR – NIC.br que alega que as sanções se destinam às empresas violadoras da privacidade e da proteção de dados pessoais no Brasil e que os efeitos extraterritoriais das ordens de bloqueio do aplicativa em questão ferem os arts. 1º e 4º da Constituição Federal.

Já a AMB defendeu que aplicativo *Whatsapp* não constitui modalidade de serviço público e que não é a lei ou os magistrado que dão causa à suspensão das atividades dos aplicativos de comunicação, mas os próprios aplicativos, ao criarem sistema de criptografia inexpugnável que os impedem de cumprir decisões de quebra de sigilo. Em linha com o que sustentou o Ministro da Justiça, sustenta que "nenhum meio de comunicação pode ficar imune à atuação do Estado, para fins de investigação criminal ou instrução processual penal" (eDOC 233, p. 12). Afirma que, no caso concreto, o Juízo de Lagarto proferiu várias decisões, de forma gradativa, para exigir o acesso às comunicações, e teve desrespeitadas todas elas.

Alegações Mais Relevantes Trazidas na Audiência Pública

Os representantes do Departamento da Polícia Federal afirmaram que *iter criminis* nos dias atuais é percorrido utilizando aplicativos de comunicação. Alegaram que "*não há uma investigação da Polícia Federal que em, em momento oportuno, não se revela que atos de cogitação, porque não atos de preparo, ordens de execução, são feitos por meio de comunicação.*" Antevendo o argumento de que a apreensão do aparelho celular ao final supriria a necessidade de interceptação, asseveraram que neste caso seria tolhida uma das principais ferramentas investigativas, que é a ação controlada, buscando demonstrar que tal argumento não pode afastar a obrigação dos meios de comunicação de oferecer, em momento oportuno, as informações requeridas judicialmente.

Aduziram que "*a persecução penal no Brasil não pode se ditar por*

empresas de informática. Ela tem que se ditar pelo Estado" e apontaram que o enfrentamento da criminalidade moderna deve se dar através de ferramentas que oportunizem a obtenção de autoria e materialidade.

Sustentaram que não se deve perguntar se o aplicativo tem viabilidade técnica, mas sim por que não tem viabilidade, ou por que não procura tê-las, defendendo o cumprimento imperativo da lei. Destacaram a importância de uma visão retrospectiva da matéria, buscando demonstrar que as empresas de e-mail (Microsoft, Gmail, etc.) também se utilizaram de argumentos técnicos para, num primeiro momento, se esquivarem do cumprimento de ordens judiciais, mas que atualmente colaboram com as investigações. Nesse sentido, destacaram que a decisão a ser tomada pelo STF poderá ser um divisor de águas, alertando que diversos meios de investigação que a Polícia Federal dispõe atualmente poderão cair por terra, sob o mesmo argumento de inviabilidade técnica utilizado pelo WhatsApp.

Ivo de Carvalho Peixinho, perito criminal, afirma que a Polícia Federal não propõe a criação de "*backdoor*", quebra de criptografia ou alterações no cliente, mas sim o fornecimento de metadados, a interceptação telemática posterior a um pedido judicial e, em casos específicos, a notificação de transmissão de conteúdo relacionado à pornografia infantil. Nesse sentido, apresentou a política de privacidade do WhatsApp (disponível em https://www.whatsapp.com/legal/#privacy-policy-information-we-collect), listando quais os metadados coletados pelo aplicativos, como indicou: (i) dados da conta (número de celular, agenda de contatos, nome do perfil, foto e mensagem de status); (ii) mensagens não entregues por 30 dias; (iii) fotos e vídeos populares guardados por mais tempo; (iv) contatos (criar, participar ou ser adicionado a grupos ou listas de transmissão e esses ficam associados a seus dados de conta); (v) dispositivo (modelo de hardware, dados do sistema operacional, navegador, endereço de IP, dados sobre a rede móvel incluindo localização).

O perito afirma que nenhum tráfego de informação é realizado sem que se passe pelos servidores do WhasApp, independente de se utilizar

celular ou computador para acessar o aplicativo. Diz do sistema de criptografia ponta-a-ponta adotado pelo WhatsApp e esclarece que todos os arquivos de mídia e outros anexos que são enviados entre usuários passam, necessariamente, pelos servidores do aplicativo.

Quanto às fotos e vídeos "virais" que são identificados (sem a identificação do conteúdo em si) pelo WhatsApp e guardados por mais tempo nos servidores, o expositor entende que tal ferramenta poderia também ser utilizada para identificar materiais relacionados à pornografia infantil.

A Procuradoria-Geral da República enviou representantes à audiência. Alegaram inicialmente, que a ausência de representação legal do WhasApp no Brasil não afasta a legitimidade do Facebook para responder e cumprir decisões judiciais envolvendo o WhatsApp, porquanto pertencem a um mesmo grupo econômico.

Sustentaram a importância de fixação, pelo STF, do enquadramento do regime jurídico da atividade desenvolvida tanto pelo WhatsApp quanto pelos demais aplicativos de troca de mensagens instantâneas, definindo se tais atividades podem ser caracterizadas como essenciais, uma vez que, em seu entender, somente os serviços considerados essenciais encontram-se abrangidos pelo princípio da continuidade e, portanto, impedidos de serem suspensos. Defenderam que o WhatsApp é uma empresa OTT *(over the top*) que se utiliza das estruturas e serviços prestados pelas empresas de telecomunicações para prestar seus serviços (assim como a Netflix, Skype, Youtube, etc.). No mérito, defende a improcedência das ações concentradas em virtude: **i)** do caráter relativo do direito à comunicação e à liberdade de expressão; **ii)** da ausência de violação dos direitos de comunicação e de liberdade de expressão pela suspensão temporária de um aplicativo e; **iii)** da submissão do WhatsApp ao Marco Civil da Internet, especialmente no tocante ao estabelecimento de sanções em virtude do não cumprimento de ordens judiciais.

Fernanda Teixeira Souza Domingos, uma das representantes da Procuradoria-Geral da República, com base em perícia elaborada pelo Ministério Público, sustentou, ainda, a possibilidade de interceptação do

conteúdo das mensagens do WhatsApp através do ataque "*man-in-the-middle*" e ressaltou a importância das sanções impostas pelo Marco Civil da Internet para obrigar as empresas a cumprir as decisões judiciais.

Ressaltando a dimensão internacional da controvérsia, o expositor Vladimir Barros Aras defendou ser inimaginável a criação no Brasil, a partir do resultado do julgamento das presentes ações concentradas, de um "*paraíso digital em que criminosos desse tipo pudessem cometer infrações penais, violando direitos fundamentais tão importantes, como o direito à privacidade.*"

No que tange aos aspectos técnicos da arquitetura do sistema, Demi Getschko, representante do Comitê Gestor da Internet no Brasil e pelo Núcleo de Informação e Coordenação do Ponto BR, afirmou que quanto mais se pretende "apertar" a internet no sentido de monitorar e de interceptar as atividades ali desenvolvidas, mais a internet se protege, criando mecanismos contrários.

