Rodrigo Gomes Paixão

O SUPREMO TRIBUNAL FEDERAL E A REGULAÇÃO JUDICIAL DA CRIPTOGRAFIA: diálogos entre a Suprema Corte e a Audiência Pública nº21

Monografia apresentada à Escola de Formação da Sociedade Brasileira de Direito Público - SBDP, sob orientação de João Pedro Favaretto e tutoria de Rafaella Navas e Júlia Gabrielle.

SÃO PAULO

2020

AGRADECIMENTOS

Sou grato, acima de tudo, a Deus. Dentre todos os detalhes que me impediram de ceder neste ano, talvez ao longo de minha vida, minha fé foi o mais importante.

Em segundo lugar, agradeço a você, mãe. Desde cedo nossa trajetória foi difícil e você foi a única família que tive. A ausência de um pai me colocou numa família mais tradicional que qualquer dita família tradicional: um filho e uma mãe. Mas você esteve comigo, e isso é tudo o que importa. Você esteve comigo, me observando todo dia, quando eu ria, quando chorava, quando pedia ajuda e quando sofria em silêncio. Em todos esses momentos, você estendeu sua mão, seja para me levantar quando caí, seja para erguer meu braço aos céus quando venci.

Obrigado, mãe. Obrigado, Valdeci. Você foi e é fundamental.

Não me esquecerei de meu orientador, João Pedro e de minhas tutoras, Rafaella Navas e Júlia Gabrielle. Acredito que a palavra que norteou nossa relação foi equilíbrio. Por sorte, por Deus ou por pura ironia do destino, recebi duas tutoras, muito mais do que merecia, mas exatamente o que eu precisava. Tive poucos momentos de conversa com vocês, poucas interações, mas quando eu precisei, vocês estiveram lá. Nem em uma fração mais ou menos do que eu precisei. Por isso eu só agradeço e peço ao tempo que fixe suas presenças em minha vida.

O período foi atípico, de pandemia. O distanciamento físico concretizou todo o distanciamento emocional que sempre vivemos e nunca nos demos conta. O mundo é caótico e difícil, nos digladiamos por empregos ruins, por relacionamentos ruins, por pouco amor. A vida as vezes parece se resumir a sobreviver. Encontrar algo que valha a pena nessa realidade é raro, mas é possível. E quando isso ocorre é emocionante e é importante que guardemos essa conquista com carinho. Por isso que agradeço às pessoas que foram "achados de felicidade" para mim.

Para além daqueles que já são constantes em minha jornada, quero

lembrar de duas pessoas especiais que conheci com a SBDP: Taís e Alice. Taís, obrigado por ter sido amiga, por ter me compreendido e relevado minhas falhas e exageros. Obrigado por me fazer não me sentir excluído. Você sabe como foi difícil para mim.

Alice, que seus dias sejam lindos como muitos dos meus foram por sua causa. Você é tinta, pincel e a vida é um quadro. Que você seja arte.

Aos que leram até aqui, asseguro que não me alongarei muito mais. Me dou o direito deste desabafo porque foi tanto esforço e luta para vencer o desgaste emocional e físico neste ano, o distanciamento, as frustrações, as perdas, foi tanto... eu apenas preciso de alguns parágrafos para expor o que guardo em meu peito. Não peço que leia, apenas que compreenda.

E como Emicida diz, a vida é só um detalhe. E esse ano foi só um detalhe. Minhas dificuldades são só um detalhes. Este trabalho foi só um detalhe. Apesar disso, são os detalhes, as pequenas coisas que constroem as grandes conquistas. E sobreviver a 2020, definitivamente, não foi só um detalhe.

RESUMO

Mais de 120 milhões de pessoas usam o WhatsApp no Brasil. Os impactos da suspensão de suas atividades seriam gigantescos. Desde aqueles que usam o aplicativo para trabalhar até os que se comunicam com pessoas próximas restariam prejudicados. E isso aconteceu, mais de uma vez. O motivo dos bloqueios, por sua vez, pode ser resumido em uma palavra: criptografia. Este, porém, não é um vocábulo comum do dia a dia jurídico. Para discutir os aspectos das suspensões do aplicativo WhatsApp e dos dispositivos legais que fundamentaram as suspensões, foram impetradas, respectivamente, a ADPF 403 e a ADI 5527 no Supremo Tribunal Federal. Como reação, para entender o que é criptografia e qual sua relação com os bloqueios, os ministros-relatores das referidas ações convocaram a Audiência Pública nº 21. Dessa maneira, a monografia pretende discutir e analisar os votos proferidos no julgamento conjunto dessas ações, tentando traçando os diálogos que eles estabeleceram com as exposições da audiência. O objetivo maior é descobrir de quais formas os conceitos tecnológicos influenciaram votos jurídicos na Suprema Corte nacional.

Palavras-chave: Criptografia; Audiência Pública nº 21 do Supremo Tribunal Federal; Ministros relatores; Expositores; ADI 5527; ADPF 403.

LISTA DE SIGLAS

ADI	Ação Direta de Inconstitucionalidade
ADPF	Arguição de Descumprimento de Preceito Fundamental
CF	Constituição Federal
MCI	Marco Civil da Internet
MPF	Ministério Público Federal
PF	Polícia Federal
STF	Supremo Tribunal Federal

Sumário

INTRODUÇÃO

Em dezembro de 2015, a juíza Sandra Regina Nostre Marques, da 1ª Vara Criminal de São Bernardo do Campo, determinou o bloqueio [1] do WhatsApp em todo o Brasil como forma de sancionar sua empresa controladora por descumprir ordens judiciais de acesso a dados de usuário. A ordem foi emitida para auxiliar na investigação de tráfico de drogas. Foi solicitada a interceptação de mensagens do WhatsApp de três contas de suspeitos. A empresa foi notificada duas vezes e, após o descumprimento a decisão, foi feito o pedido de bloqueio pelo Ministério Público[2].

Pouco se sabe sobre o fundamento desta decisão, uma vez que ela está em sigilo, mas se sabe que ela foi a *primeira* decisão de bloqueio do WhatsApp que foi *efetivamente* implementada. Logo em seguida, a WhatsApp Inc. ingressou com o mandado de segurança nº 2271462-77.2015.8.26.0000 contra a decisão, que foi deferido pelo desembargador Xavier de Souza, do Tribunal de Justiça de São Paulo.

Em abril do ano seguinte (2016), um juiz da Vara Criminal de Lagarto (SE) determinou novo bloqueio[3] do WhatsApp em todo o Brasil, outra vez como sanção pelo descumprimento de ordens de interceptação.

A Polícia Federal havia pedido o bloqueio do aplicativo WhatsApp por 72h pelo fato de a empresa Facebook ter atrasado o cumprimento da ordem

[1] Justiça manda bloquear WhatsApp por 48 horas a partir desta quinta-feira (2015). Disponível em:https://agenciabrasil.ebc.com.br/geral/noticia/2015-12/justica-manda-bloquear-whatsapp-por-48-horas-partir-desta-quinta-feira.

[2] Essa não foi a primeira vez que um site ou serviço ficou fora do ar devido a uma decisão judicial. Uma das decisões mais relevantes que foi, inclusive, um dos fatores que motivaram a criação do Marco Civil da Internet, ocorreu em 2007 com a suspensão temporária do YouTube. A suspensão ocorreu por conta de um processo envolvendo uma celebridade brasileira que teve um vídeo de momento íntimo gravado e compartilhado no YouTube. Após diversas tentativas sem êxito de tornar o vídeo indisponível, um juiz ordenou que o acesso à plataforma fosse suspenso. Assim, usuários do Brasil inteiro ficaram privados de acessar o YouTube por algumas horas, até que o mesmo juiz revogou a decisão. (SOUZA, BRANCO 2016). Disponível em: https://goo.gl/nLe8Xe Acesso em: 20 out. 2020.

[3] Justiça determina bloqueio do WhatsApp em todo o Brasil por 72 horas (2016). Disponível em: https://veja.abril.com.br/tecnologia/justica-determina-bloqueio-do-whatsapp-em-todo-o-brasil-por-72-horas/

de interceptação de mensagens em tempo real pelo aplicativo, fundamentando o pedido no art. 12, III, do Marco Civil da Internet (Lei 12.965/2014).

Dessa vez, os alvos da investigação eram 36 usuários que estavam supostamente envolvidos em uma organização criminosa que patrocinava o tráfico interestadual de drogas. A Polícia Federal apresentou um parecer, acolhido pelo Juiz, que tratava sobre a possibilidade de interceptação das mensagens, apesar dos limites técnicos alegados pelo WhatsApp.

O WhatsApp Inc. respondeu ao bloqueio impetrando o mandado de segurança nº 201600110899, no qual declarava, dentre outras questões, a impossibilidade técnica de interceptação das mensagens privadas pelo aplicativo.

Após mais de 24h de bloqueio e diante do caos que a interrupção dos serviços do WhatsApp causou, o desembargador responsável concedeu a liminar[4] de suspensão do bloqueio.

Estas foram duas das três primeiras decisões de bloqueio afetando o aplicativo, sendo as duas primeiras a serem efetivamente executadas. Depois desses eventos, houve um novo bloqueio do WhatsApp[5].

Nesse meio tempo, houve a propositura da ADPF 403 pelo Partido Popular Socialista (PPS) [6] , que questiona se há violação à liberdade de comunicação quando o bloqueio de aplicativos de mensagens é determinado, e da ADI 5527, proposta pelo Partido da República (PR)[7] que contesta a constitucionalidade dos incisos III e IV do art. 12 do Marco Civil da Internet utilizados para fundamentar os bloqueios.

[4] Suspensão do bloqueio do WhatsApp, (2016). Disponível em: http://www.omci.org.br/jurisprudencia/97/suspensao-do-bloqueio-do-whatsapp
[5] Descumprimento de ordem judicial de entrega de dados, (2016). Disponível em: http://bloqueios.info/pt/casos/bloqueio-por-descumprimento-de-ordem-judicial-de-entrega-de-dados-2/
[6] Partido pede que STF suspenda decisão judicial que bloqueou WhatsApp, (2016). Disponível em: https://www.conjur.com.br/2016-jul-19/partido-stf-suspenda-decisao-bloqueou-whatsapp
[7] Questionados artigos do Marco Civil da Internet que permitem bloqueio de aplicativos, (2016). Disponível em: http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=317478&caixaBusca=N

No dia 27 de outubro de 2016, a Min. Rosa Weber e o Min. Edson Fachin, relatores das ações supramencionadas, convocaram conjuntamente a uma Audiência Pública para tratar do tema. Esta se deu no dia 02 de junho de 2017. Na convocação, os ministros estabeleceram quatro perguntas norteadoras para a audiência (que serão explicitadas a frente). Todas elas tratavam sobre criptografia.

Urge, então, a questão: qual seria a relação do bloqueio de aplicativos de comunicação com criptografia? E mais, por que o STF convocou uma Audiência Pública que trata, em sua maioria, sobre criptografia se o caso é sobre bloqueio de aplicativos?

Os bloqueios executados seguiam certo padrão: 1) era determinada a interceptação dos dados; 2) a empresa informava *impossibilidade* do atendimento da ordem judicial; 3) por conta da inércia no atendimento, era determinada a suspensão das atividades do aplicativo.

O WhatsApp, em todas as oportunidades de se defender judicialmente das ordens de bloqueio, alegou que descumpria a ordem de interceptação por impossibilidade técnica, visto que o tipo de *criptografia* adotada pelo aplicativo tornava impossível realizar o pedido.

Essa foi uma das motivações da audiência pública. A premissa de sua convocação foi a necessidade de entender o que é criptografia, qual a espécie de criptografia adotada pelo WhatsApp e se as alegações dadas pela empresa eram verdadeiras. Compreender estes conceitos, além de ser imprescindível para a decisão dos Ministros relatores, é requisito para que o leitor compreenda melhor o exposto nesta monografia, os debates ocorridos e a relação da tecnologia criptográfica com o bloqueio de aplicativos. De tal forma, explicarei a seguir o que é criptografia e como funciona a espécie de criptografia adotada pelo WhatsApp.

Criptografia é uma técnica para cifrar dados a partir de um código (chave), tornando-os impossíveis de serem entendidos por agentes que não o detêm. É uma forma de codificar certas informações.

Assim, ela atua para evitar a exposição de dados sigilosos como senhas, proteger informações contidas em transações bancárias e blindar os

diversos meios modernos de comunicação, como trocas de e-mails e as trocas de mensagens.

No âmbito do WhatsApp, mais especificamente nos aplicativos de comunicação criptografados, falamos que ela atua para que as mensagens trocadas pelos usuários não possam ser compreendidas por terceiros. Elas se tornam *ininteligíveis*[8]*.*

Uma vez entendido o que é criptografia, é preciso entender como funciona o tipo de criptografia adotado pelo WhatsApp, que é a "criptografia de ponta a ponta".

Nela, a mensagem é cifrada em sua origem e só será decifrada no destino. O nome torna a compreensão um pouco mais intuitiva: "ponta a ponta". Apenas as pontas da comunicação (quem envia a mensagem e quem a recebe) poderão ter acesso ao conteúdo decifrado. Mas, para ter acesso, é preciso que as próprias mensagens criptografadas sejam descriptografadas e, para isso, o WhatsApp adota um sistema de chaves.

Cada pessoa possui um par de chaves complementares. O Emissor, ao enviar, tem sua mensagem cifrada por uma chave que chamamos "pública". Ela tem esse nome pois todos têm acesso à chave usada para cifrar a informação. Entretanto, para decifrar a informação, é preciso uma chave "privada", que apenas e tão somente as partes possuem em seus celulares.

Assim, imaginemos que "A" deseje enviar uma mensagem a "B". "A" escreverá a mensagem e usará a sua chave pública para cifrá-la. Todos saberão qual a chave necessária para cifrar a mensagem, pois ela é pública, mas isso não faz com que eles saibam qual é a mensagem, nem que consigam decifrá-la. Quando a mensagem chegar a "B", este usará sua chave privada - a qual apenas "B" tem acesso - para decifrar o conteúdo, viabilizando a comunicação.

Cabe ressaltar que o WhatsApp gera uma única chave de encriptação para *cada* mensagem. Isso significa que a cada mensagem enviada, uma

[8] "Que não se entende". *Dicionário Houaiss da língua portuguesa*. Rio de Janeiro: Objetiva, 2009.

chave diferente é utilizada, o que torna as comunicações mais seguras ainda, porque, se de algum modo alguém tiver acesso a uma chave privada, ela só servirá para decifrar uma única mensagem, não podendo ser usada para decifrar as mensagens anteriores.

Os bloqueios aconteceram porque o WhatsApp descumpriu ordens de interceptação de mensagens, mas ele alegadamente só o fez porque, como as chaves privadas, responsáveis por decifrar o conteúdo criptografado, são geradas a cada mensagem e apenas ficam com as pontas da comunicação, em tese, ninguém além dos usuários-pontas da comunicação, nem mesmo o próprio WhatsApp, conseguiria ter acesso às mensagens sem que a criptografia fosse enfraquecida.

Podemos, agora, responder a uma nova pergunta: por que é importante que o STF entenda se a criptografia pode e/ou deve ser enfraquecida para julgar a constitucionalidade do artigo 12 do MCI?

Os fundamentos usados para a ordem judicial de bloqueio estão no art. 10, § 1º do MCI[9]:

> Art. 10. A guarda e a disponibilização [...] 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** [...] **mediante ordem judicial** [...] (grifos nossos)

Foi com base nesses trechos que foi requerido que o WhatsApp disponibilizasse conteúdo de comunicações privadas de usuários-réus no processo criminal.

[9] BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília. 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

A empresa não forneceu os dados e foi, primeiramente, multada para depois ter suas atividades suspensas, com base no inciso II do artigo 12 da mesma lei.

> Art. 12. Sem prejuízo das demais sanções cíveis, criminais ou administrativas, **as infrações às normas previstas nos arts. 10** e 11 **ficam sujeitas**[...] **às seguintes sanções** [...]
>
> II – **multa** [...]; III - **suspensão temporária das atividades** que envolvam os atos previstos no art. 11[101];(grifos nossos)

Conforme os artigos mencionados, o provedor é obrigado a disponibilizar os registros de comunicação, podendo ser alvo de sanções caso não o faça. Entretanto, se for impossível tecnicamente que o provedor realize o pedido, não há razão em puni-lo porque a sanção não só não resolverá o problema em nenhuma ordem.