Apontou que a "*criptografia é algo que não está no crivo de ser criticável ou não. Ela é uma ferramenta para o desenvolvimento da comunidade, seja da área privada, pública, ou que for e, portanto, deve ser protegida e não entra em questão se se deveria permitir ou não a criptografia."*

Indicou os perigos de se criar acessos privilegiados – as chamadas "*backdoors"* – para permitir a interceptação na medida em que não se tem como garantir a integridade e a segurança do sistema. Citou, como exemplo de falha de segurança, o cyber ataque "*WannaCry*", ocorrido em 2016, que a partir de uma vulnerabilidade identificada e explorada secretamente pela NSA (Agência Nacional de Segurança dos EUA) para fins de inteligência e segurança nacional, acabou resultando numa ação criminosa que atacou em massa usuários individuais e corporativos em todo o mundo. Falou ainda da chamada "*Criptowar*" ocorrida nos Estados Unidos onde, na década de 80-90, o Governo americano tinha o monopólio dos padrões de criptografia e os regulava nos mesmos moldes da regulação de munição militar. Posteriormente, em 1996, no caso *Bernstein vs United States*, considerou-se a criptografia como liberdade de expressão, podendo ser livremente difundida. Finalizou citando o

Decálogo elaborado pelo CGI.br, que dispõe que a criptografia é instrumental aos direitos humanos de privacidade e liberdade de expressão; é uma tecnologia que deve ser estimulada e não restringida; as plataformas que disponibilizam tecnologias de segurança da informação não devem ser penalizadas pelos usos de seus usuários. Conclui afirmando que privacidade e segurança são convergentes e não contrapostos.

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-aponta 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 desencriptá-la.

Quanto aos demais instrumentos que podem auxiliar as investigações, aponta a importância da utilização dos metadados e da geolocalização, ressaltando a riqueza de dados a serem explorados pelas autoridades públicas.

Finaliza citando trecho do Relatório Especial do Conselho de Direitos Humanos da ONU, que diz que *"A criptografia possibilita que indivíduos exerçam seus direitos à liberdade de opinião e expressão na era digital e, como tal, merece nossa proteção."*

A Federação de Empresas de Telecomunicação afirmou que as empresas de telecomunicações são responsáveis pelo transporte de todos os dados que circulam na internet, sem acessar ou interferir no conteúdo das informações inseridas ou retiradas da internet. No tocante à interceptação legal e fornecimento de dados pessoais, apontou que as empresas de telecomunicações criaram infraestrutura exclusiva para atender às ordens judiciais, resultando em um custo operacional para as mesmas. Na visão da FEBRATEL, qualquer empresa que oferte serviço no Brasil deve atender o marco legal e regulatório brasileiro, de modo que, se alinhando à posição defendida pela Polícia Federal e pelo Ministério Público Federal, entende que o WhatsApp deve cumprir as determinações judiciais que garantem o acesso das autoridades ao conteúdo das comunicações privadas.

Reconheceu a importância da criptografia para a garantia da segurança das informações e da privacidade na internet, mas defendeu a viabilidade técnica da implementação, pelo WhatsApp, de um componente que permita às autoridades monitorar as mensagens de determinado usuário através do espelhamento das conversas realizadas através do WhatsApp, ressaltando, no entanto, a problemática referente à utilização não autorizada de tal espelhamento.

Concluiu a exposição afirmando que "*fica clara que o bloqueio do*

aplicativo WhatsApp e de qualquer outra aplicação deveria ser evitado ao máximo e a interceptação de conversas de aplicações de internet é inócua de ser realizada, mas os prestadores de serviços de telecomunicações estão aptos para atender as determinações judiciais quando necessário."

Os representantes do Laboratório de Pesquisa Direito Privado e Internet da Universidade de Brasília, corroborou os termos de sua manifestação nos autos e trouxe relevantes aspectos técnicos sobre soluções alternativas à interceptação. A técnica denominada "**man-in-the-middle"** (cria-se um terceiro para intervir na comunicação, passando-se por um dos dois interlocutores), a seu ver, seria ineficaz, pois o próprio aplicativo WhatsApp tem uma funcionalidade que permite ao usuário reconhecer a atuação desse terceiro interlocutor. Uma outra forma de ataque possível ao WhatsApp seria o "**Protocolo SS7"** (espécie de man-in-the-middle), que é utilizado para a comunicação entre centrais telefônicas. Segundo o LAPIN, ele não possui criptografia e pode ser integrado a um órgão de investigação a um custo razoável. Nessa hipótese, o ataque inicial seria via SMS visando clonar o aparelho desejado. Após o clone, bastaria instalar o WhatsApp e identificar-se aos servidores com o número clonado como se o usuário houvesse trocado o aparelho, autenticando a "nova identidade" via SS7. Para os expositores, entretanto, haveria dúvida acerca do valor probatório das informações obtidas através dessa técnica na medida em que há a possibilidade de alteração das mensagens interceptadas. Já o "**espelhamento do computador"** seria um procedimento simples de se realizar, mas que dependeria de acesso físico ao aparelho. Por fim, a "**captura de metadados"** (que são os dados sobre as mensagens e não as mensagens em si), poderia ser feita sem a necessidade de quebra da criptografia.

Finalmente, o Centro de Tecnologia e Sociedade da Escola de Direito da FGV-Rio explicou, inicialmente, a diferença entre os serviços de telefonia e os serviços de internet e afirmou que a criptografia de chave pública, utilizada pelo WhatsApp, foi pensada para resolver as questões referentes à segurança e privacidade dos dados que trafegam na internet. Sustentou que no modelo teórico que o WhatsApp diz implementar, não

é possível interceptar ou espelhar as comunicações no WhatsApp.

De acordo com o Centro, a realização da interceptação e/ou do espelhamento só seria possível se o WhatsApp fizesse alterações em seus sistemas, mas essas mudanças seriam de difícil realização, pois a mudança no WhatsApp teria que ser global, visto que o mesmo aplicativo usado no Brasil é utilizado no restante do mundo. Ademais, ainda que se tivesse um WhatsApp só para o Brasil, a versão original sem as mudanças (tipo backdoor) continuaria acessível aos brasileiros. Essa alteração ainda traria problemas éticos ou jurídicos, porquanto o WhatsApp não poderia mais garantir a segurança e confiabilidade do seu sistema aos usuários; concorrenciais, visto que haveria uma migração dos usuários para outras plataformas, seja por razões lícitas ou ilícitas; além de problemas de segurança, uma vez ser improvável que uma falha de segurança implementadas no WhatsApp fique restrita a um usuário específico ou a um único ambiente.

Ainda no aspecto técnico, sustenta que o WhatsApp, se quiser, pode facilmente adotar um modelo federado de conexão que não tenha um servidor centralizado e, dessa forma, impedir tecnicamente que as empresas de telecomunicação implementem o bloqueio do WhatsApp, tornando as decisões judiciais inócuas e impossíveis de serem cumpridas.

Alegações Especificamente Trazidas pelo Whatsapp

O expositor e co-fundador do WhatsApp Brian Acton explicou que o aplicativo possibilita aos usuários mandarem mensagens de texto, mídia e documentos e fazerem chamadas de voz e vídeo com segurança e facilidade e afirma que possui mais de 120 milhões de usuários regulares no Brasil. Registrou que, desde o princípio da criação do aplicativo, a privacidade e a segurança foram essenciais e que a criptografia protege os usuários de hackers e ajuda a transmitir sensação de segurança para que os usuários realizem suas comunicações.

Defendeu os benefícios do sistema criptográfico adotado pelo aplicativo, afirmando que a criptografia ponta-a-ponta adotada pelo

WhatsApp faz com que ninguém além do usuário tenha acesso ao conteúdo das mensagens e dos dados que trafegam pelo aplicativo. Para cada mensagem enviada uma nova chave de segurança é criada, de modo que caso haja a desencriptação de uma chave, esta só revelaria uma única mensagem, e não a totalidade da conversa.

Por esse modelo, não seria possível ao WhatsApp interceptar ou ler as conversas e/ou arquivos enviados e recebidos através da plataforma de comunicação, porque o aplicativo não tem acesso às chaves privadas dos usuários. Pela mesma razão, não seria possível desabilitar a criptografia para usuários específicos, ressaltando que qualquer alteração nas chaves de segurança que pudessem permitir a interceptação seria percebida e corrigida pelo sistema de verificação de código do aplicativo. Afirmou: **a única maneira de desabilitar a criptografia para um usuário específico seria desabilitar a criptografia para todos os usuários.**

No que tange à criação de uma "*backdoor*" no aplicativo ou à implementação de uma chave-mestra, sustentou que o sistema ficaria desprotegido de modo que se algum hacker tivesse acesso à essa chave, ele acessaria qualquer mensagem e/ou arquivo de qualquer usuário do aplicativo ao redor do mundo.

As mudanças na criptografia do WhatsApp, segundo o expositor, seriam detectadas rapidamente, visto que pesquisadores da comunidade científica analisam o código do aplicativo regularmente, descobrindo e publicando qualquer vulnerabilidade que porventura o software tenha. Alternativamente, se o WhatsApp mudasse seus servidores para permitir a interceptação – utilizando a técnica de ataque *man-in-the-middle* –, a medida também seria detectada durante a verificação de segurança dos códigos, não permitindo a interceptação.

O sistema do WhatsApp, ainda de acordo com o expositor, não permite fazer o espelhamento de uma conta de determinado usuário para outro dispositivo (*smartphone*, computador, *tablet*), pois o WhatsApp Web utiliza um túnel de segurança que se conecta diretamente com o telefone, sincronizando as mensagens, ou seja, o WhatsApp Web é uma extensão do aplicativo instalado no aparelho celular, aplicando-se à ele os mesmos

óbices de ordem técnica. Uma vez estabelecida a conexão entre o WhastApp e o WhatsApp Web através da utilização de QR-Code Scan, é necessário que o celular permaneça no mesmo ambiente do computador para que o QR-Code Scan continue funcionando.

Registrou, ao fim de sua exposição, que **os metadados coletados pelos servidores do WhatsApp são disponibilizados para as forças de segurança e justiça do Brasil, de acordo com as ordens judiciais, mas o conteúdo em si das mensagens e/ou dados são sempre encriptados, não podendo ser lidos ou interceptados**.

Exame das Alegações – Mérito da Arguição

Como havia indicado no início desta manifestação, os aportes trazidos pelos *amici curiae* e pelas entidades e especialistas que participaram da audiência pública, realizado em trabalho conjunto com a e. Ministra Rosa Weber, foram fundamentais para o pleno esclarecimento dos pontos controvertidos trazidos nesta arguição.

À luz de tudo o quanto exposto, antes de examinar os argumentos jurídicos apresentados, em particular, a proporcionalidade a que alude o Cidadania, é preciso delimitar precisamente o objeto da arguição para assentar algumas premissas que orientam este voto.

São bastante recentes na jurisdição do Supremo Tribunal Federal os debates que aos poucos põem em evidência o direito das pessoas no ambiente digital. Ainda em maio de 2020, em discussão inédita nesta Corte, o Tribunal deliberou sobre a constitucionalidade de medida provisória que permitia o acesso a dados pessoais por parte do IBGE (ADI 6.387, Rel. Min. Rosa Weber, acórdão ainda pendente de publicação).

O julgamento é notável não apenas pelo ineditismo, mas sobretudo por assentar, como na brilhante manifestação da e. Ministra Rosa Weber, que mudanças políticas, sociais e econômicas demandam o reconhecimento de novos direitos, "razão pela qual necessário, de tempos em tempos, redefinir a exata natureza e extensão da proteção à

privacidade do indivíduo".

O e. Ministro Gilmar Mendes, em trecho notável de sua manifestação, bem indicou as mudanças por que passa a sociedade e, bem assim, o direito:

> "O direito fundamental à igualdade – enquanto núcleo de qualquer ordem constitucional – é submetido a graves riscos diante da evolução tecnológica. A elevada concentração de coleta, tratamento e análise de dados possibilita que governos e de empresas utilizem algoritmos e ferramentas de data analytics, que promovem classificações e esteriotipações discriminatórias de grupos sociais para a tomada de decisões estratégias para a vida social, como a alocação de oportunidades de acesso a emprego, negócios e outros bens sociais. Essas decisões são claramente passíveis de interferência por viesses e inconsistências que naturalmente marcam as análises estatísticas que os algoritmos desempenham.
>
> (...)
>
> Todo esse contexto nos indica que decisões críticas para o Estado de Direito estão sendo cada vez mais substituídas por mecanismos automatizados. Em outras palavras, de forma bem direta: vivemos na era das escolhas de Sofia automatizadas.
>
> Independente do acerto ou desacerto dessas decisões automatizadas, é inequívoco que a proteção dos valores estruturante da nossa democracia constitucional requer que o Direito atribua elementos de transparência e controle que preservem o exercício da cidadania. É por isso que, para muito além do mero debate sobre o sigilo comunicacional, este Tribunal deve reconhecer que a disciplina jurídica do processamento e da utilização da informação acaba por afetar o sistema de proteção de garantias individuais como um todo."

Como indicam essas manifestações, o impacto tecnológico das mudanças porque passa a sociedade reclamam um permanente atualizar do alcance dos direitos e garantias fundamentais.

Os temas que envolvem o mundo digital são variados e, ainda que

sejam relacionados, não serão todos resolvidos na presente arguição de descumprimento de preceito fundamental. Mesmo que os princípios examinados nesta ação tenham aplicação em outros casos, a solução proposta por este voto **não** abrange outros debates já submetidos à pauta deste Tribunal, como a questão sobre a constitucionalidade do art. 19 da Lei 12.965, de 2014, ou Marco Civil da Internet (RE 1.037.396, Rel. Min. Dias Toffoli, Tema 987); o dever da empresa hospedeira de sítio na internet fiscalizar o conteúdo publicado e de retirá-lo do ar quando considerado ofensivo, sem intervenção do Judiciário (RE 660.861, Rel. Min. Luiz Fux, Tema 533); a aplicabilidade do direito ao esquecimento na esfera civil quando for invocado pela própria vítima ou pelos seus familiares (RE 1.010.606, Rel. Min. Dias Toffoli, Tema 786); a licitude do acesso a informações contidas em aparelho celular (RE 1.042.075, Rel. Min. Dias Toffoli, Tema 977); ou, finalmente, a constitucionalidade de medidas de cooperação jurídica internacional (ADC 51, Rel. Min. Gilmar Mendes).

O debate, na presente ação, é distinto. Com efeito, o **objeto da presente arguição é (i) saber se é constitucional a ordem judicial de acesso por órgãos do Estado ao conteúdo de comunicações protegidas por criptografia, conforme previsão constante do art. 7º, II, do Marco Civil da Internete; e, em sendo constitucional, (ii) saber se a sanção prevista no inciso III do art. 12 do mesmo diploma legal pode ser aplicada pelo Poder Judiciário**.

Os dois dispositivos têm a seguinte redação:

> "Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
>
> (...)
>
> II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;"
>
> "Art. 12. Sem prejuízo das demais sanções cíveis, criminais ou administrativas, as infrações às normas previstas nos arts. 10 e 11 ficam sujeitas, conforme o caso, às seguintes sanções,

> aplicadas de forma isolada ou cumulativa:
>
> (...)
>
> III - suspensão temporária das atividades que envolvam os atos previstos no art. 11; ou"

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.