Por isso é importante que o STF entenda se a criptografia pode ou deve ser enfraquecida. E, com isso em mente, a audiência pública se mostra não apenas necessária, mas fundamental. Se não fosse possível a interceptação, ao menos no âmbito da comunicação por aplicativos que usam a criptografia de ponta a ponta, as sanções perderiam sua razão de ser.

Disso, depreendi que seria um importante questionamento saber "se, e como os votos dos ministros relatores na ADI 5527 e ADPF 403 dialogaram com as contribuições dos expositores da audiência pública n.21 no que diz respeito à regulação judicial da criptografia".

Dada a importância do debate, saber se os ministros seguiram as tendências apresentadas na audiência, concordaram ou discordaram dos expositores e como o fizeram é extremamente relevante. Falo "regulação judicial" [11]porque não há, ao momento em que escrevo, previsão legal no

[10] Apenas a título de esclarecimento, o art. 11, mencionado no inciso segundo do art. 12, MCI, traz em seu bojo "**qualquer operação [...] de comunicações".**

[11] "De forma análoga, no Brasil, possíveis regulações do Legislativo, ou a decisão do STF que julgue a constitucionalidade das medidas de bloqueio, podem gerar consequências diretas na adoção de criptografia forte por estes serviços". (LIGUORI FILHO, SALVADOR, 2018)

ordenamento brasileiro sobre criptografia, de forma que a decisão da Suprema Corte ditará os moldes desta regulação.

1. Metodologia

Do já exposto é possível compreender a relação da criptografia de ponta a ponta com os bloqueios e com as ações impetradas. Todo o caráter técnico desse debate motivou os Ministros relatores Edson Fachin e Rosa Weber a convocar a Audiência Pública nº 21.

A relação estabelecida corroborou na pergunta de pesquisa: "se, e como os votos dos ministros relatores na ADI 5527 e ADPF 403 dialogaram com as contribuições dos expositores da audiência pública n.21 no que diz respeito à regulação judicial da criptografia"?

O presente texto, então, tem como fim maior averiguar as formas com que a sociedade (expositores da audiência) reverberou no mundo jurídico (votos dos relatores) no que tange a criptografia, os bloqueios e as ações impetradas.

Com isso, foi definido o primeiro passo: procurar a transcrição da audiência pública, pois não seria possível estabelecer como foi o diálogo sem entender a audiência em si. Para tal, bastou seguir a seguinte sequência de abas no sítio do STF: Processos > Audiências Públicas > Realizadas. Isso resultou numa página com informações sobre as 30 Audiências Públicas já realizadas pelo Supremo, dentre elas, a que interessa à presente monografia - Audiência pública nº 21: "Marco Civil da Internet e Suspensão do aplicativo WhatsApp por Decisões Judiciais no Brasil" [12] . Esta página continha informações sobre a audiência, de sua transcrição.

Com a transcrição da audiência em mãos, nova busca foi efetuada visando a transcrição dos votos dos Ministros Relatores, porque o foco da pergunta de pesquisa repousa sobre eles. O objetivo foi contemplado

[12]Disponível em: http://www.stf.jus.br/portal/audienciaPublica/audienciaPublica.asp?tipo=realizada

buscando a palavra "criptografia" no sítio do STF, na aba notícias, o que resultou em uma sequência de matérias jornalísticas.

Duas delas, intituladas "Relatores consideram inconstitucional quebra do sigilo de comunicação em aplicativos de mensagens"[13] e "Relatora entende que aplicativos de mensagens não podem ser obrigados a fornecer dados criptografados"[14] continham, respectivamente, a transcrição do voto do min. Edson Fachin para a ADPF 403 e da min. Rosa Weber para a ADI 5527.

Obtidos os materiais, o próximo passo foi lê-los e buscar uma forma de catalogá-los. Primeiramente, separei nos arquivos dos votos dos ministros relatores os trechos que tratavam sobre criptografia e segurança de dados (direta ou indiretamente)

O segundo passo foi ler a transcrição da audiência para desenvolver sua forma de classificar o que foi dito pelos expositores. Ao longo da leitura, defini a primeira classificação, que foi simples e ampla, apenas para fins de organização: Expositor – Textos. Dessa forma, separei os nomes de todos os expositores da audiência em tópicos. Dentro de cada um deles, coloquei suas respectivas exposições no que tangia a criptografia.

A segunda classificação, também ampla, tratava sobre argumentos a favor e contrários à manutenção da criptografia forte. Nos argumentos a favor foram inclusas quaisquer exposições que abrangessem pontos antagônicos ao enfraquecimento da criptografia ou que expusessem consequências negativas das medidas desse tipo, ou seja, tudo aquilo que se mostrasse em algum nível a favor a manutenção da criptografia forte, não só a de ponta a ponta, e que se mostrasse contrário às sanções judiciais impostas ao WhatsApp. Nos contrários, por sua vez, foram inclusas quaisquer exposições que fossem propusessem ou defendessem o enfraquecimento da criptografia adotada pelo Whatsapp.

[13] Relatores consideram inconstitucional quebra do sigilo de comunicação em aplicativos de mensagens, (2020). Disponível em: https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=444384&ori=1

[14]Relatora entende que aplicativos de mensagens não podem ser obrigados a fornecer dados criptografados (2020). Disponível em: https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=444265&ori=1

A terceira classificação se deu por temas-chave. Ela foi usada para selecionar os principais tópicos técnicos abordados e identificar quais deles seriam mais úteis à presente monografia. Após ler todos os documentos novamente, depreendi que a melhor forma de responder à pergunta de pesquisa seria organizando a audiência, inicialmente, pelas hipóteses de enfraquecimento apresentadas pelos expositores.

Isso porque a maioria dos expositores argumentaram sobre possibilidade de interceptação das mensagens e sobre a viabilidade do *enfraquecimento* da criptografia de ponta a ponta para fins de investigações criminais. Eles partiam das perguntas dos Ministros e sempre chegavam a duas hipóteses de interceptação principais: *Man-in-the-middle e Backdoors*. Os expositores se diziam favoráveis ou contrários ao enfraquecimento a partir dessas hipóteses e justificavam seus posicionamentos a partir disso.

Ademais, tais hipóteses traziam consigo consequências distintas e informações que não necessariamente se relacionavam de forma consistente a ponto de estarem juntas num mesmo tópico. Questões assim me fizeram concluir que seria melhor abordar tais hipóteses individualmente para que a monografia dialogasse melhor com a audiência e a compreensão fosse facilitada.

Além destas duas, determinou-se uma terceira e última hipótese, que é "desabilitar o uso de chaves privadas para apenas um usuário"*.* Essa questão foi levantada na convocatória da audiência pública, como veremos a seguir.

Mesmo se relacionando com as duas hipóteses que a precederam, esta última trouxe pontos relevantes que não foram bem abordados por elas, o que me levou a decidir trazê-las separadamente. O fiz de forma a evitar que a compreensão fosse prejudicada ou que faltassem informações ao debate.

Essa forma de organização e apresentação das falas permite uma visão holística pelo leitor, que facilita as comparações com os votos dos Ministros. Dessa forma, "Da audiência pública" figurará como o capítulo 2, que será dividido entre tais hipóteses.

Uma vez definidos os três âmbitos de análise da audiência, decidi separar os dois primeiros em argumentos favoráveis e contrários ao tema principal – enfraquecimento da criptografia.

O terceiro tópico não foi dividido da mesma maneira que os anteriores. Isso porque não houve uma "separação" entre argumentos favoráveis ou contrários a essa hipótese na audiência, mas apenas breves constatações de poucos expositores.

Para que o leitor se situasse melhor, antes de cada uma das hipóteses de enfraquecimento, decidi apresentar breve introdução do contexto da audiência pública e, após as três, conclusões preliminares. Com isso, a estruturação do capítulo 2 foi a seguinte:

2. Da audiência pública

2.1. O que foi e expositores

2.2. Hipóteses de enfraquecimento da Criptografia

2.2.1 Hipótese do *man-in-the-middle*

2.2.1.1 Argumentos Favoráveis

2.2.1.2 Argumentos Contrários

2.2.2. Hipótese dos *backdoors*

2.2.2.1 Argumentos Favoráveis

2.2.2.2 Argumentos Contrários

2.2.3. Desabilitar as chaves privadas para apenas um usuário

2.3. Conclusões Preliminares

Ao encerrar a análise da audiência pública, o foco restaria nas escolhas metodológicas para os votos dos Ministros Relatores, de forma que fosse estabelecido o diálogo com o dito na audiência, objetivo da pesquisa.

Uma das formas de fazê-lo seria dividir os votos em pontos favoráveis e contrários ao enfraquecimento e conclusão, seguindo uma estrutura parecida com a estabelecida para alguns dos tópicos do capítulo precedente.

Porém, a minha escolha metodológica aqui foi mais simples: seguir a ordem de exposição dos ministros e relacionar ponto a ponto com os expositores.

Essa linha metodológica conserva, de certa forma, a linha de raciocínio e ordem interna dos votos dos ministros, o que faria mais sentido, uma vez que o foco do trabalho são seus votos, não os argumentos favoráveis e contrários. Além disso, dessa maneira foi possível constatar em quais momentos do voto eles mencionaram os dados da audiência e com qual frequência o fizeram.

Dessa maneira, a divisão de tópicos foi a seguinte:

3. Dos Votos dos Relatores

3.1. Rosa Weber

3.2. Edson Fachin

Como dito, a análise dos votos seguirá a ordem de exposição dos argumentos pelos ministros relatores, de forma a, a cada ponto relevante, ser traçada relação com o exposto na audiência pública. Mesmo que em segundo plano, algumas relações entre os dois votos poderão ser estabelecidas, a depender do caso.

De todo o dito, exponho aqui a estrutura completa do trabalho:

INTRODUÇÃO

1. Metodologia

2. Da audiência pública

2.1. O que foi e expositores

2.2. Hipóteses de enfraquecimento da Criptografia

2.2.1 Hipótese do *man-in-the-middle*

2.2.1.1 Argumentos Favoráveis

2.2.1.2 Argumentos Contrários

2.2.2. Hipótese dos *backdoors*

2.2.2.1 Argumentos Favoráveis

Conforme determinado neste capítulo, sigo agora com a presente monografia analisando, primeiramente, a audiência pública.

2. Da audiência pública

2.1. O que foi e expositores

Em 27/10/2016 o Ministro Edson Fachin convocou audiência pública no âmago da ADPF 403, visando discutir a suspensão do aplicativo WhatsApp por decisões judiciais no Brasil. Por conta da grande proximidade entre a discussão posta na ADPF 403 e o objeto da ADI 5.527, como visto na introdução, o escopo da audiência foi ampliado de forma a comportar as questões constitucionais postas nas duas ações.

Assim, juntos, a ministra Rosa Weber e o ministro Edson Fachin marcaram a audiência pública para os dias 2 e 5 de junho. Eles selecionaram, dentre os 182 pedidos de participação, 23 especialistas[15] e representantes de entidades para participar dos debates além de demais interessados na audiência.

[15] Definidos participantes e cronograma da audiência pública sobre WhatsApp e Marco Civil da Internet (2017). Disponível em: http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=341437

Segue a lista de participantes:

1) WhatsApp Inc. – Brian Acton, confundador
2) Departamento de Polícia Federal
3) Facebook Serviços Online do Brasil Ltda.
4) Membros do Ministério Público indicados pelo Procurador-Geral da República
5) Comitê Gestor da Internet no Brasil (CGI.br) e Núcleo de Informação e Coordenação do Ponto BR (NIC.br)
6) Professor Anderson Nascimento (University of Washington-Tacoma)
7) Professor Diego de Freitas Aranha (Instituto de Computação da Universidade Estadual de Campinas – UNICAMP)
8) Professor Marcos Antônio Simplício Júnior (Departamento de Engenharia de Computação e Sistemas Digitais da Escola Politécnica da Universidade de São Paulo - USP)
9) Federação Brasileira de Telecomunicações – FEBRATEL
10) Federação das Associações das Empresas de Tecnologia da Informação – ASSESPRO NACIONAL
11) Associação InternetLab de Pesquisa em Direito e Tecnologia
12) Instituto de Tecnologia e Sociedade do Rio – ITS Rio
13) Ministério da Ciência, Tecnologia, Inovações e Comunicações – MCTIC
14) INSPER (Expositor: Renato Muller da Silva Opice Blum)
15) Laboratório de Pesquisa Direito Privado e Internet da Universidade de Brasília – UnB (Expositor: Marcelo Amarante Ferreira Gomes)
16) Associação dos Magistrados Brasileiros – AMB (Expositores: Thiago Rodovalho e Alberto Pavie Ribeiro)
17) Conselho Federal da Ordem dos Advogados do Brasil – CFOAB (Expositor: Alexandre Rodrigues Atheniense)
18) Centro de Tecnologia e Sociedade da Escola de Direito da FGVRio (Expositora: Jamila Rodrigues Venturini)
19) Centro de Pesquisa e Desenvolvimento em Telecomunicações – CPQD (Expositor: Alexandre Melo Braga)
20) Instituto Beta para Democracia na Internet – IBIDEM (Expositor:

Paulo Rena da Silva Santarem)
21) Núcleo Direito, Incerteza e Tecnologia da Faculdade de Direito da USP(Expositor: Juliano Souza de Albuquerque Maranhão)
22) Centro de Competência em Software Livre do Instituto de Matemática e Estatística da USP (Expositor: Nelson Posse Lago)
23) Instituto Brasileiro de Defesa do Consumidor – IDEC (Expositor: Rafael Augusto Ferreira Zanatta)

A forma de seleção, segundo a convocatória, seguiu os seguintes critérios: " (i) representatividade, especialização técnica e expertise do expositor ou da entidade interessada e (ii) garantia da pluralidade da composição da audiência e dos pontos de vista a serem defendidos"[16].

Dessa forma, os convocados abrangeram centros/núcleos/institutos de pesquisa vinculados ou não a Universidades, órgãos públicos como o Ministério de Ciência e Tecnologia e mesmo institutos vinculados a órgãos públicos como a Polícia Federal. Havia também entidades sindicais, professores universitários, comitês multissetoriais como o CGI.br e até o próprio co-fundador do WhatsApp, Brian Acton.

Para participar da audiência, os expositores tinham que responder algumas questões, levantadas pelos ministros-relatores na convocatória[17]:

1 – Em que consiste a criptografia ponta a ponta (end to end) utilizada por aplicativos de troca de mensagens como o WhatsApp?

2 – Seria possível a interceptação de conversas e mensagens realizadas por meio do aplicativo WhatsApp ainda que esteja ativada a criptografia ponta a ponta (end to end)?

[16] Decisão de convocação de audiência pública para discutir o bloqueio do aplicativo *WhatsApp* por decisões judiciais no Brasil (2016). Disponível em: http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/adpf403.pdf
[17] Decisão de convocação de audiência pública para discutir o bloqueio do aplicativo *WhatsApp* por decisões judiciais no Brasil (2016). Disponível em: http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/adpf403.pdf

3 – Seria possível desabilitar a criptografia ponta a ponta (end to end) de um ou mais usuários específicos para que, dessa forma, se possa operar interceptação juridicamente legítima?

4 – Tendo em vista que a utilização do aplicativo WhatsApp não se limita a apenas uma plataforma (aparelhos celulares/smartphones), mas permite acesso e utilização também em outros meios, como, por exemplo, computadores (no caso do WhatsApp mediante o WhatsApp Web/Desktop), ainda que a criptografia ponta a ponta (end to end) esteja habilitada, seria possível "espelhar" as conversas travas no aplicativo para outro celular/smartphone ou computador, permitindo que se implementasse ordem judicial de interceptação em face de um usuário específico?

Note que as quatro perguntas têm em comum um tema: criptografia. O ministro Fachin afirmou que os habilitados a participar da audiência deveriam, como pré-requisito para sua atuação, trazer respostas a essas perguntas, mas que outras questões que considerassem relevantes ao tema poderiam também ser abordadas.

Elas possuem também elevada amplitude, indo desde a natureza e o funcionamento da criptografia ponta a ponta até a viabilidade de interceptação e eventuais hipóteses de como desabilitar ou utilizar essa criptografia em outras plataformas, o que viabilizaria profundo entendimento do tema, necessário para que os ministros julgassem da melhor forma possível.

Apesar disso, o interesse geral na audiência esteve focado nas perguntas 2 e 3, (mais ainda na 2) mesmo que não as respondendo propriamente, de forma que as manifestações sobre as demais questões foram menos frequentes.