Essas premissas coincidem parcialmente com às que apresentaram James A. Lewis, Denis E. Zheng e William A. Carter no Relatório *The Effect of Encryption on Lawful Access to Communication and Data* (disponível em: https://www.csis.org/analysis/effect-encryption-lawful-access-communications-and-data; acesso em 17.05.2020). Elas indicam, de um lado, a legitimidade do argumento trazido pelos órgãos de segurança, assim como atestam, caso se tenham em vista os precedentes que reconhecem a constitucionalidade das interceptações telemáticas, a adequação e a necessidade.

Assim, 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.**

A resposta a essa questão depende de um rigoroso exame de proporcionalidade, isto é, de uma avaliação cuidadosa para se o que se ganha com a promoção de um interesse público é ou não compensado com a restrição de direitos. Além disso, é preciso que a Corte leve em devida conta a certeza científica que se tem sobre essas informações, assim como o grau de institucionalização promovido pelo Estado. Afinal, "quanto mais grave for o peso de uma interferência em um direito constitucional, maior deve ser a certeza sobre as premissas que a fundamentam" (ALEXY, Robert. *On Balancing and Subsumption. A Strucutral Comparison.* In: Ratio Juris, v. 16, n. 4, dez. 2003, p. 446).

O voto estrutura-se, portanto, no exame dos argumentos sobre os direitos envolvidos e sobre a intensidade da interferência neles causada a partir de possíveis alterações no modelo de criptografia adotado pelo *Whatsapp*.

A Proteção Constitucional à Privacidade, à Liberdade de Opinião e de Manifestação do Pensamento e a Proibição de Violações de Direitos Fundamentais

O Cidadania invoca, como direito a ser especialmente protegido, o direito à comunicação, garantido no art. 5º, IX, da CRFB e violado, de forma desproporcional, por um conjunto de decisões judiciais. O parâmetro constitucional invocado tem o seguinte teor:

> "Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> (...)
> IX - é livre a expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença;"

Os *amici curiae*, por sua vez, invocam não apenas o direito à comunicação, mas também os direitos de livre expressão do pensamento e de proteção à privacidade:

> "Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> (...)
> IV - é livre a manifestação do pensamento, sendo vedado o anonimato;
> (...)
> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo

> dano material ou moral decorrente de sua violação;
>
> XI - a casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial;
>
> XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;"

Esses direitos, como se sabe, correspondem às garantias que também vêm expressas em tratados de direitos humanos, como o Pacto Internacional de Direitos Civis e Políticos e o Pacto de São José da Costa Rica:

> **Pacto Internacional de Direitos Civis e Políticos**
>
> "Artigo 17
>
> 1. Ninguém será objecto de ingerências arbitrárias ou ilegais na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem de ataques ilegais à sua honra e reputação.
>
> 2. Toda a pessoa tem direito a proteção da lei contra essas ingerências ou esses ataques.
>
> (...)
>
> Artigo 19
>
> 1. Ninguém pode ser discriminado por causa das suas opiniões.
>
> 2. Toda a pessoa tem direito à liberdade de expressão; este direito compreende a liberdade de procurar, receber e divulgar informações e ideias de toda a índole sem consideração de fronteiras, seja oralmente, por escrito, de forma impressa ou artística, ou por qualquer outro processo que escolher.
>
> 3. O exercício do direito previsto no parágrafo 2 deste artigo implica deveres e responsabilidades especiais. Por conseguinte, pode estar sujeito a certas restrições,

expressamente previstas na lei, e que sejam necessárias para:

a) Assegurar o respeito pelos direitos e a reputação de outrem;

b) A proteção da segurança nacional, a ordem pública ou a saúde ou a moral públicas."

Pacto de São José da Costa Rica

"Artigo 11. Proteção da honra e da dignidade

1. Toda pessoa tem direito ao respeito de sua honra e ao reconhecimento de sua dignidade.

2. Ninguém pode ser objeto de ingerências arbitrárias ou abusivas em sua vida privada, na de sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais à sua honra ou reputação.

3. Toda pessoa tem direito à proteção da lei contra tais ingerências ou tais ofensas.

(...)

Artigo 13. Liberdade de pensamento e de expressão

1. Toda pessoa tem direito à liberdade de pensamento e de expressão. Esse direito compreende a liberdade de buscar, receber e difundir informações e idéias de toda natureza, sem consideração de fronteiras, verbalmente ou por escrito, ou em forma impressa ou artística, ou por qualquer outro processo de sua escolha.

2. O exercício do direito previsto no inciso precedente não pode estar sujeito a censura prévia, mas a responsabilidades ulteriores, que devem ser expressamente fixadas pela lei e ser necessárias para assegurar:

a. o respeito aos direitos ou à reputação das demais pessoas; ou

b. a proteção da segurança nacional, da ordem pública, ou da saúde ou da moral públicas.

3. Não se pode restringir o direito de expressão por vias ou meios indiretos, tais como o abuso de controles oficiais ou particulares de papel de imprensa, de freqüências radioelétricas ou de equipamentos e aparelhos usados na difusão de

> informação, nem por quaisquer outros meios destinados a obstar a comunicação e a circulação de idéias e opiniões.
>
> 4. A lei pode submeter os espetáculos públicos a censura prévia, com o objetivo exclusivo de regular o acesso a eles, para proteção moral da infância e da adolescência, sem prejuízo do disposto no inciso 2.
>
> 5. A lei deve proibir toda propaganda a favor da guerra, bem como toda apologia ao ódio nacional, racial ou religioso que constitua incitação à discriminação, à hostilidade, ao crime ou à violência."

Como se depreende da leitura desses dispositivos, não se extrai deles, de imediato, sua aplicação direta à proteção das pessoas no ambiente digital. É preciso interpretá-los, portanto, à luz das invocações tecnológicas, sob pena de retirar-lhes a máxima eficácia que deles exige a Constituição.

O guia de interpretação deve, portanto, ser o seguinte: **os direitos que as pessoas têm *offline* devem também ser protegidos *online.*** Direitos digitais são direitos fundamentais.

Essa é a orientação do Conselho de Direitos Humanos das Nações Unidas (A/HRC/RES/32/13) e é também a orientação que começou a ser esboçada por este Tribunal no julgamento da ADI 6.387, relatada pela e. Ministra Rosa Weber. Nesse julgamento, o e. Ministro Gilmar Mendes bem sublinhou que: "nunca foi estranha à jurisdição constitucional a ideia de que os parâmetros de proteção dos direitos fundamentais devem ser permanentemente abertos à evolução tecnológica."

Esta Corte tem se mantido atenta à necessidade de atribuir máxima eficácia aos direitos fundamentais mesmo diante de mudanças tecnológicas. Foi, assim, por exemplo, com o direito ao sigilo bancário, ao sigilo fiscal e ao sigilo telefônico (MS 23.452, Rel. Min. Celso de Mello, DJ 12.05.2000), inclusive para *emails* (RHC 132.115, Rel. Min. Dias Toffoli, DJe 18.10.2018).

O caso do direito à privacidade é exemplar. Ele não apenas envolve o direito de ser deixado a sós, como afirma o Justice Brandeis, mas também,

como advertia pioneiramente Stéfano Rodotà "algo muito mais complexo que requeira proteção em razão de escolhas de vida que devem ser protegidas contra o controle estatal e estigmatização social" (Traduções livres de: RODOTÀ, Stefano. General Presentation of Problems related to Transsexualism. In: Transsexualism, Medicine and Law: Proceedings of the XXIIIrd Colloquy on European Law. Strasbourg: Concil of Europe Publishing, 1995. p. 22-23).

Na internet, a proteção de privacidade não é apenas proteção individual, mas garantia instrumental do direito à liberdade de expressão. Isso porque o fluxo de informações é feito tanto pelos dados que são recebidos, quanto pelos dados enviados. Toda e qualquer escolha do usuário, inclusive não realizar escolha alguma, pode ser medida, calculada, comparada e comprada. Ficar sozinho não significa ficar em silêncio. Por isso, novamente, feliz a definição de Stéfano Rodotà: "a privacidade é o direito de manter o controle sobre a sua própria informação e de determinar a maneira de construir sua própria esfera pública" (RODOTÀ, Stéfano. Data Protection as a Fundamental Right. In: In: Gutwirth S., Poullet Y., De Hert P., de Terwangne C., Nouwt S. (eds). Reinventing Data Protection? Dordrecht: Springer, 2009, p. 78).

Em 2013, as Nações Unidas incorporam essa definição. Depois de descoberto um grande esquema de espionagem de milhões de usuários de redes sociais, as representações diplomáticas do Brasil e da Alemanha propuseram à Assembleia Geral das Nações Unidas minuta de resolução sobre a proteção da privacidade no ambiente digital. A Resolução, aprovada por consenso, assenta que a Assembleia Geral das Nações Unidas (tradução livre):

> "1. Reafirma o direito à privacidade, segundo o qual ninguém será objeto de ingerências arbitrárias ou ilegais em sua vida privada, em sua família ou sua correspondência, nos termos do artigo 12 da Declaração Universal de Direito Humanos e do artigo 17 do Pacto Internacional de Direitos Civis e Políticos;
>
> 2. Reconhece a natureza global e aberta da Internet e o

> rápido avanço das tecnologias de informação e comunicação como um motor de progresso para as várias formas de desenvolvimento;
>
> 3. Afirma que os mesmos direitos que as pessoas têm offline devem também ser protegidos online, incluindo o direito à privacidade;
>
> 4. Chama todos os Estados a:
>
> (a) Respeitar e proteger o direito à privacidade, inclusive no contexto às comunicações digitais;
>
> (b) Adotar todas as medidas para por fim às violações desses direitos e a criar condições para prevenir essas violações, incluindo pela garantia de que leis nacionais relevantes atendam às obrigações assumidas pelo direito internacional dos direitos humanos;
>
> (c) Revisar seus procedimentos, suas práticas e sua legislação relativamente à vigilância das comunicações, sua interceptação e a coleta de dados pessoais, incluindo a vigilância em massa, sua interceptação e coleta, com vistas à garantir o direito à privacidade por meio da completa e efetiva implementação de suas obrigações internacionais;
>
> (d) Estabelecer e manter os mecanismos de controle independentes e efetivos capazes de assegurar a transparência e a *accountability* dos sistemas domésticos de vigilância de comunicações, sua interceptação e a coleta de dados pessoais.

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.

No âmbito do Marco Civil da Internet, a proteção à privacidade é feita pela atribuição dos seguintes direitos aos usuários:

> "Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
>
> I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;
>
> II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;
>
> III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;"

Trata-se, portanto, de norma que, não obstante sua natureza de legislação ordinária, densifica o comando constitucional e internacional sobre a privacidade do fluxo de comunicações. Ele é, substancialmente, a ponte que atualiza e adapta o alcance do direito à privacidade ao mundo digital.

Não por acaso, invocam os *amici curiae* o art. 7º, II, como interpretação autêntica da dimensão digital do direito assegurado no art. 5º, X e XI, da Constituição Federal. De fato, quando do envio do projeto de lei que deu origem ao Marco Civil, fez observar o Ministro da Justiça o seguinte (EMI Nº 00086 – MJ/MP/MCT/MC, de 25.04.2011):

> "Para o Poder Judiciário, a ausência de definição legal específica, em face da realidade diversificada das relações virtuais, tem gerado decisões judiciais conflitantes, e mesmo contraditórias. Não raro, controvérsias simples sobre responsabilidade civil obtêm respostas que, embora direcionadas a assegurar a devida reparação de direitos individuais, podem, em razão das peculiaridades da Internet, colocar em risco as garantias constitucionais de privacidade e liberdade de expressão de toda a sociedade.
>
> (...)
>
> No terceiro capítulo, ao tratar da provisão de conexão e de

> aplicações de internet, o anteprojeto versa sobre as questões como: o tráfego de dados, a guarda de registros de conexão à Internet, a guarda de registro de acesso a aplicações na rede, a responsabilidade por danos decorrentes de conteúdo gerado por terceiros e a requisição judicial de registros. As opções adotadas privilegiam a responsabilização subjetiva, como forma de preservar as conquistas para a liberdade de expressão decorrentes da chamada Web 2.0, que se caracteriza pela ampla liberdade de produção de conteúdo pelos próprios usuários, sem a necessidade de aprovação prévia pelos intermediários. A norma mira os usos legítimos, protegendo a privacidade dos usuários e a liberdade de expressão, adotando como pressuposto o princípio da presunção de inocência, tratando os abusos como eventos excepcionais."

A fim de não deixar dúvidas sobre a relevância que esse direito deve assumir no ambiente digital, o Marco Civil ainda prevê, em seu art. 8º, "a garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet".

A proteção constitucionalmente assegurada ao direito à privacidade é, portanto, elevada, digna dos direitos que detêm a mais ampla primazia no ordenamento nacional.

A mesma conclusão pode ser feita para o direito à liberdade de pensamento e de expressão que conta, no âmbito da jurisprudência desta Corte, com um grau elevado de proteção. São marcos da atuação dessa Corte votos memoráveis como o que assentou a precedência das liberdades de pensamento e de expressão (ADPF 130, Rel. Min. Ayres Britto, DJe 05.11.2009); o que fixou a primazia *prima facie* da liberdade de expressão no confronto com outros direitos fundamentais (ADI 4.815, Rel. Ministra Cármen Lúcia, DJe 29.01.2016); e o que reconheceu que a democracia não existirá e a livre participação política não florescerá onde a liberdade de expressão for ceifada, pois esta constitui condição essencial ao pluralismo de ideias, que por sua vez é um valor estruturante para o salutar funcionamento do sistema democrático (ADI 4.451, Rel. Min.

Alexandre de Moraes, DJe 06.03.2019).

Em cada um desses precedentes reconheceu-se não apenas a liberdade de expressar o pensamento, como também a de ter opiniões. No caso da ADPF sobre a lei de imprensa, reconheceu-se que o direito à informação crítica – em essência a que diverge da versão oficial do Estado – como sendo integrante da própria liberdade de pensamento. Biografias não autorizadas – as que, não raro, constroem outra narrativa, crítica, da vida das pessoas – integram a liberdade de opinião. O humor e a crítica social, ainda quando dirigidos a candidatos em período eleitoral, não podem ser restringidos, antes, legitimam a própria democracia.

É extensa, pois, a jurisprudência desta Corte e a direção que deflui de suas razões é inequívoca: o ordenamento constitucional outorga grande força à liberdade de pensamento e de expressão.

A mesma força, ademais, é outorgada pelos tratados internacionais de direitos humanos, tendo sido cogitado, quando da elaboração do Pacto Internacional de Direitos Civis e Políticos, atribuir valor absoluto à liberdade de ter uma opinião (NOWAK, Manfred. UN Covenant on Civil and Political Rights: CCPR Commentary. Kehl am Rhein: Engel, 2005, p. 445). O texto final do Pacto Internacional de Direitos Civis e Políticos não acolheu, porém, o caráter absoluto do direito de opinião ou de sua expressão. Prevaleceu, assim, a ideia, comum a todos os ordenamentos constitucionais, de que não existem direitos absolutos.

As restrições a esses direitos, ao menos do que se extrai da jurisprudência do Comitê de Direitos Humanos, devem ser cautelosamente justificadas. No termos do Comentário Geral n. 34, as restrições a esses direitos devem ser previstas em lei, ser necessárias e visar à garantia de um relevante interesse público (CCPR/C/GC/34, par. 33).