Explicar no que consiste a criptografia de ponta a ponta foi, quando muito, usado como introdução para saber se seria possível a interceptação de mensagens com sua manutenção e entender a viabilidade de desabilitá-la apenas para alguns usuários.

Era fundamental que não só os ministros, mas todos os interessados compreendessem o funcionamento da criptografia adotada pelo WhatsApp,

pelo tema ter um caráter majoritariamente técnico e ser de difícil compreensão. Em contrapartida, não foram muitos os expositores que se dispuseram a explicá-la. Estes foram, em ordem de apresentação: Brian Acton[18] - WhatsApp, Anderson Nascimento[19] - Universidade de Washington, Marcos Simplício[20] - Escola Politécnica da USP, Diego Aranha[21] - UNICAMP e Pablo de Camargo[22] - Centro de Tecnologia e Sociedade da Faculdade de Direito da FGV.

Dessa maneira, como o debate estava focado nestas questões, os principais tópicos foram trazidos no bojo da possibilidade ou não de interceptação de conversas e mensagens. Por isso, é importante que o leitor entenda o debate sobre a possibilidade ou não de interceptação de mensagens e, caso haja tal possibilidade, qual é ou quais são elas.

Tal compreensão não só situará o leitor do cenário da audiência pública, mas será fundamental para que compreenda a resposta para a pergunta de pesquisa. Para entender "como" os votos ministros dialogaram com as exposições da audiência, é preciso primeiro entender o que foi dito, quem disse e por que foi dito. Esse detalhamento será feito no tópico seguinte.

2.2. Hipóteses de enfraquecimento da Criptografia

Entraremos aqui no conteúdo da Audiência Pública para explicitar as respostas trazidas pelos expositores para as questões levantadas pelos

[18] Transcrição da Audiência Pública n.21, 2017, pág. 32-33. Disponível em: http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADI5527ADPF403AudinciaPblicaMarcoCivildaInterneteBloqueioJudicialdoWhatsApp.pdf..

[19] Transcrição da Audiência Pública n.21, 2017, pág. 85. Disponível em: http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADI5527ADPF403AudinciaPblicaMarcoCivildaInterneteBloqueioJudicialdoWhatsApp.pdf..

[20] Transcrição da Audiência Pública n.21, 2017, pág. 147. Disponível em: http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADI5527ADPF403AudinciaPblicaMarcoCivildaInterneteBloqueioJudicialdoWhatsApp.pdf..

[21] Transcrição da Audiência Pública n.21, 2017, pág. 225. Disponível em: http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADI5527ADPF403AudinciaPblicaMarcoCivildaInterneteBloqueioJudicialdoWhatsApp.pdf..

[22] Transcrição da Audiência Pública n.21, 2017, pág. 304-305. Disponível em: http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADI5527ADPF403AudinciaPblicaMarcoCivildaInterneteBloqueioJudicialdoWhatsApp.pdf..

Ministros Relatores na convocação da audiência. Isto será feito por meio de três grandes temas: *Hipótese do man-in-the-middle, hipótese dos backdoors* e *desabilitar o uso de chaves privadas para apenas um usuário*.

Conforme explicado no capítulo 1, esta foi a forma mais própria para não só simplificar a compreensão ao leitor, mas abranger os pontos-chave do debate.

Com as ações de bloqueio do WhatsApp, houve, inicialmente, uma disputa de narrativas acerca da possibilidade de interceptação das mensagens para que as ordens judiciais pudessem ser satisfeitas. Enquanto a empresa permanecia firme, argumentando não haver viabilidade técnica, os requerentes alegavam justamente o contrário[23].

Entretanto, o debate na Audiência Pública foi outro. Os expositores em consenso argumentaram haver possibilidade de interceptação das mensagens. Claro que os contrários aos métodos de interceptação apresentaram riscos e falhas, mas não negaram em momento algum a possibilidade.

Assim, o debate restou não sobre a possibilidade de interceptação em si, mas sobre os porquês dessa possibilidade, além da viabilidade do *enfraquecimento* da criptografia de ponta a ponta para fins de investigações criminais. Por isso foi dito no tópico anterior que as perguntas 2 e 3 não foram "propriamente" respondidas. De toda forma, o debate se deu em torno delas.

Como dito pela representante do Ministério Público Federal, Neide Mara Cardoso, "discute-se a possibilidade de viabilizar as investigações com a criptografia, apesar dela"[24].

Felipe Alcântara de Barros, um dos representantes da Polícia Federal, fez importante questionamento na audiência, que elucida o dito no parágrafo

[23] No segundo bloqueio do app, por exemplo, a Polícia Federal entregou parecer técnico, que foi inclusive acolhido pelo Juízo de primeira instância, acerca da possibilidade de interceptação de mensagens apesar da criptografia de ponta-a-ponta.

[24] Transcrição da Audiência Pública n.21, 2017, pág. 119. Disponível em: http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADI5527ADPF403AudinciaPblicaMarcoCivildaInterneteBloqueioJudicialdoWhatsApp.pdf..

anterior: "A pergunta não é 'Os senhores têm viabilidade técnica? '. Não. A pergunta é: 'Por que não as têm? ', 'Por que não procuram tê-las? '."[25]

O dito por Barros também caracteriza o debate da Audiência Pública: os porquês de ter ou não viabilidade técnica. E não havendo, por que não haver? Ele fez esse questionamento por constatar que todo o *iter criminis*, todo o caminho a se percorrer para que um crime ocorra é facilmente percorrido pelos aplicativos de comunicação[26]. Saber se tal constatação foi de alguma forma influente ou se ao menos fora mencionada nos votos dos ministros relatores é importante e reflete a pergunta de pesquisa.

Vladimir Aras, também representante do Ministério Público Federal, trouxe visão parecida à de Barros ao dizer que, por serem instrumentos criados por homens, eles poderiam ser desenhados de forma diferente para que, quando fosse necessário, quando houvesse "absoluta necessidade diante critérios de proporcionalidade adequadas", houvesse a possibilidade desses dados serem compartilhados[27].

Ou seja, houve aproximações com as hipóteses de enfraquecimento da criptografia em virtude das necessidades que alguns expositores trouxeram. Da mesma forma, outros expositores alegaram ser inviável o implemento dessas hipóteses por conta das consequências negativas, como será exposto.

Desta maneira, pretendo, nos tópicos seguintes, trazer os argumentos apresentados na audiência pública n. 21, tanto favoráveis como contrários a cada uma das principais hipóteses de interceptação de mensagens - Hipótese do *man-in-the-middle,* e hipótese dos *backdoors* e desabilitar o uso de chaves privadas para apenas um usuário, conforme definido no capítulo 1.

2.2.1 Hipótese do *man-in-the-middle*

[25] Transcrição da Audiência Pública n.21, 2017, pág. 18. Disponível em: http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADI5527ADPF403AudinciaPblicaMarcoCivildaInterneteBloqueioJudicialdoWhatsApp.pdf

[26] Transcrição da Audiência Pública n.21, 2017, pág. 16. Disponível em: http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADI5527ADPF403AudinciaPblicaMarcoCivildaInterneteBloqueioJudicialdoWhatsApp.pdf

[27] Transcrição da Audiência Pública n.21, 2017, pág. 53. Disponível em:

A primeira hipótese apresentada na audiência foi o ataque *man-in-the-middle*. Ele é nada mais que uma tentativa de interceptar a comunicação. O procedimento seria colocar "um homem no meio" do remetente e o destinatário.

O remetente enviaria sua mensagem e, antes de chegar ao receptor, ela seria acessada por um intermediário. Como dito por Thiago Guimarães, representante da Universidade de Brasília, o intermediário "passará a se personificar como dois interlocutores, de forma que possa optar apenas em acompanhar a comunicação dos usuários, passando-se por eles, replicando as mensagens, de forma a continuar invisível".[28]

2.2.1.1. Argumentos Favoráveis

Uma das maiores preocupações dos expositores favoráveis ao enfraquecimento se dava por conta do processo de investigação e persecução penal. Ao permanecer inviável a investigação nos aplicativos protegidos pela criptografia de ponta a ponta, há "um cenário livre na criminalidade", afirma Felipe Barros, da Polícia Federal[29]. Disso a necessidade de obter acesso a tais mensagens.

Esse foi um argumento trazido não a favor da hipótese *man-in-the-middle* especificamente, mas das hipóteses de enfraquecimento em si. Fernanda Domingos, representante do Ministério Público, em concordância com Barros, trouxe o único argumento expresso a favor da hipótese do *man-in-the-middle.*

A Procuradora afirmou que a perícia do MPF "concluiu que seria possível sim, o chamado ataque *man-in-the-middle,* em que a empresa poderia forçar

http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADI5527ADPF403AudinciaPblicaMarcoCivildaInterneteBloqueioJudicialdoWhatsApp.pdf.

[28] Transcrição da Audiência Pública n.21, 2017, pág. 270. Disponível em: http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADI5527ADPF403AudinciaPblicaMarcoCivildaInterneteBloqueioJudicialdoWhatsApp.pdf.

[29] Transcrição da Audiência Pública n.21, 2017, pág. 17. Disponível em:

uma nova troca de chaves – como, inclusive, foi admitido aqui pelo Senhor Representante do WhatsApp", e isso para a investigação seria muito relevante.

Ela inclusive afirma que interceptar as mensagens se faz necessário independente da notificação do sistema de verificação de segurança[30], que informaria para os usuários de que a chave foi trocada e que eles estão provavelmente sendo monitorados[31].

Ivo de Carvalho, Perito da Polícia Federal, também entende ser possível a interceptação de mensagens, a vendo como uma forma de cooperação entre o aplicativo e os órgãos de investigação. Porém, ele não menciona expressamente a hipótese do *man-in-the-middle,* apenas sugerindo uma "troca de chaves diferentes para conseguir ter acesso a essas mensagens"[32], o que sugere que ele estava falando desta hipótese, por ser a mais plausível.

2.2.1.2 Argumentos Contrários

Como já dito, o WhatsApp adota um sistema de chaves. Portanto, para que o referido ataque pudesse ser viabilizado, seria necessário que o aplicativo modificasse seus servidores para interferir nesse sistema de troca.

Partindo disso, Brian Acton, co-fundador do WhatsApp, afirmou que o servidor teria que fornecer às duas pontas da comunicação chaves falsas e administrá-las para que o processo seja efetivo[33]. O usuário mandaria uma

[30] Conforme afirmam os expositores Brian Acton (pág. 34) e Marcos Simplício (pág. 50), os usuários do WhatsApp podem confirmar que suas mensagens não foram falsificadas, usando um processo chamado Verificação do Código de Segurança. Ele permite que o recebedor confirme que a chave do emissário foi utilizada para criptografar as mensagens, e não a chave não desejada, de uma terceira parte. Isso quer dizer que os usuários podem telefonar ou enviar mensagens e comparar seu código de segurança para confirmar que as suas mensagens foram enviadas um para o outro.

[31] Transcrição da Audiência Pública n.21, 2017, pág. 49. Disponível em: http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADI5527ADPF403AudinciaPblicaMarcoCivildaInterneteBloqueioJudicialdoWhatsApp.pdf.

[32] Transcrição da Audiência Pública n.21, 2017, pág. 26. Disponível em: http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADI5527ADPF403AudinciaPblicaMarcoCivildaInterneteBloqueioJudicialdoWhatsApp.pdf..

[33] Transcrição da Audiência Pública n.21, 2017, pág. 102. Disponível em:

mensagem supondo que ela está criptografada e que só seu destinatário consegue abri-la, quando, "na realidade o WhatsApp consegue abrir, repassar para os órgãos responsáveis e depois recifrar e enviar" ao destinatário, "para que este não perceba que há algo errado na comunicação"[34].

Ele apontou um dos problemas dessa medida, ao dizer que se o WhatsApp modificar os seus servidores para interferir no sistema de troca de chaves, a interceptação seria detectável devido ao sistema de verificação do código de segurança[35] e os usuários saberiam imediatamente que estariam sendo monitorados[36].

Apesar de Fernanda Domingos ter visto esse cenário como um ônus aceitável[37], Simplício e Acton o viram de forma distinta. Isso porque, como dito pelo co-fundador do WhatsApp, os usuários geralmente possuem muitas conversas. Dessa maneira, ele afirma que as chaves que precisariam ser substituídas envolveriam muita gente e teriam que ser forjadas por ambos os lados da conversa. E os usuários seriam notificados disso[38].

"Certamente dá para fazer de uma forma quase imperceptível para o usuário comum, mas não para o usuário suspeito", concorda e acrescenta Demi Getchko, do Comitê Gestor da Internet no Brasil (CGI.br)[39]. Segundo

---

[34] Transcrição da Audiência Pública n.21, 2017, pág. 148. Disponível em: http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADI5527ADPF403AudinciaPblicaMarcoCivildaInterneteBloqueioJudicialdoWhatsApp.pdf.

[35] Os usuários do WhatsApp podem confirmar que suas mensagens não foram falsificadas, usando um processo chamado Verificação do Código de Segurança (ACTON, 2017, pág.34). Ela permite que o recebedor confirme que a chave do emissário foi utilizada para criptografar as mensagens, e não a chave não desejada, de uma terceira parte (ACTON, 2017, 35).

[36] Transcrição da Audiência Pública n.21, 2017, pág. 36. Disponível em: http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADI5527ADPF403AudinciaPblicaMarcoCivildaInterneteBloqueioJudicialdoWhatsApp.pdf.

[37] Há pesquisa doutrinária de certa forma favorável a este pensamento. Tércio Sampaio, que analisa os limites à função fiscalizadora do Estado trouxe em um resumo de seu artigo que: "A privacidade é regida pelo princípio da exclusividade, cujos atributos principais são a solidão (o estar-só), o segredo, a autonomia. Na intimidade protege-se sobretudo o estar-só; na vida privada, o segredo; em relação à imagem e à honra, a autonomia. A privacidade tem, pois, a ver com a inviolabilidade do sigilo, porém, não significa um impedimento absoluto à autoridade fiscal. O acesso aos dados é permitido ainda que seja proibida a interceptação da comunicação. (FERRAZ JÚNIOR, 1993, pág. 1).

[38] Transcrição da Audiência Pública n.21, 2017, pág. 102. Disponível em: http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADI5527ADPF403AudinciaPblicaMarcoCivildaInterneteBloqueioJudicialdoWhatsApp.pdf..

[39] Transcrição da Audiência Pública n.21, 2017, pág. 80. Disponível em: http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADI5527ADPF403AudinciaPblicaMarcoCivildaInterneteBloqueioJudicialdoWhatsApp.pdf...

Getchko, o usuário suspeito vai sempre checar se há alguém "no meio". Além disso, Acton traz que quanto maior o número de conversas, maior a chance de a notificação: "se nós tivermos cinquenta conversas, a chance de uma dessas conversas ligar essa notificação aumenta muito[40]". Em conversas de grupos, a interceptação seria mais facilmente perceptível.

Brian segue em concordância com Getchko, afirmando que nesses casos o aplicativo notificaria o usuário por meio do sistema verificação do modo de segurança[41]. As pessoas usualmente não prestariam atenção nisso, mas é plausível pensar que usuários com atividades suspeitas, como os investigados nas ações que geraram os bloqueios, acusados de tráfico de drogas e pornografia infantil, provavelmente achariam estranha essa mudança de chaves e ficariam atentos a isso, checando com frequência.

Simplício, professor da Poli-USP, diz ainda que o mecanismo de verificação permite que, ao abrir o aplicativo e clicar no nome de um usuário, o indivíduo saiba "qual é o cadeado correspondente a ele[42]. Isso, aliado às notificações do sistema de verificação, poderia fazer com que o usuário saiba que está sendo monitorado, pois, "as mensagens não teriam um código de segurança que combinasse com o código do emissor original"[43].

Claro que tanto há a chance de o usuário notar como há a chance de não notar, mas essa possibilidade em si já é muito preocupante. O co-fundador do WhatsApp aponta uma perigosa consequência deste fato: uma vez que o alvo saiba que está sendo investigado, ele poderia começar a "dar informação falsa para a Polícia, o que colocaria em risco muitos policiais"[44].

---

[40] Transcrição da Audiência Pública n.21, 2017, pág. 102. Disponível em: http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADI5527ADPF403AudinciaPblicaMarcoCivildaInterneteBloqueioJudicialdoWhatsApp.pdf.

[41] Transcrição da Audiência Pública n.21, 2017, pág. 103. Disponível em: http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADI5527ADPF403AudinciaPblicaMarcoCivildaInterneteBloqueioJudicialdoWhatsApp.pdf..

[42] Transcrição da Audiência Pública n.21, 2017, pág. 150. Disponível em: http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADI5527ADPF403AudinciaPblicaMarcoCivildaInterneteBloqueioJudicialdoWhatsApp.pdf...

[43] Transcrição da Audiência Pública n.21, 2017, pág. 36. Disponível em: http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADI5527ADPF403AudinciaPblicaMarcoCivildaInterneteBloqueioJudicialdoWhatsApp.pdf..

[44] Transcrição da Audiência Pública n.21, 2017, pág. 103. Disponível em: http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADI5527ADPF403AudinciaPblicaMarcoCivildaInterneteBloqueioJudicialdoWhatsApp.pdf..

Ainda, faz sentido dizer que é improvável que o indivíduo que sabe que está sendo monitorado continue a cometer atos ilícitos por meio do aplicativo. "Alguém que sabe que está tendo o celular ou um telefone qualquer grampeado, é improvável que continue cometendo o ato. Muito pelo contrário, é mais provável que comece a dar informações falsas sobre o caso[45]", diz Simplício.

Uma reflexão sobre quem efetivamente está sendo investigado: ao interceptar as mensagens do usuário, não só ele será monitorado, mas todos aqueles com quem ele se comunica, o que inclui inúmeras pessoas não suspeitas e não criminosas.

Dessa maneira, com as grandes chances de o usuário suspeito descobrir que está sendo monitorado, além do fato de ele não necessariamente só se comunicar com outros usuários suspeitos, resta como também alvos da investigação inúmeros usuários comuns.

Na verdade, uma vez que o criminoso saiba que está sendo monitorado, os únicos a o serem verdadeiramente serão os usuários comuns, conforme afirma Demi Getchko: "ao se colocar alguém no meio, não se está, na verdade, monitorando os caras do mal, está monitorando os usuários normais"[46]:

Uma interceptação com grandes chances de monitorar apenas usuários comuns, além de inefetiva, viola inúmeros direitos fundamentais, fora que vai contra o próprio caráter original da interceptação, que é de ser **excepcional**, em casos com autorização judicial, acontecendo apenas em situações específicas.

2.2.2. Hipótese dos *backdoors*

[45] Transcrição da Audiência Pública n.21, 2017, pág. 149. Disponível em: http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADI5527ADPF403AudinciaPblicaMarcoCivildaInterneteBloqueioJudicialdoWhatsApp.pdf..

[46] Transcrição da Audiência Pública n.21, 2017, pág. 80. Disponível em: http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADI5527ADPF403AudinciaPblicaMarcoCivildaInterneteBloqueioJudicialdoWhatsApp.pdf..

Os *backdoors*, popularmente chamados de *porta dos fundos,* seriam outra maneira de viabilizar o acesso excepcional. De forma simples, o desenvolvedor colocaria na própria estrutura do software uma funcionalidade que poderia ser acessada por uma espécie de chave-mestra.

Com o sistema de chaves do WhatsApp, seria necessário estabelecer uma espécie de falha na criptografia que viabilizasse o uso dessa chave-mestra, ou a possibilidade de programar uma intervenção que viabilizasse captar a mensagem antes dela ser cifrada ou logo após ser decifrada[47].

2.2.2.1. Argumentos Favoráveis

Como dito no capítulo "*hipóteses de enfraquecimento",* o procurador de Justiça do MPF Vladimir Aras sugeriu que os aplicativos que fazem uso da criptografia de ponta a ponta fossem desenhados de forma diferente para que quando houvesse "absoluta necessidade diante critérios de proporcionalidade adequadas", existisse uma possibilidade de obter os dados[48].

Isso, segundo Aras, se faz necessário porque a alegação feita é que "não há meios de conferir acesso ao Estado a esses dados[49]*".* E essa é sua preocupação. O subprocurador relembra que sempre Estado pode ter acesso a dados por ordem judicial no "mundo físico[50] " e que a busca de dados também é importante para a defesa de direitos.

Barros, em certa conformidade com Aras, afirma que a "persecução penal no Brasil não pode se ditar por empresas de informática; ela tem que

---

[47] Transcrição da Audiência Pública n.21, 2017, pág. 373. Disponível em: http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADI5527ADPF403AudinciaPblicaMarcoCivildaInterneteBloqueioJudicialdoWhatsApp.pdf..

[48] Transcrição da Audiência Pública n.21, 2017, pág. 53. Disponível em: http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADI5527ADPF403AudinciaPblicaMarcoCivildaInterneteBloqueioJudicialdoWhatsApp.pdf..

[49] Transcrição da Audiência Pública n.21, 2017, pág. 53. Disponível em: http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADI5527ADPF403AudinciaPblicaMarcoCivildaInterneteBloqueioJudicialdoWhatsApp.pdf.

[50] Transcrição da Audiência Pública n.21, 2017, pág. 54. Disponível em:

se ditar pelo Estado [51] ". Ou seja, não deveria caber aos aplicativos a possibilidade de negar ao Estado informações requeridas judicialmente.

Assim, a conclusão de Aras foi na direção de que haver essa possibilidade seria um obstáculo. Seria permitir que fosse criado, no Brasil, um "paraíso digital em que criminosos (...) pudessem cometer infrações penais, violando direitos fundamentais tão importantes quanto o direito à privacidade".[52]

Maximiliano Salvadori, do Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC) em sua fala relembrou o dito por Aras de forma analógica à situação dos bancos. Aras ressaltou que eles criam sistemas que viabilizam a quebra do sigilo bancário por determinação legal.

Ele diz isso para afirmar que a Suprema Corte pode incentivar a ciência a criar uma solução, caso queiram efetivamente "manter um sistema de comunicação de dados com criptografia para todos, porém com a possibilidade de intervenção estatal".[53]

Neide Mara, também procuradora do MPF, afirma que eles não são "contra a criptografia", [54]por também se munirem dela. Mara dialoga com o dito por Aras e ainda ressalta que o que o MPF quer é discutir a possibilidade de investigar com a criptografia, para que não haja no país "uma empresa ou qualquer instituição funcionando em que a criminalidade possa ocorrer sem que os órgãos de persecução penal possam combater a criminalidade".[55]

Essa seria, então, a principal vantagem do acesso exclusivo via *backdoors*: viabilizar e facilitar o combate à criminalidade, evitando que haja

[51] Transcrição da Audiência Pública n.21, 2017, pág. 54-55. Disponível em: http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADI5527ADPF403AudinciaPblicaMarcoCivildaInterneteBloqueioJudicialdoWhatsApp.pdf..
[52] Transcrição da Audiência Pública n.21, 2017, pág. 54-55. Disponível em: http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADI5527ADPF403AudinciaPblicaMarcoCivildaInterneteBloqueioJudicialdoWhatsApp.pdf..
[53] Transcrição da Audiência Pública n.21, 2017, pág. 284-285. Disponível em: http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADI5527ADPF403AudinciaPblicaMarcoCivildaInterneteBloqueioJudicialdoWhatsApp.pdf..
[54] Transcrição da Audiência Pública n.21, 2017, pág. 119-120. Disponível em: http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADI5527ADPF403AudinciaPblicaMarcoCivildaInterneteBloqueioJudicialdoWhatsApp.pdf..
[55] Transcrição da Audiência Pública n.21, 2017, pág. 120. Disponível em:

o chamado "paraíso digital". Em conformidade a isso, há uma reflexão de Barros sobre um cenário semelhante que já ocorreu no Brasil. Ele diz que no passado, empresas como Microsoft e Gmail trouxeram os mesmos argumentos que os apresentados pelo WhatsApp e mesmo assim, hoje é possível ter acessos excepcionais pelo MPF e PF[56];

Concordando com Nara, por fim, Fernanda Domingos, também representante do MPF, se baseia em um documento técnico da Perícia do Ministério Público que explica o uso das chaves na criptografia de ponta a ponta para garantir que "em alguns casos, a empresa detém a chave mestra e, quando é possível, ela consegue decifrar imagens e seu conteúdo". Apesar de falar sobre imagens, ela o faz para supor que também haveria a possibilidade para mensagens.

2.2.2.2 Argumentos Contrários

Os *backdoors* ou porta dos fundos nada mais seriam que fornecer um acesso exclusivo e especial para as autoridades de investigação. Para esse acesso existir, o Professor Diego Aranha, da UNICAMP, afirma que seria necessário inserir uma "falha *intencional* de projeto num protocolo criptográfico".

Com isso, o professor expõe um primeiro ponto negativo. A falha não teria qualquer objetivo de segurança. Pelo contrário, ela tornaria a elaboração do software mais complicada, criando vulnerabilidades[57].

Um exemplo de vulnerabilidade criada é a necessidade primordial de se defender o próprio *acesso excepcional.* Fábio Wladimir, Monteiro representante da Assespro, lembra que haverá "chaves, ou uma chave-

http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADI5527ADPF403AudinciaPblicaMarcoCivildaInterneteBloqueioJudicialdoWhatsApp.pdf..

[56] Transcrição da Audiência Pública n.21, 2017, pág. 19. Disponível em: http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADI5527ADPF403AudinciaPblicaMarcoCivildaInterneteBloqueioJudicialdoWhatsApp.pdf..

[57] Transcrição da Audiência Pública n.21, 2017, pág. 135. Disponível em: http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADI5527ADPF403AudinciaPblicaMarcoCivildaInterneteBloqueioJudicialdoWhatsApp.pdf..

mestra de que dê acesso a essa funcionalidade de desativar encriptação ou de espelhar".

Assim, comunicação, que era foco prioritário, restará em segundo plano dos objetivos de segurança porque o uso dessa porta dos fundos resulta na necessidade de protegê-lo e controlá-lo devidamente para que terceiros ilegítimos não consigam essa "chave-mestra". E isso é arriscado.

Brian Acton expõe ainda que qualquer hacker que obtiver esse acesso excepcional, que conseguir acessar essa chave-mestra "poderia ler mensagens por todo o WhatsApp[58]". Isso resultaria em violações de direitos de incontáveis usuários.

Além, Diego Aranha, professor do Instituto de Computação da Unicamp afirma que proteger essa porta dos fundos pode ser muito difícil, para não dizer inviável. Se a funcionalidade for implementada, ela não pode ficar disponível para qualquer um. Assim, será necessária uma forma de guardar o acesso a essa funcionalidade.

Esse acesso "é um alvo extremamente valioso"[59]. E Fábio Wladimir ainda ressalta que a chance de manter esse alvo seguro, de assegurar que apenas aqueles autorizados a usá-lo que o usarão é bem pequena.

Para justificar essa baixa probabilidade, o representante da Assespro traz um exemplo: a famosa praga virtual *WannaCry*[60]*.* Esse caso é muito conhecido por ter envolvido a Agência Nacional de Segurança Americana (NSA), que é o maior empregador de especialistas de segurança do mundo.

Dados na NSA foram vazados por hackers e, com isso, descobriu-se uma falha de segurança no sistema operacional do Windows. A agência já sabia dessas informações e as mantinha em segredo com a intenção de usá-las posteriormente. Essa falha descoberta atingiu proporções globais, de

---

[58] Transcrição da Audiência Pública n.21, 2017, pág. 37. Disponível em: http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADI5527ADPF403AudinciaPblicaMarcoCivildaInterneteBloqueioJudicialdoWhatsApp.pdf..

[59] Transcrição da Audiência Pública n.21, 2017, pág. 181. Disponível em: http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADI5527ADPF403AudinciaPblicaMarcoCivildaInterneteBloqueioJudicialdoWhatsApp.pdf...

[60] Entenda o ciberataque que afetou mais de 200 mil PCs em 150 países. Disponível em: https://olhardigital.com.br/especial/wannacry/

forma que usuários, empresas e instituições do mundo todo foram prejudicados – cerca de 200 mil computadores em 150 países diferentes foram atingidos, causando prejuízos de bilhões, principalmente a governos[61].

Essa situação foi usada para exemplificar o ponto negativo que os *backdoors* carregam: mesmo os sistemas de segurança mais seguros criados pela humanidade foram violados e tiveram informações vazadas.

Monteiro usa o fato de sequer a maior agência de segurança do mundo ter conseguido defender seus bancos de informações e ferramentas de ataques de hackers e criminosos para refletir sobre o risco de haver uma chave-mestra, um acesso excepcional a dados de usuários do mundo todo disponíveis no WhatsApp.

Ainda, em expressa conformidade com Anderson Nascimento, professor da Universidade de Washington, Monteiro afirma que é "consenso[62] para a comunidade científica (...) que esses mecanismos certamente reduzem o nível de segurança[63]". Anderson Nascimento menciona artigo "*Keys under the doormat"*[64]*,* texto escrito pelos maiores especialistas de criptografia e segurança de informação e entregue ao presidente dos EUA, para corroborar que há consenso.

Uma outra questão foi trazida pelo professor da UNICAMP Diego Aranha. Ele ressalta que caso o *backdoor* fosse implementado, a empresa, no caso, o WhatsApp precisaria "proteger o acesso a essa porta dos fundos contra os seus próprios funcionários, que (...) podem vir a ser coagidos ou

---

[61] Transcrição da Audiência Pública n.21, 2017, pág. 182. Disponível em: http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADI5527ADPF403AudinciaPblicaMarcoCivildaInterneteBloqueioJudicialdoWhatsApp.pdf...

[62] A Transcrição da Audiência Pública n.21, 2017, pág. 91 e pág. 183. Disponível em: http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADI5527ADPF403AudinciaPblicaMarcoCivildaInterneteBloqueioJudicialdoWhatsApp.pdf.

[63] O debate é internacional. Nos Estados Unidos, a pesquisadora especialista em criptografia, ligada ao Center for Internet and Society da Universidade de Stanford, Riana Pfefferkorn, em relatório publicado em 2018[63], explicitou que eventuais medidas de regulação que impusessem às empresas de tecnologia o dever de garantir acesso excepcional aos dados criptografados, para a ulterior necessidade de investigação pelas autoridades, não seria algo positivo para o governo americano (PFEFFERKORN, 2018).

[64] ABELSON, Harold; ANDERSON, Ross. et al. Keys under doormats: mandating insecurity by requiring government access to all data and communications.: mandating insecurity by requiring government access to all data and communications**. Journal Of Cybersecurity**, [s.l.], p. 1-11, 17 nov. 2015. Oxford University Press (OUP). http://dx.doi.org/10.1093/cybsec/tyv009.

atacados por terceiras partes e serem forçados a utilizar essa porta dos fundos para fins"[65]. Ou seja, eles não poderiam se restringir a se defender apenas de hackers.

Além disso, como dito por Pablo de Camargo, do Centro de Tecnologia e Sociedade da FGV, obrigar o WhatsApp a implementar um *backdoor* e entregar seus dados de comunicação o colocaria em "situação de disparidade de concorrência com os outros aplicativos [66] ", o que representa uma repercussão econômica negativa.

Os usuários criminosos simplesmente migrariam para a alternativa mais segura e, com eles, inúmeros usuários comuns [67] , como dito por Monteiro, representante da Assespro. Nelson Lago (IME-USP) chega a afirmar que a facilidade com que o usuário pode migrar para outro aplicativo é "ridícula". E isso não seria apenas no Brasil, pois, como bem sabemos, o WhatsApp é um aplicativo internacional que conecta usuários de todo o mundo.

Uma reação assim poderia influenciar a decisão a ser mais extensiva, aplicando-se a todos os aplicativos porque não faria sentido obrigar apenas o WhatsApp a ter algum tipo de porta dos fundos, já que isso só resultaria na migração para os outros aplicativos.

Por fim, traz-se o Professor Diego Freitas da Unicamp, que cita vários exemplos de agentes que dependem da criptografia de ponta a ponta e que seriam afetados pelo seu enfraquecimento: "ativistas que lutam contra governos autoritários; (...) fontes de jornalismo investigativo; comunicação entre clientes e seus próprios advogados; (...) delatores de ação maliciosa dentro de empresas[68]".

---

[65] Transcrição da Audiência Pública n.21, 2017, pág. 136. Disponível em: http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADI5527ADPF403AudinciaPblicaMarcoCivildaInterneteBloqueioJudicialdoWhatsApp.pdf...