"Necessária" significa que a medida deve ser mais importante do que "útil", "razoável" ou "desejável", como já indicou a Corte Europeia de Direitos Humanos (The Sunday Times v. United Kingdom, julgamento de 26 de abril de 1979, par. 59) e o interesse público relevante é o que é legitimado pelo próprio Pacto, ou seja, segurança nacional, ordem, moral

ou saúde pública.

In casu, os órgãos de segurança pública e a Procuradoria-Geral da República apontam que o acesso excepcional garante aos agentes de investigação um mecanismo indispensável para a consecução de suas atividades de investigação em casos graves, como já reconheceu a jurisprudência desta Corte para as interceptações telemáticas.

De fato, a legislação brasileira prevê salvaguardas à proteção da privacidade nos casos de interceptação de comunicações, como a excepcionalidade da medida, a restrição apenas para casos mais graves e, finalmente, a reserva de jurisdição.

O próprio Marco Civil da Internet, no art. 7º, II, indica a possibilidade de restrição da privacidade. A dúvida, portanto, não recai sobre a relevância do direito que fundamenta a restrição, em alguns casos, sem dúvidas, elevada, mas a de saber se o que se ganha com o acesso excepcional é modico o suficiente para justificá-la.

O Conflito entre os Direitos de Privacidade e Liberdades de Pensamento e Expressão e a Necessidade de Proteção dos Direitos Fundamentais

Dois tipos de interferência no **direito à privacidade** foram suscitadas em documentos internacionais e em manifestações feitas pelos *amici curiae*: as interferências diretas do governo sobre a ação das pessoas no ambiente digital e a coleta indiscriminada de dados pessoais, por empresas, governos e organizações criminosas.

Em relação às interferência governamentais, o Conselho de Direitos Humanos tem demonstrado preocupação com a exposição de jornalistas e suas fontes, que, juntamente com os defensores de direitos humanos, são alvos frequentes de ações governamentais. Assim, a capacidade de vigilância que a internet pode realizar é vista como uma grande ameaça para a atuação desses profissionais e, por consequência, para os direitos de expressão de todas as demais pessoas (A/HRC/34/L.7/R.1).

No que tange às violações pela coleta indiscriminada de dados pessoais, a doutrina tem apontado que a preocupação decorre da própria

arquitetura do sistema:

> "(...) a relevância constitucional do processamento e da utilização de informação dá-se, portanto, a partir dos seguintes elementos: a) a dependência dos indivíduos em relação à infraestrutura de comunicação e informação; b) os riscos individuais que o processamento e a utilização de informação podem causar; c) a influência do processamento e da utilização de informações no sistema de direitos fundamentais como um todo; e d) a ineficácia de um sistema de proteção *ex post*, baseado meramente na reparação de danos."
>
> (MENDES, Laura Schertel Ferreira. Habeas data e autodeterminação informativa: os dois lados da mesma moeda. Direitos Fundamentais & Justiça, Belo Horizonte, ano 12, n. 39, p. 185-216, jul./dez. 2018. p. 214).

Em resposta a essas violações, as empresas passaram a colocar à disposição dos usuários mecanismos de criptografia e de anonimato. A presente arguição destina-se a investigar, concretamente, se a proteção criptográfica aos direitos à privacidade à liberdade de opinião e à liberdade de expressão pode ser afastada. Conquanto não seja propriamente objeto desta ação, a referência ao anonimato, em sua complementariedade com a criptografia, servirá como *tertium comparationes*. Nesse sentido, o Relator Especial David Kaye chama atenção para o fato de que a criptografia e o anonimato são especialmente úteis para o desenvolvimento e compartilhamento de opiniões, o que geralmente ocorre por meio de comunicações online como o e-mail, mensagens de texto e outras interações (A/HRC/29/32, par. 17).

A criptografia é um meio de proteger a privacidade das pessoas no ambiente digital. A criptografia nada mais é do que um processo matemático de conversão de mensagens, informações ou dados que os torna ilegíveis por qualquer pessoa a não ser o destinatário da mensagem. A criptografia serve, assim, para proteger o conteúdo da mensagem, mas ela não protege os chamados "metadados", como, por exemplo, o endereço de IP. O anonimato visa, precisamente, a evitar a identificação

desses dados. Exemplos de tecnologias empregadas para esse fim (proteção do anonimato) são a criação de redes privadas virtuais (VPNs), serviços *proxy*, e redes *peer-to-peer* (A/HRC/29/32, par. 7, 8 e 9).

De acordo com David Kaye, no relatório já referido nesta manifestação, "a criptografia garante segurança para que os indivíduos possam verificar que suas mensagens são encaminhadas apenas para as pessoas desejadas, sem qualquer interferência ou alteração, e que as comunicações por eles recebidas sejam também confiáveis (A/HRC/23/40 e Corr.1, par. 23)"; já o anonimato visa proteger os indivíduos dos poderes do "metadados", isto é, da coleta em massa de dados, porquanto eles podem especificar o comportamento individual, as relações sociais, as preferências privadas e até mesmo a identidade das pessoas, como o próprio Conselho de Direitos Humanos já teve oportunidade de reconhecer (A/HRC/27/37, par. 19).

Em *obiter dicta*, cumpre indicar que referência à proteção ao anonimato, vista aqui como necessária para a proteção das pessoas na era dos metadados, pode aparentar conflito com a disposição constitucional que, reconhecendo a liberdade de pensamento, veda o anonimato. A vedação constitucional do anonimato não tem, porém, o alcance de impedir ou de inviabilizar a proteção à privacidade. A previsão constitucional constante do art. 5º, IV, "é livre a manifestação do pensamento, sendo vedado o anonimato", tem origem na Primeira Constituição Republicana, mais especificamente, em seu art. 72, § 12. Interpretada pelo constitucionalista e e. Ministro deste Supremo Tribunal Federal João Barbalho, a cláusula alcançava até mesmo o pseudônimo: "a prescrição constitucional envolve também a prohibição do pseudonymo, outro meio de illudir ou dificultar a responsabilidade, e não menos prejudicial" (CAVALCANTI, João Barbalho Uchôa. Constituição Federal Brasileira (1891): Comentada. Brasília: Senado Federal, Conselho Editorial, 2002, p. 321). Fosse verdadeiro o alcance máximo dessa previsão, este Tribunal, em suprema ironia, teria de julgar inconstitucional Stanislaw Ponte Preta. A previsão constitucional deve, pois, ser estritamente interpretada. Tal como indicado por João Barbalho,

a proibição ao anonimato tinha por objetivo assegurar a responsabilidade de quem, abusivamente, desvirtuava a liberdade de expressão. Levando-se em conta o regime de responsabilização ulterior que se aplica à liberdade de expressão, a proibição do anonimato visava apenas assegurar que haveria responsabilidade. Hoje, como ontem, a melhor interpretação constitucional da expressão "vedado o anonimato" é a de, minimamente, garantir a responsabilidade, sempre ulterior, de quem abusa de sua liberdade de expressão ou de opinião. Vale dizer, é à luz da teleologia do comando constitucional, que se deve interpretar eventual restrição à liberdade de pensamento. Assim, desde que assegurada a responsabilização nos casos de abuso, o anonimato *online* não violaria o direito à liberdade de expressão.