[66] Transcrição da Audiência Pública n.21, 2017, pág. 308. Disponível em: http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADI5527ADPF403AudinciaPblicaMarcoCivildaInterneteBloqueioJudicialdoWhatsApp.pdf..

[67] Transcrição da Audiência Pública n.21, 2017, pág. 183. Disponível em: http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADI5527ADPF403AudinciaPblicaMarcoCivildaInterneteBloqueioJudicialdoWhatsApp.pdf..

Inclusive, afirmou que os investigadores de crimes que precisam de comunicação confidencial para se comunicar entre si restariam prejudicados, o que afastaria a segurança da criptografia forte dos âmbitos onde ela é mais necessária[69].

O volume de argumentos contrários ao implemento dos *backdoors* foi grande. Alguns autores, inclusive, mostraram que a hipótese se assemelha a proibir a criptografia"[70]. Proibir porque, como dito pelo Professor Aranha, ao impedir a criação de um software sem os *backdoors*, limita-se a liberdade de criação do próprio programador[71].

Marcos Antônio Simplício, da Escola Politécnica da USP, também o vê como restrição dessa liberdade, dizendo que "seria como impedir, em um certo momento, numa área da matemática, as pessoas de fazerem multiplicações".

O sentido está no fato de as técnicas criptográficas serem nada mais que matemática na forma de software. Dessa forma, banir o uso de encriptação forte - seja impedindo que ela seja usada ou obrigando que possua *backdoors* - seria o mesmo que criminalizar parte da matemática

Simplício também diz que vários precedentes judiciais confirmam que a liberdade de programar é equivalente à liberdade de expressão [72] , de transformar um ato em código funcional, o que fundamenta mais a tese.

---

[68] Transcrição da Audiência Pública n.21, 2017, pág. 138. Disponível em: http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADI5527ADPF403AudinciaPblicaMarcoCivildaInterneteBloqueioJudicialdoWhatsApp.pdf..

[69] Transcrição da Audiência Pública n.21, 2017, pág. 140. Disponível em: http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADI5527ADPF403AudinciaPblicaMarcoCivildaInterneteBloqueioJudicialdoWhatsApp.pdf..

[70] Transcrição da Audiência Pública n.21, 2017, pág. 152. Disponível em: http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADI5527ADPF403AudinciaPblicaMarcoCivildaInterneteBloqueioJudicialdoWhatsApp.pdf..

[71] Transcrição da Audiência Pública n.21, 2017, pág. 135. Disponível em: http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADI5527ADPF403AudinciaPblicaMarcoCivildaInterneteBloqueioJudicialdoWhatsApp.pdf..

[72] Transcrição da Audiência Pública n.21, 2017, pág. 134. Disponível em: http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADI5527ADPF403AudinciaPblicaMarcoCivildaInterneteBloqueioJudicialdoWhatsApp.pdf..

Todos esses pontos são relevantes para pensar a constitucionalidade tanto dos bloqueios como da criptografia. Como dito pouco acima, o WhatsApp é um aplicativo internacional, que conecta pessoas do mundo todo.

As consequências positivas e negativas da decisão da Suprema Corte seriam sentidas pelos usuários do aplicativo ao longo do globo. Mesmo que os ministros relatores não correspondam ao entendimento do STF, eles devem ter em mente esses ônus e bônus levantados na audiência.

2.2.3. Desabilitar o uso de chaves privadas para apenas um usuário:

Uma das perguntas realizadas pelos ministros na convocatória para a audiência pública foi a seguinte:

> 2 – Seria possível a interceptação de conversas e mensagens realizadas por meio do aplicativo WhatsApp ainda que esteja ativada a criptografia ponta a ponta (end to end)?[73]

A ideia desse procedimento seria interceptar e ler as mensagens apenas desses usuários, sem se munir de outras formas de interceptação.

Como explicado na Introdução, o WhatsApp adota um sistema de chaves para cada mensagem enviada. Com esse sistema, tanto o emissor como o receptor possuem um par de chaves, responsáveis por cifrar e decifrar as mensagens. Brian Acton afirma que "o WhatsApp foi construído de forma que só pode enviar mensagens cifradas"[74].

[73] Decisão de convocação de audiência pública para discutir o bloqueio do aplicativo *WhatsApp* por decisões judiciais no Brasil (pág. 9), disponível em: http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/adpf403.pdf

[74] Transcrição da Audiência Pública n.21, 2017, pág. 35. Disponível em: http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADI5527ADPF403AudinciaPblicaMarcoCivildaInterneteBloqueioJudicialdoWhatsApp.pdf..

Acton diz que, dessa maneira, "todas as mensagens mandadas por todos os usuários são criptografadas". O sistema não consegue enviar ou receber mensagens não submetidas à criptografia"[75]. Com isso ele afirma não haver jeito de desativar a criptografia para um usuário específico durante a entrega da mensagem.

Isso é melhor explicado por Fábio Wadimir, que disse não ser possível desabilitar a criptografia sem alterar o design do sistema. Ou seja, só seria possível desabilitá-la se a mudança fosse para todos os usuários.

Acton diz ainda que mesmo que houvesse um jeito de não criptografar as mensagens, uma vez que o aplicativo obrigatoriamente só envia mensagens submetidas a criptografia, "essa mudança efetivamente evitaria que o usuário enviasse ou recebesse qualquer mensagem pelo WhatsApp. Essencialmente, o WhatsApp seria inutilizado para aquele usuário[76]".

Além disso, como o aplicativo tenta, caso as chaves sejam desabilitadas, automaticamente regenerá-las, de forma que o usuário possa voltar a enviar mensagens com segurança, tanto Acton e como Diego Aranha concluem que a única forma de desativar a criptografia para um usuário seria desativar para todos os demais.

2.3. Conclusões preliminares

Uma das propostas metodológicas apresentadas foi separar os argumentos das hipóteses *man-in-the-middle* e *backdoors* em favoráveis e contrários. Isso serviria para melhor organização e talvez facilitar, visualmente, tendências da audiência e quantidade de argumentos. Nesse sentido, os argumentos favoráveis às hipóteses foram em número e em profundidade nitidamente menores que os contrários.

---

[75] Transcrição da Audiência Pública n.21, 2017, pág. 36. Disponível em: http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADI5527ADPF403AudinciaPblicaMarcoCivildaInterneteBloqueioJudicialdoWhatsApp.pdf..

[76] Transcrição da Audiência Pública n.21, 2017, pág. 36. Disponível em: http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADI5527ADPF403AudinciaPblicaMarcoCivildaInterneteBloqueioJudicialdoWhatsApp.pdf..

Dentre as 23 entidades de especialistas[77] e representantes convocados para participar dos debates, eis os que se manifestaram favoravelmente ao enfraquecimento da criptografia: Departamento de Polícia Federal; Membros do Ministério Público Federal; Ministério da Ciência, Tecnologia, Inovações e Comunicações – MCTIC e a Federação de Empresas de Telecomunicação (FEBRATEL)[78].

Muitos dos expositores trouxeram pontos pouco relevantes ao debate objeto da presente monografia, de forma que não foram citados. Apesar disso, o número de expositores favoráveis em relação ao total de entidades aprovadas é baixo – foram 4 dentre as 23 entidades convocadas. Um fato interessante é que estes foram expositores, principalmente, do MPF e da PF, órgãos fundamentais na persecução penal.

Apesar de lidarem com essas questões, outro ponto interessante é que esses grupos não se caracterizam por serem especialistas em criptografia ou em segurança digital. São representantes do Poder Público – mesmo que em âmbitos distintos - com interesses diversos nessa questão.

Esses representantes tenderam a se voltar mais para a necessidade responsabilização penal dos acusados - que foi o que gerou os bloqueios e o debate - que pelas consequências de um eventual enfraquecimento da criptografia. As consequências negativas foram abordadas por eles como ônus necessários para que a persecução penal pudesse acontecer.

As repercussões econômicas, consequências para a segurança e privacidade dos usuários foram preteridas, sendo priorizadas questões como impunidade, necessidade de submissão ao poder público, etc.

Por outro lado, não só o volume de argumentos contrários às hipóteses do *man-in-te-middle* e dos *backdoors,* mas também o número de expositores foi mais amplo. Estes, em sua maioria representantes de Universidades,

[77] Definidos participantes e cronograma da audiência pública sobre WhatsApp e Marco Civil da Internet (2017). Disponível em: http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=341437

[78] O representante da FEBRTEL, Eduardo Levy Cardoso, apenas se disse favorável ao enfraquecimento, mas não trouxe argumentos sobre a criptografia em si. Ele se restringiu a explicar o funcionamento da federação, dizer que eles são incapazes de interceptar mensagens, mas, havendo possibilidade, o WhatsApp deveria fazê-lo.

Centros de Pesquisa, podem ser identificados como de perfil mais técnico-científico. Os grupos favoráveis procuraram focar nos ônus de um eventual enfraquecimento da criptografia, afirmando em geral que as consequências são mais prejudiciais que positivas.

Apesar de suas diferenças, tanto os grupos favoráveis como os contrários, como dito no tópico *"hipóteses de enfraquecimento"* argumentaram haver possibilidade de interceptação das mensagens. Isso foi consenso. Isto já diverge do afirmado pelo WhatsApp nas ações de bloqueio.

Pode-se, então, resumir os principais pontos positivos e negativos do enfraquecimento da criptografia em:

A) Positivos

i) a persecução penal não seria ditada por empresas privadas, mas pelo Estado; ii) não teríamos um cenário livre na criminalidade – paraíso digital; iii) a investigação pela Polícia Federal seria mais efetiva; iv) manutenção dos sistemas de segurança, mas com possibilidade de intervenção estatal

B) Negativos

i) interceptação por *man-in-the-middle* seria detectável; ii) risco de a polícia receber informações falsas enviadas propositalmente pelos criminosos que sabem que estão sendo monitorados; iii) vigilância de pessoas não suspeitas e inocentes; iv) redução da segurança; v) WhatsApp colocado em disparidade econômica; vi) repercussão internacional

Cabe, agora, averiguar como o consenso, as semelhanças, diferenças, pontos positivos e negativos se refletiram nos votos dos Ministros Relatores. Da audiência, é possível depreender que em questão de volume de expositores e volume numérico, ao menos, os argumentos favoráveis às hipóteses de enfraquecimento restaram vencidos.

3. Dos Votos dos Relatores

Três anos após a Audiência Pública n. 21, no dia 27 de maio (quarta-feira) às 14h, o Plenário do Supremo Tribunal Federal (STF) iniciou o julgamento da ADPF 403 e da ADI 5527, por meio de videoconferência transmitida pela Rádio Justiça e pelo canal do STF no YouTube[79].

Neste dia, a ministra Rosa Weber partilhou seu tempo com exposições dos amici curiae, sendo a única a votar. No dia seguinte, (28) Edson Fachin, relator da ADPF, proferiu seu voto. Em seguida, o exame pelo Plenário do STF das ações foi suspenso pelo pedido de vista do Ministro Alexandre de Mo- raes.[80]

Apenas dois votos não representam o entendimento do STF, servindo apenas para elucidar uma tendência que não necessariamente se manterá. Apesar disso, eles não perdem sua relevância, pois não deixam de ser votos de ministros da Suprema Corte Brasileira.

Portanto, analisarei os votos nos dois tópicos seguintes, buscando semelhanças com as exposições da audiência, peculiaridades e semelhanças entre si, para averiguar se, e como eles dialogaram com as contribuições dos expositores da audiência pública n.21 no que diz respeito à regulação judicial da criptografia, que é o objetivo da presente monografia.

3.1. Rosa Weber

Como visto no capítulo 2, o entendimento majoritário dos expositores foi contrário à implementação de hipóteses de interceptação de mensagens no WhatsApp. A argumentação dos expositores foi em sua maioria no sentido de que essas hipóteses não só resultariam no enfraquecimento da

[79] Pleno – Bloqueio de serviços de mensagens – COM AUDIODESCRIÇÃO, (2020). Disponível em: https://www.youtube.com/watch?v=E0XVN_4ve4U e Relatora entende que aplicativos de mensagens não podem ser obrigados a fornecer dados criptografados, (2020). Disponível em: http://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=444265&ori=1

[80] Pleno – Sigilo de comunicação em aplicativos de mensagens (2020). Disponível em: htps://www.youtube.com/watch?v=0UVpr-cYt-Q e Relatores consideram inconstitucional quebra do sigilo de comunicação em aplicativos de mensagens, (2020). Disponível em: http://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=444384&ori=1)

criptografia, mas também da segurança dos usuários como um todo, o que poderia resultar em inúmeras violações de direitos.

Apesar disso, importantes pontos sobre a necessidade de se obter o acesso excepcional foram trazidos. Tendo em vista o âmbito procedimental penal, os expositores que defenderam as hipóteses de enfraquecimento o fizeram por entender que a investigação criminal restaria muito prejudicada, caso o acesso excepcional não fosse assegurado.

Entretanto, como constatado no tópico "conclusões parciais", foi unânime o entendimento na audiência de que haveria possibilidade material das interceptações, sendo sopesado apenas suas consequências.

A ministra Rosa Weber, em seu voto, coloca essa possibilidade material do cumprimento da ordem como uma das duas circunstâncias que mais importam no que tange as ordens de bloqueio.

Antes disso, a Ministra fez considerações iniciais, ressaltando o caráter fundamental da audiência pública (aqui, sem entrar no mérito do exposto), avaliando a legitimidade ativa do Partido Republicano e expondo os artigos que abrangem o mérito da ação. Após, teceu breve comentário sobre a "virtualização da vida privada em nossos dias" e sobre o histórico dos bloqueios de aplicações no Brasil. Neste último, a ministra trouxe exemplos de suspensões e bloqueios que ocorreram ao longo do mundo, aproximando o contexto brasileiro do internacional.

Depois disso, a ministra entrou no mérito das ordens de bloqueio do WhatsApp em si, no item 7 de seu voto "Das ordens de bloqueio do WhatsApp". Ela relata que elas partiram da premissa de que houve descumprimento da ordem judicial. Com isso, ela definiu duas circunstâncias que, segundo ela mesma, mais importam ao assunto: Uma de caráter legal " (i) a legalidade e a Constitucionalidade da ordem de disponibilização do conteúdo das Mensagens" e a já mencionada" e outra, a "(ii) possibilidade material do cumprimento da ordem", que é de caráter mais técnico.

A partir disso, a ministra focou a maior parte de sua argumentação em questões de direitos fundamentais, com destaque para a liberdade de

expressão – embora tenha separado um tópico exclusivo para esse tema, a liberdade de expressão figurou ao longo de todo o voto.

Para situar melhor o leitor, após as considerações iniciais, que se findaram no tópico "Ordens de Bloqueio", a ministra dividiu sua argumentação da seguinte forma e ordem:

> - Considerações sobre o direito às liberdades de expressão e de comunicação (art. 5º, IX, da CF
>
> - Considerações sobre o direito à privacidade (art. 5º, X, da Constituição da República)
>
> - Considerações sobre o sigilo das comunicações privadas (art. 5º, XII, da Constituição da República)
>
> - Do dever de guarda de metadados
>
> - Da Lei Geral de Telecomunicações (Lei nº 9.472/1997
>
> - Influxos do standard normativo da Convenção de Budapeste sobre o Cibercrime
>
> - Análise da constitucionalidade dos preceitos impugnados
>
> **- A questão da criptografia**
>
> - Das sanções previstas no art. 12, III e IV, da Lei nº 12.965/2014
>
> - Conclusão
>
> (Grifo Nosso)

Note que apesar de ter sido convocada toda uma audiência pública sobre criptografia, a ministra separou apenas um capítulo para tratar explicitamente do tema. A ministra relatora iniciou as seis páginas de argumentação do capítulo ressaltando a importância da criptografia para tornar a sociedade mais segura, informando que a tecnologia protege elementos essenciais do dia a dia, como as comunicações, transações online, que são realidade natural na modernidade. Este foi o primeiro diálogo com

exposições da audiência, mas ele não ocorreu de forma totalmente explícita. Explico:

O Professor Bruno Magrani, representante do Facebook, disse que a criptografia faz parte do dia a dia. Ele afirma que, por exemplo, quando um indivíduo acessa um e-mail, realiza compras online, usa um aplicativo de celular para acessar sua conta bancária, quando faz saques em caixas eletrônicos, ele está agindo sob a presença da criptografia. Disso, conclui que "sem criptografia para garantir a segurança dessas atividades online, haveria muito mais incidentes de segurança, e ninguém se sentiria efetivamente seguro para desenvolver tais atividades na internet".[81]

É importante ressaltar que ministra não cita essas situações em específico, mas traz, de forma generalista, o dito por Magrani: "o desenvolvimento e disseminação de tecnologias criptográficas na contemporaneidade é o que torna as comunicações e as transações online mais seguras e, em consequência, a sociedade também fica mais segura[82]". Na Audiência, o Professor Diego Aranha também trouxe a importância da criptografia no dia a dia de forma generalista, ao dizer que "a criptografia está em todo lugar"[83].

Posteriormente, ela trouxe a importância da criptografia de chave pública – que, como visto na introdução desta monografia, se relaciona diretamente com a espécie de criptografia adotada o WhatsApp. Mais que estar presente na introdução, é importante dizer que muitos expositores explicaram o funcionamento desta espécie de criptografia na audiência, o que provavelmente foi feito para que os Ministros também pudessem entender.

A seguir, ministra continuou com argumentos de caráter mais introdutório, até dar a entender de forma mais explícita que concorda com a

[81] Transcrição da Audiência Pública n.21, 2017, pág. 60. Disponível em: http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADI5527ADPF403AudinciaPblicaMarcoCivildaInterneteBloqueioJudicialdoWhatsApp.pdf..

[82] SUPREMO TRIBUNAL FEDERAL. Tribunal Pleno. ADI 5527-DF, Rel. Min. Rosa Weber, j. 27/05/2020, p. 28.
Disponível em: http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI5527voto.pdf

[83] Transcrição da Audiência Pública n.21, 2017, pág. 129. Disponível em: http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADI5527ADPF403AudinciaPblicaMarcoCivildaInterneteBloqueioJudicialdoWhatsApp.pdf..

compreensão do lado majoritário dos expositores da audiência. Ela afirmou ser ”inadmissível contrassenso, e mesmo retrocesso, tornar ilegal ou limitar dessa maneira o uso de criptografia[84]”.

Note que ela não se restringe às hipóteses de interceptação mencionadas na audiência. Ao usar as expressões “limitar” e “tornar ilegal”, é possível depreender que quaisquer hipóteses que enfraqueçam a criptografia – sejam os *backdoors,* o *man-in-the-middle,* desabilitar chaves, proibir a criptografia ou outras – configurariam esse retrocesso. A ministra também não fez restrição à criptografia de ponta a ponta, espécie adotada pelo WhatsApp, o que mostra o quão abrangente essa afirmação foi.

A seguir, ela parece dialogar com o professor Diego Freitas da Unicamp ao afirmar que a criptografia tem “garantido a segurança da comunicação de grupos de direitos humanos e indivíduos que se mobilizam contra regimes opressivos ao redor do mundo”.

Ela o faz para depois afirmar que a difusão da criptografia é uma das formas de assegurar segurança à comunicação de grupos de direitos humanos e indivíduos que enfrentam regimes opressivos, também atuando para assegurar ao indivíduo o direito à privacidade[85].

Freitas, em suas falas, traz exemplos de agentes que seriam diretamente afetados com a imposição de restrições à criptografia[86] - ativistas que lutam em outros países contra os seus governos autoritários, por exemplo.

Isso mostra certa proximidade entre o voto da ministra e a linha argumentativa majoritária da audiência, que via o enfraquecimento da criptografia como uma potencial forma de violações de direitos.

---

[84] SUPREMO TRIBUNAL FEDERAL. Tribunal Pleno. ADI 5527-DF, Rel. Min. Rosa Weber, j. 27/05/2020, p. 28. Disponível em: http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI5527voto.pdf

[85] SUPREMO TRIBUNAL FEDERAL. Tribunal Pleno. ADI 5527-DF, Rel. Min. Rosa Weber, j. 27/05/2020, p. 28. Disponível em: http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI5527voto.pdf

[86] Transcrição da Audiência Pública n.21, 2017, pág. 136. Disponível em:

Os debates sobre meios e a viabilidade de se enfraquecer a criptografia no STF se iniciaram oficialmente com a convocatória para audiência e com suas as perguntas-base. A min. Rosa Weber, em dado momento, reduziu os questionamentos principais - sobre a possibilidade de interceptação de mensagens e a possibilidade de desabilitar a criptografia – a um único, se

questionando *se caberia ao Estado* obrigar os desenvolvedores de software, fabricantes de dispositivos e outros a enfraquecer a encriptação[87].

E é um questionamento plausível saber se é competência de uma corte definir quais dessas consequências e limitações técnicas de viabilizar ou não as interceptações são as "melhores".

A Ministra não se responde imediatamente, mas faz menção à hipótese de *backdoors* [88] , informando o também dito por Anderson Nascimento e Wladimir Monteiro: tal hipótese vem sendo abandonada por ter como uma de suas principais consequências a redução da segurança, um consenso na comunidade científica[89].

Isso bate de frente com direitos fundamentais como a proteção da liberdade de expressão e sigilo das informações, explicita a min. Rosa Weber[90], o que parece conferir legitimidade à Suprema Corte Brasileira, na qualidade de defensora de direitos fundamentais.

A ministra ainda diz o mesmo que foi dito pelo representante da Federação das Associações de Empresas de tecnologia da Informação, Fábio Wladimir Monteiro: uma das consequências imediatas do enfraquecimento da criptografia de um aplicativo em específico seria que os usuários que faziam

http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADI5527ADPF403AudinciaPblicaMarcoCivildaInterneteBloqueioJudicialdoWhatsApp.pdf..

[87] SUPREMO TRIBUNAL FEDERAL. Tribunal Pleno. ADI 5527-DF, Rel. Min. Rosa Weber, j. 27/05/2020, p. 28.
Disponível em: http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI5527voto.pdf

[88] SUPREMO TRIBUNAL FEDERAL. Tribunal Pleno. ADI 5527-DF, Rel. Min. Rosa Weber, j. 27/05/2020, p. 28.
Disponível em: http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI5527voto.pdf

[89] Transcrição da Audiência Pública n.21, 2017, pág. 91 e 183. Disponível em: http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADI5527ADPF403AudinciaPblicaMarcoCivildaInterneteBloqueioJudicialdoWhatsApp.pdf..

[90] SUPREMO TRIBUNAL FEDERAL. Tribunal Pleno. ADI 5527-DF, Rel. Min. Rosa Weber, j. 27/05/2020, p. 28.

uso dele para cometer crimes simplesmente migrariam para aplicativos fora do alcance das autoridades[91].

A relatora, então, responde parcialmente sua pergunta - se caberia ao Estado obrigar os desenvolvedores de aplicações a criarem softwares menos seguros - afirmando que o "Estado não pode ambicionar que a migração parauma plataforma diversa da anteriormente regulada signifique uma oportunidade para afrouxamento de garantias e liberdades[92]".

Ela não responde direta e expressamente a questão. Mas afirma que uma vez que o poder público obrigue os desenvolvedores de software, fabricantes de dispositivos e outros a enfraquecer a encriptação por eles adotada, tendo em mente que isso só fará com que os usuários migrem para a plataforma diversa da regulada, ele estará viabilizando a redução de garantias. Isso, por sua vez, não me parece estar em conformidade com o caráter de defensor de direitos fundamentais e da Constituição que a Suprema Corte possui.

Então, ela se afasta um pouco do caráter técnico da maioria das exposições da audiência, partindo para um lado mais jurídico, – mesmo que não tão jurídico quanto as demais partes de seu voto - fazendo, assim, outro questionamento: "qual é o sentido de uma Constituição que, no ano de 2020, protege o sigilo das comunicações telegráficas, mas não protege o sigilo das comunicações realizadas por aplicações de internet ou qualquer outro meio pelo qual as pessoas de fato se comunicam hoje[93]"?

Ela o responde imediatamente, dizendo que a Constituição não pode ser lida como um "museu de direitos". Ou seja, a Constituição não pode estar em desconformidade com os avanços tecnológicos. Com isso, ela reafirma

---

91 Transcrição da Audiência Pública n.21, 2017, pág. 183. Disponível em: http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADI5527ADPF403AudinciaPblicaMarcoCivildaInterneteBloqueioJudicialdoWhatsApp.pdf..

92 SUPREMO TRIBUNAL FEDERAL. Tribunal Pleno. ADI 5527-DF, Rel. Min. Rosa Weber, j. 27/05/2020, p. 28.
Disponível em: http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI5527voto.pdf

93 SUPREMO TRIBUNAL FEDERAL. Tribunal Pleno. ADI 5527-DF, Rel. Min. Rosa Weber, j. 27/05/2020, p. 29.
Disponível em: http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI5527voto.pdf

que ” A criptografia, como recurso tecnológico, tem-se revestido de especial relevo na implementação de direitos humanos”.

Isso também foi dito na audiência por Bruno Magrani, do Facebook, que trouxe trecho de um relatório do Conselho de Direitos Humanos das Nações Unidas, que diz que “ a criptografia viabiliza que indivíduos exerçam seus direitos de liberdade de opinião e expressão na área digital e, portanto, merece forte proteção”.

A ministra não menciona esse relatório em seu voto, mas traz outros exemplos de legislações que estão intimamente ligadas a direitos assegurados pela a proteção de dados e a proteção da privacidade, ou seja, pela criptografia. Dois exemplos são os artigos 17 e 19 do Pacto Internacional sobre Direitos Civis e Políticos, no âmbito das Nações Unidas[94]:

> art. 17 “(...) ninguém poderá ser objetivo de ingerências arbitrárias ou ilegais em sua vida privada, em sua família, em seu domicílio ou em sua correspondência”
>
> art. 19 – “Toda pessoa terá direito à liberdade de expressão; esse direito incluirá a liberdade de procurar, receber e difundir informações e ideias de qualquer natureza, independentemente de considerações de fronteiras, verbalmente ou por escrito, em forma impressa ou artística, ou por qualquer outro meio de sua escolha[95]”.

A min. Rosa Weber, ao longo de seu voto, muito tratou sobre liberdade de expressão e não foi diferente ao abordar a questão da criptografia. Ao trazer os artigos 17 e 19 do referido pacto, ela relaciona a proteção contra intromissõesarbitrarias (viabilizada pela criptografia) com a liberdade de expressão.

Ela ainda menciona estudo da UNESCO que concluiu que os pilares de uma internet segura são “acesso a informação e conhecimento, liberdade de

[94] SUPREMO TRIBUNAL FEDERAL. Tribunal Pleno. ADI 5527-DF, Rel. Min. Rosa Weber, j. 27/05/2020, p. 30.
Disponível em: http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI5527voto.pdf

[95] BRASIL. Decreto Legislativo n° 226, de 12 de dezembro de 1991; Pacto Internacional sobre Direitos Civis e Políticos. Brasília. 1992.
Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/1990-1994/d0592.htm

expressão, privacidade e ética". Disso, a ministra conclui que a proteção de dados e da privacidade são "fatores críticos para a preservação não só da liberdade de expressão como da própria segurança dos usuários das redes de informação e comunicação".[96]

Com isso ela parece querer evidenciar em seu voto o caráter fundamental da proteção de dados e da privacidade para a preservação da liberdade de expressão, o que está em consonância com o entendimento majoritário da audiência - as consequências da manutenção da criptografia à forma atual são muito mais benéficas do que as de imposição de hipóteses de enfraquecimento.

Ainda no debate sobre preservação desses direitos, a ministra afirma que toda pessoa tem o direito de se expressar livremente e com segurança. A ministra diz mais de uma vez ao longo de seu voto que a liberdade de expressãodeve ser assegurada, mas que isso não pode ser restrito a alguns âmbitos.

Com isso, ela conclui o já dito pela UNESCO (Organização das Nações Unidas para a Educação, a Ciência e a Cultura) em 2015, pelos expositores na Audiência Pública e por muitos outros especialistas: práticas que reduzam a segurança da criptografia, como as hipóteses do *man-in-the-middle,* ou do *backdoor* podem deixar os usuários da Internet vulneráveis a outras ameaças ilegítimas e, dentre essas ameaças, resta ameaçada a liberdade de expressão.

Ela cita novo texto da UNESCO que diz que mesmo que haja motivos razoáveis para a vigilância estatal por meio dessas alternativas, as preocupações com as consequências potencialmente prejudiciais a direitos e liberdades democráticas pesam na balança[97].

A ministra deixa isso claro ao dizer que o cerne da questão não repousa, como dito pelas entidades favoráveis ao enfraquecimento da criptografia na audiência, sobre a segurança pública. Isso porque – e aqui ela dialoga

[96] SUPREMO TRIBUNAL FEDERAL. Tribunal Pleno. ADI 5527-DF, Rel. Min. Rosa Weber, j. 27/05/2020, p. 31.
Disponível em: http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI5527voto.pdf
[97] SUPREMO TRIBUNAL FEDERAL. Tribunal Pleno. ADI 5527-DF, Rel. Min. Rosa Weber, j. 27/05/2020, p. 31.
Disponível em: http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI5527voto.pdf

novamente com o representante da Assespro, Fábio Monteiro - a mesma tecnologia que permitiria às autoridades facilidades para a investigação traz consigo o risco de ser usadas por criminosos – não suspeitos, mas criminosos – para que estes obtivessem informações privadas de futuras vítimas[98].

Ou seja, aqui, ela não só concorda novamente com um expositor contrário ao enfraquecimento da criptografia, mas discorda de um dos pontos das entidades favoráveis ao feito.

A min. Rosa Weber coloca que mesmo que as investigações tenham certo caráter deurgência, de imediatismo, isso não justifica os danos futuros que poderiam decorrer do enfraquecimento, como maiores riscos de ciberataques, fraudes, roubos de identidade, invasão da intimidade extorsão etc[99].

Todos os argumentos contrários ao implemento das hipóteses de enfraquecimento da criptografia, em alguma medida, viam os ônus como grandes demais para as vantagens que esse implemento conferiria. A relatora viu a situação da mesma forma.

A Ministra também informa, por meio de estudo da UNESCO, o papel desempenhado pela criptografia na criação de condições materiais para o exercício dos direitos relacionados à proteção da privacidade e da liberdade de expressão. Ela mais uma vez bate na tecla da liberdade de expressão e opinião, mencionando David Kaye, relator especial da ONU sobre a promoção e proteção do direito à liberdade de opinião e expressão, que diz que a criptografia fornece aos indivíduos um meio de exercer esses seus direitos.

Em âmbito legal novamente, a ministra menciona um princípio da Recomendação Relativa às Diretrizes para Política de Criptografia da Organização para a Cooperação e Desenvolvimento Econômico - OCDE[100], que diz:

---

[98] SUPREMO TRIBUNAL FEDERAL. Tribunal Pleno. ADI 5527-DF, Rel. Min. Rosa Weber, j. 27/05/2020, p. 31.
Disponível em: http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI5527voto.pdf

[99] SUPREMO TRIBUNAL FEDERAL. Tribunal Pleno. ADI 5527-DF, Rel. Min. Rosa Weber, j. 27/05/2020, p. 31.
Disponível em: http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI5527voto.pdf

[100] Recomendação Relativa às Diretrizes para Política de Criptografia da Organização para a Cooperação e Desenvolvimento Econômico – OCDE (1997). Disponível em:

> "o direito fundamental dos indivíduos à privacidade, incluindo o sigilo das comunicações e a proteção dos dados pessoais, deve ser respeitado nas políticas nacionais de criptografia e na implementação e uso de métodos criptográficos".

Com isso, ela conclui seu argumento sobre a "questão da criptografia" afirmando que a criptografia funciona para garantir a preservação do sigilo das comunicações expressa no **art. 5º, XII, da CF**. Diz, por fim, que "entendimento diverso significaria submeter a regra, que é a proteção do sigilo das comunicações, à exceção, que é o acesso do Estado ao conteúdo da comunicação privada no curso da persecução criminal", o que apenas corrobora o já explicitado: a Ministra se mostrou em total concordância com os expositores contrários ao enfraquecimento da criptografia, tanto em aspectos técnicos como legais.

3.2 Edson Fachin

O ministro Fachin inicia fazendo uma síntese do voto e estabelecendo sete premissas de sua argumentação. As cinco primeiras não guardam relação tão direta com o objeto da presente monografia, mas as duas últimas, sexta e sétima premissas, guardam.

Na sexta[101] , o ministro ressalta a importância da criptografia e do anonimato para a proteção de direitos, permitindo o desenvolvimento e compartilhamento de opiniões, o que a faz imprescindível para a vida pública.