No que tange à **liberdade de opinião**, livre de ingerências arbitrárias, é preciso ter-se em conta que a maneira pela qual a opinião se expressa *online* tem particularidades. As pessoas constantemente salvam suas opiniões, *emails*, páginas visitadas, arquivos encontrados na internet e os armazenam em seus computadores pessoais, na nuvem, em arquivos protegidos. As violações desse direito podem ocorrer tanto *offline*, com a intimidação, *bullying*, violências físicas ou psicológicas, quanto *online*, pela negativa de acesso, pela vigilância constante ou campanhas de ódio. O direito à opinião abrange, ainda, o direito à formação de opinião, que é muito próximo do direito de buscar e receber informações. No ambiente digital, esquemas de vigilância constante interferem drasticamente com o livre usufruto desse direito. Esse risco de coleta indiscriminada de informação é também mitigado pela criptografia e pelo anonimato.

Finalmente, a proteção dada pela criptografia e pelo anonimato também são extremamente úteis em locais e cenários em que predominam atividades censórias. A rejeição absoluta à censura feita pela Constituição de 1988 ganha, pois, força com esses mecanismos de proteção. Além disso, porque o direito à liberdade de expressão tem uma dimensão transnacional, a criptografia e o anonimato poderiam ser utilizados para promover a prevalência dos direitos humanos.

É inegável que a garantia a proteção à privacidade e à liberdade de

expressão por meio da criptografia traz riscos à segurança pública. Esse risco é medido pelos aumentos de custos para a realização de investigações criminais, porquanto a capacidade de monitoramento e de interceptação de mensagens é tida como um dos principais – e para alguns crimes até a única – formas de se apurar ilícitos.

Durante a audiência pública, em pergunta dirigida sobretudo aos representantes dos órgãos de segurança, perguntou-se, especificamente, quais os crimes que exigiriam a investigação preferencialmente ou exclusivamente a partir de interceptações. Os representante do Ministério Público Federal, mencionaram, especificamente, pornografia infantil, organizações criminosas, tráfico de drogas e tráfico de armas.

De acordo com o Relatório do Departamento de Justiça dos Estados Unidos, a disseminação de pornografia infantil, que estava praticamente extinta nos anos 80, ressurgiu de maneira significativa por lá. Grandes organizações criminosas utilizam do *Whatsapp* como verdadeiro registro de contabilidade, como a imprensa brasileira tem pioneiramente investigado (https://www.vice.com/pt_br/article/ypnmkv/dos-salveiros-ao-whatsapp-como-o-pcc-usou-as-tecnologias-para-expandir).

Em que pesem, porém, os problemas trazidos por quem abusa da liberdade *online,* "de acordo com os dados disponíveis, o número de casos afetados pela criptografia é pequeno" (LEWIS, James A.; ZHENG, Denis E.; e CARTER, William A. *The Effect of Encryption on Lawful Access to Communication and Data,* disponível em: https://www.csis.org/analysis/effect-encryption-lawful-access-communications-and-data; acesso em 17.05.2020).

No mesmo sentido, David Kaye, no Relatório apresentado ao Conselho de Direitos Humanos, apontou que, não obstante as demandas por acessos especiais à criptografia das empresas de aplicativo, os Governos ainda não demonstraram que o uso criminoso da criptografia constitui uma barreira insuperável para os objetivos das polícias (A/HRC/29/32, par. 42).

De fato, como restou amplamente demonstrado durante a audiência pública, a concessão de privilégios especiais a agentes do governo para o

acesso à criptografia, seja por meio de *backdoors*, seja pela permissão de ataques do tipo *man in the middle*, seja, ainda, pela custódia de chaves (*key escrows*), apresenta riscos graves à segurança de todos. Como advertiu o Professor Diego Aranha durante a audiência pública: o benefício obtido pela redução do proteção criptográfica é negativo. Não há nenhum interesse de segurança de rede na concessão de um acesso excepcional: ele só aumentará a insegurança para os usuários. Além disso, tanto os criminosos, quanto os demais usuários podem simplesmente migrar de sistema, a indicar que qualquer benefício pontualmente estimável é momentâneo.

Não existe acesso apenas para as pessoas boas. *Backdoor* apenas para *good guys* não funciona. Dito de outro modo, de nada adianta deixar a chave debaixo do tapete (Abelson, Harold et al. Keys under doormats: mandating insecurity by requiring government access to all data and communications. In: *Journal of Cybersecurity*, v. 1,n. 1, 2015, p. 73):

> "If law enforcement wishes to prioritize exceptional access, we suggest that they need to provide evidence to document their requirements and then develop genuine, detailed specifications for what they expect exceptional access mechanisms to do."

> "Se os órgãos de segurança querem priorizar o acesso excepcional, nós sugerimos que eles forneçam evidências que documentem sua exigência e que eles desenvolvam especificações genuínas e detalhadas para o quê eles esperam que os mecanismos de acesso excepcional possam fazer" (*tradução livre*).

Outras consequências também relativizam o sucesso de uma iniciativa como essa. Além dos riscos de tornar a vulnerabilidade do sistema explorável por outras pessoas, eventual acesso excepcional de um aplicativo faria com que os usuários migrassem em direção a outros, mais seguros. No caso de criminosos, a consequência provável, como se teve

oportunidade de debater na audiência pública, é de optarem por sistemas ainda mais restritos, ainda mais difíceis de serem rastreados, quando não sistemas que poderia, quiçá, ser tidos por ilegais.

É contraditório, portanto, que em nome da segurança pública deixe-se de promover e buscar uma internet mais segura. Uma internet mais segura é direito de todos e dever do Estado. Medidas que, à luz da melhor evidência científica, trazem insegurança aos usuários somente se justificam se houver certeza comparável aos ganhos obtidos em outros áreas. Não é isso, porém, o que ocorre. **O risco causado pelo uso da criptografia ainda não justifica a imposição de soluções que envolvam acesso excepcional.**

À luz de todas essas considerações, poder-se-ia, então, questionar se a criptografia ponta-a-ponta poderia ser restrita apenas a agentes de governo, isto é, se seria possível proibir o acesso da criptografia aos todos os cidadãos. A resposta, aqui, seria negativa. Além de promover aspectos fundamentais da vida humana como a proteção à integridade, ao sigilo, à confidencialidade, à autenticidade e à privacidade das mensagens transmitidas, a criptografia assegura um acesso mais justo a pessoas que estão em situação de vulnerabilidade.

Padrões sistemáticos de vigilância e mensagens dirigidas impactam desproporcionalmente essas pessoas, seja porque têm menos acesso aos meios de proteção, seja porque barreiras impedem seu acesso a essas ferramente em absoluta condição de igualdade.

Em síntese, **é inconstitucional proibir as pessoas de utilizarem a criptografia ponta-a-ponta, pois uma ordem como essa impacta desproporcionalmente as pessoas mais vulneráveis**.

É importante frisar, por fim, que o reconhecimento de um direito constitucional à criptografia forte não diminui nem isenta as empresas que produzem os aplicativos de se conformarem com a legislação brasileira, nem a descumprirem as ordens judiciais que, na medida da estrita proporcionalidade, exijam a entrega de dados que não dependam da quebra de criptografia.

Nada do que aqui se assentou exime as empresas de adotarem

medidas que visem reduzir a prática de ilícitos, especialmente os que ocorrem por meio de seus canais de comunicação. A criptografia não autoriza o desvirtuamento deliberado de campanhas eleitorais, a disseminação de discurso de ódio e o envio indiscriminado de materiais ofensivos. O interesse em uma internet mais segura é também o de uma sociedade mais segura. Todos – governo, cidadãos e empresas – devem colaborar para sua plena realização.