Na sétima, o ministro traz o caráter contraditório de enfraquecer a segurança da internet em nome da segurança pública. Ou seja, já na introdução, o ministro dá sinais de que seu entendimento seria semelhante ao de Rosa Weber e o entendimento majoritário dos expositores da audiência.

https://www.oecd.org/sti/consumer/34023696.pdf

[101] SUPREMO TRIBUNAL FEDERAL. Tribunal Pleno. ADPF 403-DF, Rel. Min. Edson Fachin, j. 28/05/2020, p. 1. Disponível em:

A seguir, o ministro faz um resumo das partes e amici curiae sobre as preliminares e sobre o mérito, invocando seus principais argumentos. Ele gasta aproximadamente 40 páginas nesse resumo (metade do conteúdo do voto), o dividindo nos seguintes tópicos[102]:

1. Alegações das Partes sobre as Preliminares
    1.1 Alegações da Procuradoria-Geral da República
    1.2 Alegações do Ministério da Justiça
    1.3 Alegações dos *amicus curiae*
    1.4 Exame das alegações trazidas
2. Alegações das Partes sobre o Mérito
    2.1 Alegações do Partido requerente
    2.2 Alegações do Ministério da Justiça
    2.3 Alegações do Procurador-Geral da República
    2.4 Alegações dos *Amici Curiae*
3. Alegações mais relevantes trazidas na audiência pública
    3.1 Alegações especificamente trazidas pelo WhatsApp
4. Exame das Alegações – Mérito da Arguição

Ao fazer o exame das alegações trazidas pelas partes sobre as preliminares, o ministro relator conclui que a arguição de descumprimento de preceito fundamental merece ser conhecida. Parte, então, para alegações sobre o mérito.

http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADPF403voto.pdf

[102] O ministro não numerou os tópicos, como feito aqui, mas o fiz para organizar melhor e simplificar a menção a cada um deles.

Estas, por mais que guardem relação com os bloqueios e serem parte da ADPF em si, não guardam relação com o objetivo da presente monografia, que é averiguar se e como os votos dos ministros relatores na ADI 5527 e ADPF 403 dialogaram com as contribuições dos expositores da audiência no que diz respeito à regulação judicial da criptografia. Dessa forma, esse "resumo" feito pelo ministro não seria bem aproveitado aqui, de forma que não entraremos em detalhes do dito, mas poderia ser em uma nova pesquisa que analisasse justamente as alegações das partes nas ações e como elas reverberaram nos votos.

No tópico número 3, o ministro apresenta as "alegações mais relevantes trazidas na audiência pública". Por considerá-las "mais relevantes", de certa forma ele faz um juízo de valor, importando ao seu voto as que mais acrescentaram ao debate, em sua visão. Assim, é importante compreender como ele separou esses argumentos mais relevantes, quem foi mencionado, quem não, o que ele colocou das exposições dos mencionados, etc. Detalharei a seguir:

Dentre todas as 23 entidades convocadas, o ministro mencionou 6: a Polícia Federal, a Procuradoria Geral da República, o Comitê Gestor da Internet no Brasil (CGI.Br), o Professor Anderson Nascimento, a Federação de Empresas de Telecomunicação (FEBRATEL) e o Laboratório de Pesquisa de Direito Privado e Internet da Universidade de Brasília.

Ele não separou os grupos em tópicos ou em temas. Apenas fez um resumo do que foi dito por eles, seguindo a ordem das apresentações da audiência.

Sobre a Polícia Federal, o ministro trouxe quatro afirmações dadas por Barros: i) sobre todo o *iter criminis* ser percorrido utilizando os aplicativos de comunicação; ii) sobre a persecução penal não poder ser ditada por empresas de informática, devendo sê-la pelo Estado; iii) a ação controlada não pode afastar a obrigação dos meios de comunicação de oferecer, em momento oportuno, as informações requeridas judicialmente; iv) no passado, empresas como Microsoft e Gmail trouxeram os mesmos

argumentos que os apresentados pelo WhatsApp e mesmo assim, hoje é possível ter acessos excepcionais pelo MPF e PF;[103]

Ele ainda menciona os pontos do Perito da Polícia Federal, Ivo Carvaho, sobre metadados.

Sobre a PGR, mencionou sua alegação de que há legitimidade do Facebook para responder e cumprir decisões que envolvam o WhatsApp; expôs que eles em linhas gerais os pontos que eles usam para defender a improcedência das ações; trouxe a sustentação de Fernanda Teixeira de que há possibilidade de interceptar mensagens do WhatsApp por meio do ataque *man-in-the-middle*[104]*.*

Sobre o CGI.Br, que teve como único representante Demi Geschko, trouxe seu apontamento de que a "criptografia é uma ferramenta para o desenvolvimento da comunidade, seja da área privada, pública; trouxe suas indicações sobre os perigos de criar acessos privilegiados – hipótese dos *backdoors* e as disposições do decálogo elaborado pelo CGI.br, que dispõe que a criptografia é instrumental aos direitos humanos de privacidade e liberdade de expressão[105].

Sobre Anderson Nascimento, informou que ele explica em linhas gerais o que é criptografia e quais seus objetivos. Também informou que o professor esclareceu não ser possível a interceptação de mensagens pelo WhatsApp em virtude de sua criptografia e que trouxe detalhes técnicos sobre as alternativas de interceptação; por fim, destacou que o professor disse haver aplicativos de mensagens que não possuem representação no Brasil e que poderiam ser utilizados pelos usuários[106].

---

[103] SUPREMO TRIBUNAL FEDERAL. Tribunal Pleno. ADPF 403-DF, Rel. Min. Edson Fachin, j. 28/05/2020, p. 42.
Disponível em: http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADPF403voto.pdf
[104] SUPREMO TRIBUNAL FEDERAL. Tribunal Pleno. ADPF 403-DF, Rel. Min. Edson Fachin, j. 28/05/2020, p. 44.
Disponível em: http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADPF403voto.pdf
[105] SUPREMO TRIBUNAL FEDERAL. Tribunal Pleno. ADPF 403-DF, Rel. Min. Edson Fachin, j. 28/05/2020, p. 45.
Disponível em: http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADPF403voto.pdf
[106] SUPREMO TRIBUNAL FEDERAL. Tribunal Pleno. ADPF 403-DF, Rel. Min. Edson Fachin, j. 28/05/2020, p. 46.

Sobre a Federação de Empresas de Telecomunicação, trouxe suas alegações sobre serem responsáveis pelo transporte de todos os dados que circulam na internet, sem acessar ou interferir no conteúdo das informações inseridas; informou que elas alegaram ter criado infraestrutura exclusiva para atender às ordens judiciais e que elas se alinham ao entendimento da Polícia Federal e do Ministério Público Federal, entendendo que o WhatsApp deve cumprir as determinações judiciais[107].

Sobre os representantes do Laboratório de Pesquisa de Direito Privado e Internet da Universidade de Brasília, informou que eles trouxeram aspectos técnicos do ataque *man-in-the-middle*, espelhamento do computador e captura de metadados[108].

Por fim, sobre o Centro de Tecnologia e Sociedade da Escola de Direito da FGV-Rio, trouxe sua afirmação de que no modelo teórico que o WhatsApp diz implementar, não é possível interceptar ou espelhar as comunicações[109].

Note que o ministro pareceu tentar ser abrangente, pois cada um desses grupos expôs uma linha argumentativa um pouco diferente. Ele apenas mencionou o dito por cada um, em muitas oportunidades fazendo simples citação direta.

Até então, o ministro não esboçou qualquer entendimento sobre resultados da audiência e pareceu ter dado prioridade a argumentos de todas as ordens, mas que, de alguma forma se relacionassem com criptografia.

Observe que, diferente dos tópicos anteriores, nos quais ele separa por subtópicos as apresentações de todas as partes e amicus curiae, as expondo, neste ele apenas coloca como subtópico os argumentos do representante do WhatsApp em "Alegações Especificamente Trazidas pelo Whatsapp" - apesar de serem em 23 as entidades convocadas para a Audiência. Isso parece

[107] SUPREMO TRIBUNAL FEDERAL. Tribunal Pleno. ADPF 403-DF, Rel. Min. Edson Fachin, j. 28/05/2020, p. 47.
Disponível em: http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADPF403voto.pdf
[108] SUPREMO TRIBUNAL FEDERAL. Tribunal Pleno. ADPF 403-DF, Rel. Min. Edson Fachin, j. 28/05/2020, p. 48.
Disponível em: http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADPF403voto.pdf
[109] SUPREMO TRIBUNAL FEDERAL. Tribunal Pleno. ADPF 403-DF, Rel. Min. Edson Fachin, j. 28/05/2020, p. 48-49.

significar alguma distinção ou relevância maior dada pelo ministro a este expositor.

Ao apresentar as alegações especificamente trazidas pelo WhatsApp, ele segue não fazendo nenhum juízo de valor ou análise de todo o exposto, apenas resumindo.

Ele menciona as explicações de Brian Acton sobre o funcionamento do WhatsApp e qual a função do aplicativo, suas defesas sobre os benefícios da criptografia de ponta a ponta adotada pelo WhatsApp e por que razão não seria possível que ele interceptasse ou lesse conversas. Traz seus expostos sobre desabilitar a criptografia para apenas um usuário, sobre os backdoors, sobre a técnica do *man-in-the-middle,* sobre espelhar conta em outro dispositivo e sobre a coleta de metadados pelos servidores do aplicativo[110].

Após, o ministro inicia os argumentos finais de seu voto no tópico 4: "exame das alegações – Mérito da Arguição". Como visto, o ministro, na maior parte de seu voto, apenas traz o que foi dito ao longo da ação e da audiência, sem fazer qualquer análise, mas apenas resumindo. De tal forma, não faz sentido para responder se as exposições dialogaram com os votos, objeto desta monografia, analisar esses trechos em que o ministro apenas replica o dito, sem fazer juízos.

Disto e por termos compreendido a estrutura do voto do min. Edson Fachin, não cabendo mais comentários sobre, partamos para a análise do conteúdo de suas alegações.

Como já exposto, o "entendimento majoritário" na audiência pública foi na linha de que os ônus que o implemento de hipóteses de interceptação de mensagens carrega não compensam os bônus, sendo prejudiciais e com um grande volume de consequências negativas - dentre as quais, a violação de direitos fundamentais como liberdade de expressão, direito à privacidade, etc.

[110] SUPREMO TRIBUNAL FEDERAL. Tribunal Pleno. ADPF 403-DF, Rel. Min. Edson Fachin, j. 28/05/2020, p. 49-51.

O entendimento minoritário seguiu a linha de que os ônus compensavam, dada a necessidade de viabilizar as investigações criminais e impedir que os aplicativos de comunicação protegidos por criptografia de ponta a ponta se tornassem "cenários livres na criminalidade".

Como vimos, inicialmente o ministro já dá a entender que concorda com o entendimento majoritário por apresentar em uma de suas premissas a visão de que é contraditório enfraquecer a segurança da internet em nome da segurança pública. Porém, apenas após 50 páginas de resumos que ele começa seu exame de mérito, o que confirmaria essa compreensão inicial.

O ministro inicia seu exame expressando o ineditismo dessas circunstâncias. Ele afirma que mesmo que os princípios examinados tenham aplicação em outros casos, a solução proposta por seu voto não abrangeria outros debates já submetidos à pauta da Suprema Corte[111]. Ele cita alguns exemplos de casos nos quais os mesmos princípios deste foram abordados, mas ressalta que o debate nesta ação é novo e distinto.

O ministro apresenta dois objetos da ADPF, e o primeiro deles é, pode-se dizer, precursor ao questionamento principal trazido pela min. Rosa Weber. Ele diz que um dos objetos da ação é (i) saber se é constitucional a ordem judicialde acesso por órgãos do Estado ao conteúdo de comunicações protegidas por criptografia, conforme previsão constante do art. 7º, II, do Marco Civil da Internet[112];

Ser ou não constitucional a ordem judicial de acesso passa pelo seguinte ponto: Caso seja, seriam necessárias alternativas, mudanças no protocolo criptográfico que viabilizassem a ordem judicial. É adequado, então, trazer o questionamento levantado pela min. Rosa Weber: Cabe ao Estado obrigar os desenvolvedores a criar essa alternativa? Há de averiguar se o min. Edson Fachin respondeu algo nesse sentido.

---

[111] SUPREMO TRIBUNAL FEDERAL. Tribunal Pleno. ADPF 403-DF, Rel. Min. Edson Fachin, j. 28/05/2020, p. 53.
Disponível em: http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADPF403voto.pdf

[112] SUPREMO TRIBUNAL FEDERAL. Tribunal Pleno. ADPF 403-DF, Rel. Min. Edson Fachin, j. 28/05/2020, p. 53.
Disponível em: http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADPF403voto.pdf

O segundo objetivo, por sua vez, parte da premissa de que os bloqueios são constitucionais. Assim, a ação objetivaria (ii) saber se a sanção prevista no inciso III do art. 12 do mesmo diploma legal pode ser aplicada pelo Poder Judiciário[113].

O Ministro expõe sua primeira conclusão, novamente concordando com a min. Rosa Weber e trazendo a liberdade de expressão como direito defendido pela criptografia. Ele diz que *como atestam os participantes da sociedade civil queparticiparam da audiência*[114], a criptografia funciona como ferramenta para assegurar a proteção necessária à liberdade de expressão numa sociedade democrática. Assim, conclui que a "criptografia é (...) um meio de se assegurar a proteção de direitos que, em uma sociedade democrática, são essenciais para a vida pública[115]".

Essa conclusão, para além de se relacionar com o voto da min. Rosa Weber, parece se relacionar com o proferido por um dos expositores da audiência. Ela se assemelha à afirmação de Ronaldo Lemos, do Instituto de Tecnologia e Sociedade do Rio (ITS-RIO), além de um dos "pais" do Marco Civil da Internet, que disse que "a criptografia é essencial para promover direitos quesão chave de abóbada do Estado Democrático de Direito (...)".[116]

Em seguida, o min. Edson Fachin expõe sua segunda conclusão, ao alegar que não só a sociedade civil, mas todos os órgãos do Estado "reconhecem que a criptografia protege os direitos dos usuários da internet, garantindo a privacidade de suas comunicações[117]".

---

[113] SUPREMO TRIBUNAL FEDERAL. Tribunal Pleno. ADPF 403-DF, Rel. Min. Edson Fachin, j. 28/05/2020, p. 53.
Disponível em: http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADPF403voto.pdf
[114] SUPREMO TRIBUNAL FEDERAL. Tribunal Pleno. ADPF 403-DF, Rel. Min. Edson Fachin, j. 28/05/2020, p. 54.
Disponível em: http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADPF403voto.pdf
[115] SUPREMO TRIBUNAL FEDERAL. Tribunal Pleno. ADPF 403-DF, Rel. Min. Edson Fachin, j. 28/05/2020, p. 54.
Disponível em: http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADPF403voto.pdf
[116] Transcrição da Audiência Pública n.21, 2017, pág. 208. Disponível em: http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADI5527ADPF403AudinciaPblicaMarcoCivildaInterneteBloqueioJudicialdoWhatsApp.pdf..
[117] SUPREMO TRIBUNAL FEDERAL. Tribunal Pleno. ADPF 403-DF, Rel. Min. Edson Fachin, j. 28/05/2020, p. 54. Disponível em:

Com isso, o ministro afirma não fazer sentido apenas a sociedade (sem participação estatal) se mobilizar para garantir tal proteção. O Estado brasileiro também deve se mobilizar para alcançar o maior e melhor cenário de segurança do ambiente digital[118].

O interessante nessa afirmação é que, conforme exposto nas conclusões preliminares, foram justamente representantes do Estado, em seus variados âmbitos (Ministério Público, Polícia Federal e o Ministério de Ciência e Tecnologia), que foram contrários à manutenção da criptografia - apesar de reconhecerem que ela realmente protege tais direitos.

A terceira e última conclusão do ministro relator foi, na verdade, uma preocupação. Ele aborda dificuldades técnicas oriundas desse modelo de privacidade – aplicativos de comunicação protegidos por criptografia.

Ele afirma que as apurações de crimes que violam direitos fundamentais e ameaçam o Estado de Direito – como pornografia infantil e condutas racistas - dependem da autorização do próprio usuário do serviço, o que dificulta a questão[119].