Para combater esse tipo de violação – e apenas para ela – a legislação previu as sanções do art. 12, III e IV, do Marco Civil da Internet. Normativamente, ela deveria ser aplicada pela Autoridade Nacional de Proteção de Dados, nos termos do art. 55-J, IV, da Lei 13.709, de 2018 (Lei Geral de Proteção de Dados Pessoais). Há, portanto, a obrigação legal e há mecanismos sancionatórios próprios para responsabilizar as empresas que violarem os direitos à privacidade e à liberdade de expressão e opinião.

Não se desconhece que, lamentavelmente, a Autoridade Nacional ainda não foi instalada. Neste ponto, é de todo pertinente a crítica formulada pelo Min. Gilmar Mendes, quando do julgamento da ADI 6.389:

> "Sobre esse último ponto, não há como deixar de observar que, no caso brasileiro, malgrado ter transcorrido mais de um ano da promulgação da LGPD, ainda não foram adotadas medidas legislativas para instituição da Autoridade Nacional de Proteção de Dados.
>
> Esse quadro de baixa institucionalidade de um regime efetivo de proteção de dados pessoais no Brasil tem sido agravado por iniciativas normativas recentes, e como a Medida Provisória 959, publicada no Diário Oficial da União de 29.4.2020, que adiou, mais uma vez, a Lei Geral de Proteção de Dados (LGPD). A previsão agora é de que ela entre em vigor apenas em 3 de maio de 2021."

Essa omissão em institucionalizar um regime efetivo de proteção de

dados, omissão verdadeiramente inconstitucional, poderá, a tempo e modo ser resolvida pela jurisdição brasileira, desde que provocada.

Seja como for, a suspensão das atividades do aplicativo ou mesmo sua proibição, mesmo diante da baixa institucionalidade, não caberá para o caso de descumprimento de decisão judicial de quebra de criptografia, mas para um quadro de violação grave do dever de obediência à legislação. Não é preciso minudenciar, mas é evidente que mesmo aqui a sanção deverá observar a proporcionalidade, tendo sempre em conta o direito do usuário de não ter suspenso seu acesso à internet. É certo, pois, que **não cabe aos juízes que ordinariamente autorizam as interceptações telemáticas aplicar a sanção prevista no art. 12, III, do Marco Civil da Internet.**

Essa interpretação, no entanto, só é posta em dúvida, caso se admita a possibilidade de se determinar o enfraquecimento da criptografia, ou, para o caso do *WhatsApp*, de se determinar a disponibilização do **conteúdo** das mensagens. Reconhecendo, tal como se fez nesta manifestação, que os juízes não podem determinar o acesso excepcional ao conteúdo de mensagem criptografada, não é necessária a declaração de inconstitucionalidade ou a fixação de interpretação conforme do art. 12, III, do Marco Civil, porque o único sentido da norma é precisamente o que já está garantido pelo ordenamento, qual seja, o de que cabe à Autoridade Nacional e não ao Judiciário a decisão sobre a suspensão do aplicativo.

Por todo o exposto, **julgo procedente** a presente arguição de descumprimento de preceito fundamental para declarar a inconstitucionalidade parcial sem redução de texto tanto do inciso II do art. 7º, quanto do inciso III do art. 12 da Lei 12.965/2014, **de modo a afastar qualquer interpretação do dispositivo que autorize ordem judicial que exija acesso excepcional a conteúdo de mensagem criptografada ponta-a-ponta ou que, por qualquer outro meio, enfraqueça a proteção criptográfica de aplicações da internet**.

Registro que a procedência da arguição é total, pois, nos termos da fundamentação, não é constitucionalmente admissível a suspensão do

aplicativo de mensagens *WhatsApp* por decisão judicial.

Por fim, gostaria de pontuar, não sem antes elogiar a brilhante manifestação feita pela e. Ministra Rosa Weber, a divergência com o voto que veio de ser proferido por Sua Excelência.

O aplicativo *WhatsApp* não permite que o **conteúdo** das comunicações trocadas entre os usuários seja disponibilizado, porque isso exigiria que o aplicativo alterasse seu sistema de criptografia, introduzindo uma vulnerabilidade em seu sistema.

Com as vênias da e. Min. Rosa Weber, ordens judiciais, ainda que para fins de investigação criminal ou instrução processual penal – como ocorre nas ações que são impugnadas na presente arguição –, não podem determinar que o aplicativo de internet modifique seu sistema de criptografia. Daí porque a necessidade de inconstitucionalidade sem redução de texto do art. 7º, II, e 12, III, ambos do Marco Civil da Internet, para a afastar qualquer interpretação do dispositivo que autorize ordem judicial que exija acesso excepcional a conteúdo de mensagem criptografada ponta-a-ponta ou que, por qualquer outro meio, enfraqueça a proteção criptográfica de aplicações da internet.

A necessidade de declaração de inconstitucionalidade é bem explicitada por Jacqueline de Souza Abreu (Passado, presente e futuro da criptografia forte: desenvolvimento tecnológico e regulação. *In:* Revista Brasileira de Políticas Públicas, v. 7, n. 3, dez de 2017, p. 34), ao identificar que inexiste no Marco Civil a obrigação explícita de que aplicações de internet tenham habilidade de quebrar sigilo ou, como se defende nesta manifestação, de proteger uma criptografia forte:

> "Quando [o Marco Civil da Internet] obriga que empresas retenham informações, o dever se estende apenas a registros (IP, data e hora de acesso), o que as obriga a, necessariamente, ser capazes de atender a pedidos de quebra de sigilo apenas desses metadados (art. 15). Portanto, o dever jurídico, extraído do direito brasileiro vigente, de que aplicações de internet sejam capazes de quebrar sigilo de conteúdo de comunicações não é evidente; carece de fundamentação — e pode muito bem ser

que a conclusão seja de que não exista".

Por entender que o risco causado pelo uso da criptografia ainda não justifica a imposição de soluções que envolvam acesso excepcional ou ainda outras soluções que diminuam a proteção garantida por uma criptografia forte, penso que não há como obrigar que as aplicações de internet que ofereçam criptografia ponta-a-ponta quebrem o sigilo do conteúdo de comunicações, ao menos à luz das informações que traduzem o consenso científico atual sobre a matéria.

De acordo com o meu voto, eliminada do ordenamento a interpretação que autorize o acesso excepcional, entendo ser dispensável a interpretação conforme para impedir as ordens de bloqueio por decisões judiciais. Se o Poder Judiciário não pode determinar a interceptação do fluxo, tampouco poderia sancionar eventual descumprimento da ordem.

Estou convencido, tal como a e. Ministra Rosa Weber, que a sanção de suspensão apenas tem lugar quando os aplicativos de internet tiverem violado os direitos de privacidade dos usuários. Estou convencido, ainda, que, à luz do disposto no art. 55-J, IV, da Lei 13.709, de 2018 (Lei Geral de Proteção de Dados), compete à Autoridade Nacional de Proteção de Dados a aplicação da sanção, que poderá até mesmo levar em conta decisões judiciais não cumpridas, quando as ordens forem **legitimamente** formuladas. Penso, porém, quanto a esse ponto, que é inequívoco o sentido da norma, a dispensar a interpretação conforme.

Em síntese, senhor Presidente e eminentes pares, no atual estágio de desenvolvimento da internet, a criptografia forte é, de acordo com as principais evidências científicas, o mecanismo por excelência de garantia do relevantíssimo direito à privacidade. É possível que, com os avanços da tecnologia, esse mecanismo de proteção venha a se tornar obsoleto. É possível, ainda, que novas evidências venham a demonstrar a imprescindibilidade de mecanismos de interceptação do conteúdo de mensagens. Por ora, penso que esta Corte deva reconhecer que fragilizar a criptografia é enfraquecer o direito de todos a uma internet segura.

É como voto.