Essa conclusão me pareceu um pouco confusa. Acredito, entretanto, que o que ele quis dizer foi que com a manutenção da criptografia para os aplicativos de comunicação e a consequente impossibilidade de interceptação de mensagens e monitoramento pelos órgãos de segurança, apenas será possível investigar as conversas do usuário com a interceptação de seu aparelho celular – talvez, por mandado de justiça que defina a entrega do aparelho e ulterior quebra da senha. Isso poderia atrapalhar o processo de investigação.

Essa consequência negativa foi de certa forma exposta pelos expositores favoráveis às hipóteses de enfraquecimento da criptografia, porém o ministro a viu apenas como um desafio, nao como algo fundamental, como exposto pelos representaantes do MPF e da PF.

http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADPF403voto.pdf

[118] SUPREMO TRIBUNAL FEDERAL. Tribunal Pleno. ADPF 403-DF, Rel. Min. Edson Fachin, j. 28/05/2020, p. 54.
Disponível em: http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADPF403voto.pdf

[119] SUPREMO TRIBUNAL FEDERAL. Tribunal Pleno. ADPF 403-DF, Rel. Min. Edson Fachin, j.

Após as três conclusões - duas positivas e uma negativa no concernente à manutenção da criptografia - o ministro, então, volta às premissas apresentadas no início do voto para definir que a questão-chave da arguição é: o risco consequente do uso da criptografia justifica sua restrição e a imposição das hipóteses de enfraquecimento[120]?

O ministro avalia que para obter tal resposta, é preciso haver "um rigoroso exame de proporcionalidade", sopesando pontos positivos e negativos. Além disso, ele diz que a corte deve levar em conta o caráter técnico-científico da questão[121].

A partir disso, e só após essas ponderações, o ministro define que seu voto se estrutura no exame dos argumentos sobre os direitos envolvidos na presente questão e exame da intensidade das consequências de eventuais alterações na criptografia adotada pelo Whatsapp e como essas consequências afetariam esses direitos[122].

Aqui, ele parece se afastar um pouco do conteúdo da audiência, não fazendo menção aos expositores, mas dialoga com a relatora, trazendo os mesmos artigos que a relatora apresentou do Pacto Internacional de Direitos Civis e Políticos. Além, traz outros dois (art. 11 e art. 13 do Pacto de São José da Costa Rica) para exemplificar o fundamento legal.

Ele diz que mesmo que da leitura simples destes dispositivos não se extraia imediatamente sua aplicação no ambiente online, a interpretação deve seguir a seguinte regra: "direitos que as pessoas têm offline devem também ser protegidos online".

---

[120] SUPREMO TRIBUNAL FEDERAL. Tribunal Pleno. ADPF 403-DF, Rel. Min. Edson Fachin, j. 28/05/2020, p. 55.
Disponível em: http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADPF403voto.pdf
[121] SUPREMO TRIBUNAL FEDERAL. Tribunal Pleno. ADPF 403-DF, Rel. Min. Edson Fachin, j. 28/05/2020, p. 55.
Disponível em: http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADPF403voto.pdf
[122] Pág. 55, Voto Min. Edson Fachin, ADPF 403 SUPREMO TRIBUNAL FEDERAL. Tribunal Pleno. ADPF 403-DF, Rel. Min. Edson Fachin, j. 28/05/2020, p. 55.
Disponível em: http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADPF403voto.pdf

O ministro Edson Fachin, assim como a ministra Rosa Weber, entra no debate dos direitos on-line relacionando a questão fundamentalmente à liberdade de expressão, afirmando que garantir a proteção da privacidade é garantir o direito à liberdade de expressão em âmbito coletivo.

Ele, após o "afastamento", volta a se relacionar com a audiência, ao relembrar que os órgãos de segurança pública e a Procuradoria-Geral da República apontaram que as hipóteses de acesso excepcional "asseguram aos agentes de investigação um mecanismo indispensável para a consecução de suas atividades de investigação em casos graves[123]".

O ministro repete seu questionamento: a gravidade dos crimes faz com que o acesso excepcional seja razão suficiente para justificar a restrição da privacidade? Assim, segue trazendo exemplos de situações alarmantes na realidade digital contemporânea: situações e esquemas de vigilância constantemente interferem na livre manifestação do direito de opinião e liberdade de expressão[124].

Estas situações alarmantes foram expostas também na audiência por Ronaldo Lemos (ITS-RIO), que mencionou as denúncias de Edward Snowden [125] , e por Juliano Albuquerque, do Núcleo Direito, Incerteza e Tecnologia da Faculdade de direito da USP, que trouxe exemplos internacionais de governos autoritários que exercem controle sobre seus cidadãos e os vigiam constantemente.

O min. Edson Fachin traz então a importância da criptografia, pois ela inviabiliza a coleta indevida de informação, sendo fundamental nesses ambientes de

[123] SUPREMO TRIBUNAL FEDERAL. Tribunal Pleno. ADPF 403-DF, Rel. Min. Edson Fachin, j. 28/05/2020, p. 65.
Disponível em: http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADPF403voto.pdf

[124] SUPREMO TRIBUNAL FEDERAL. Tribunal Pleno. ADPF 403-DF, Rel. Min. Edson Fachin, j. 28/05/2020, p. 68. Disponível em: http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADPF403voto.pdf

[125] Em 2013 as divulgações de Edward Snowden, ex-agente da NSA, sobre a capacidade tecnológica de vigilância americana, influenciaram profundamente os debates sobre a violação de dados privados em toda a comunidade internacional, incluindo o Brasil, uma vez que nos documentos divulgados havia indícios de que um dos alvos da espionagem era a até então presidente Dilma Rousseff. (2013). Disponível em: http://g1.globo.com/politica/noticia/2013/09/documentos-da-nsa-apontam-dilma-rousseff-como-alvo-de-espionagem.html ; e em: "Snowden NSA Files Decoded". Guardian. (01/11/13). https://goo.gl/MEmVl5

vigilância e locais e cenários caracterizados por censura. Isso ressalta a importância da tecnologia no Brasil, pois a vedação à censura é um dos pilares Constitucionais pós 1988. Ainda, em âmbito internacional, o ministro conclui que criptografia figuraria como mecanismo capaz de assegurar direitos humanos[126].

Ele traz, assim como a ministra Weber, informação técnica externa à Audiência, citando trecho do relatório de David Kaye, apresentado no Conselho de Direitos Humanos, que 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[127]" (Grifo Nosso).

O ministro, então, começa a apresentar consequências das hipóteses de enfraquecimento, como a possibilidade de a vulnerabilidade do sistema vir a ser explorada por terceiros, a já mencionada migração para novos aplicativos – que poderia resultar em migração para sistemas mais difíceis de serem rastreados, o que dificultaria o trabalho do poder público[128].

Essas consequências figuram no rol de exposições contrárias ao enfraquecimento da criptografia, o que mostra que o ministro não deixou de dialogar e concordar com os expositores em seu voto.

Ele retoma, então, sua sétima premissa, afirmando ser contraditório, que em nome da segurança pública seja negligenciada a segurança da internet. Conclui, assim, que o risco causado pelo uso da criptografia não justifica a imposição de soluções que envolvam acesso excepcional e que é inconstitucional proibir as pessoas de utilizarem a criptografia ponta-a-ponta, pois isso impactaria desprporcionalmente as pessoas mais vulneráveis, com menores possibilidades de ter sua segurança e privacidade garantidas[129].

[126] SUPREMO TRIBUNAL FEDERAL. Tribunal Pleno. ADPF 403-DF, Rel. Min. Edson Fachin, j. 28/05/2020, p. 68.
Disponível em: http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADPF403voto.pdf
[127] SUPREMO TRIBUNAL FEDERAL. Tribunal Pleno. ADPF 403-DF, Rel. Min. Edson Fachin, j. 28/05/2020, p. 69.
Disponível em: http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADPF403voto.pdf
[128] SUPREMO TRIBUNAL FEDERAL. Tribunal Pleno. ADPF 403-DF, Rel. Min. Edson Fachin, j. 28/05/2020, p. 70.
Disponível em: http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADPF403voto.pdf

Por fim, o Ministro frisa que o fato de reconhecer a constitucionalidade da 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[130]". Ou seja, as empresas seguem responsáveis por adotar medidas que visem reduzir as práticas de ilícitos.

CONCLUSÃO

O objetivo principal desta conclusão é responder à seguinte pergunta de pesquisa: "se, e como os votos dos ministros relatores na ADI 5527 e ADPF 403 dialogaram com as contribuições dos expositores da audiência pública n.21 no que diz respeito à regulação judicial da criptografia? "

São objetivos secundários: refletir sobre o exposto no capítulo "Da audiência pública" e sobre o exposto no capítulo "Votos dos Relatores", expondo, agora, um panorama geral do debate, não só da audiência, ou só do julgamento.

Se os ministros relatores dialogaram, a resposta é inconclusiva. De todo o analisado, pode-se dizer que as contribuições dos expositores se refletiram nos votos, mas não com absoluta certeza. Isso porque não houve citações diretas, indiretas, citações de citações ou referências nas notas de rodapé, por exemplo. Por mais que muito do mapeado na audiência fosse semelhante ao exposto nos votos, não houve menção aos expositores da audiência pelos ministros. Quando muito, o ministro resumiu as manifestações deles, mas, como visto, ele o fez sem analisar o mérito.

[129] SUPREMO TRIBUNAL FEDERAL. Tribunal Pleno. ADPF 403-DF, Rel. Min. Edson Fachin, j. 28/05/2020, p. 70.
Disponível em: http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADPF403voto.pdf
[130] SUPREMO TRIBUNAL FEDERAL. Tribunal Pleno. ADPF 403-DF, Rel. Min. Edson Fachin, j. 28/05/2020, p. 71.

Em algumas oportunidades, por exemplo, os ministros pareciam ter transcrito em seus votos o dito pelos expositores, mas como suas próprias conclusões e opiniões sobre os assuntos.

Cito aqui quando o ministro Fachin conclui na página 54 de seu voto que a criptografia é um meio de se assegurar a proteção de direitos que são essenciais em uma sociedade democrática. E isso foi expressamente dito por Ronaldo Lemos, representante do ITS-RIO.

A ministra Weber, por sua vez, ao informar na página 27 de seu voto que o implemento de *backdoors* é uma hipótese que vem sendo abandonada ao longo do mundo, está basicamente replicando o que Fábio Wladimir, representante da Assespro, falou. Ela o faz novamente ao afirmar que uma das consequências de enfraquecer a criptografia do WhatsApp exclusivamente seria o fato de os usuários que se muniam dele para cometer crimes simplesmente migrarem para outros aplicativos que não estivessem sob alcance das autoridades.

Porém os ministros o fazem conforme o desenvolvimento de sua própria argumentação, sem mencionar os expositores - o que foi feito, por exemplo, com David Kaye, fonte externa de material para os votos.

Isso dificulta assegurar que foi o exprimido na audiência que os fizeram pensar assim difícil ou se, por exemplo, as conclusões foram mesmo dos ministros, influenciados por estudos externos.

Por outro lado, algumas das afirmações dos ministros pareceram ser conclusões que se deram a partir do dito na audiência. A min. Rosa Weber, por exemplo, parece partir dos exemplos trazidos por Diego Aranha, professor da Unicamp, de grupos que restariam prejudicados com o enfraquecimento da criptografia, para concluir que o enfraquecimento teria como consequência formas de violações de direitos.

Ela trouxe em seu voto a importância da criptografia de chave pública. Para que o debate sobre criptografia e, mais especificamente, sobre criptografia de ponta a ponta se iniciasse, mesmo que em âmbito jurídico,

seria necessário que os ministros entendessem esse mecanismo. Isso foi explicado na audiência e foi uma das perguntas que a motivou.

> "1 – Em que consiste a criptografia ponta a ponta (end to end) utilizada por aplicativos de troca de mensagens como o WhatsApp?"

Concluo, então, que não há provas de que eles efetivamente dialogaram com os expositores, por mais que isso pareça. Pensei em seguir esta linha de pensamento: convocação da audiência para obter informações para o julgamento – informações pedidas foram dadas pelos expositores – informações apareceram nos votos que compõem o julgamento = houve diálogo. Só que a conclusão correta não seria que houve, mas que há indícios de que houve.

Uma vez que a resposta do "se (...) houve diálogo" foi inconclusiva, traçar "como" houve, ou seja, determinar as formas que o suposto diálogo ocorreu, também o seria. Apesar de a ministra em alguns momentos falar "algo muito parecido" ou "basicamente replicar", não é possível, por exemplo, afirmar que houve citação. Só seria possível ter certeza de que a foi tirada daaudiência se os ministros dissessem que o fizeram

Sobre a audiência pública em si, cabe lembrar que as alegações iniciais do WhatsApp eram de impossibilidade técnica resultante do tipo de criptografia adotada. Uma das perguntas motivadoras da audiência foi justamente essa: "seria possível a interceptação de conversas e mensagens por meio do aplicativo WhatsApp ainda que esteja ativada a criptografia de ponta a ponta? "

Houve alguns consensos e o primeiro deles foi sobre a possibilidade de haver interceptação de mensagens e o enfraquecimento da criptografia de ponta a ponta, diferente do que era alegado originalmente pelo WhatsApp. É importante ressaltar que os argumentos não foram contra a existência de criptografia, mas contra a manutenção da criptografia forte, ou seja, sem

vulnerabilidades ou formas de interceptação pelas autoridades.

Porém, esse consenso foi um pouco complexo. Brian Acton não deixou de afirmar que com o sistema atual de criptografia do WhatsApp, não seria possível interceptar as mensagens. O Protocolo utilizado não possui vulnerabilidades. Anderson Nascimento, especialista acadêmico em criptografia, por sua vez, afirma que para que as mensagens fossem interceptadas, seria necessário alterar o protocolo criptográfico.

Por isso que a conclusão é de que há, sim, possibilidade de interceptação das mensagens. Porém não com os moldes atuais. Não faz sentido dizer que há inviabilidade técnica, sendo que há possibilidade de alterar o protocolo criptográfico e/ou implementar as hipóteses de interceptação.

O que faz sentido dizer é que o regime criptográfico atual inviabiliza a interceptação, mas não que ela não poderá acontecer em instância alguma. Talvez a melhor afirmação para definir essa situação é "o WhatsApp não pode, atualmente, interceptar, mas é possível que ele implemente hipóteses de interceptação". A afirmação de que não é possível interceptar mensagens pelo WhatsApp, portanto, não é verdadeira.

Outro consenso implícito é de que as consequências desse enfraquecimento eram negativas, mas alguns expositores as viam como necessárias para as investigações, enquanto outros as viam como desproporcionais, de forma a carregar muito mais ônus que bônus.

O perfil-base dos expositores que se manifestaram favoravelmente a este enfraquecimento era "público". Representantes do Ministério Público Federal, da Polícia Federal e do Ministério de Ciência e Tecnologia. Isso pareceu refletir nos seus anseios e argumentos, visto que eles enxergaram a possibilidade de uma empresa possuir tecnologia que dificultasse e até inviabilizasse investigações, ou seja, que inviabilizasse o acesso pelo Estado, como inadmissível.

O perfil-base dos expositores contrários ao enfraquecimento era mais diverso e, talvez, mais técnico. Eram em sua maioria pesquisadores, ligados a Universidades ou não, que, apesar de falarem em necessidade de defender

direitos como privacidade e liberdade de expressão, não se mantiveram tanto no âmbito jurídico do debate.

As consequências seriam, em primeiro plano, técnicas, matemáticas, mas com repercussões jurídicas. Os expositores favoráveis argumentaram mais juridicamente, trazendo o processo penal à baila, discutindo artigos do marco civil e até defendendo a constitucionalidade das ordens de bloqueio – isso foi feito pelo representante da associação dos magistrados, o que, por não se relacionar tanto com a regulação judicial da criptografia, não foi exposto no corpo da presente monografia.

Em resumo, os principais pontos positivos e negativos do enfraquecimento da criptografia expostos foram:

A) Positivos

i) a persecução penal não seria ditada por empresas privadas, mas pelo Estado; ii) não teríamos um cenário livre na criminalidade – paraíso digital; iii) a investigação pela Polícia Federal seria mais efetiva; iv) manutenção dos sistemas de segurança, mas com possibilidade de intervenção estatal

B) Negativos

i) interceptação por *man-in-the-middle* seria detectável; ii) risco de a polícia receber informações falsas enviadas propositalmente pelos criminosos que sabem que estão sendo monitorados; iii) vigilância de pessoas não suspeitas e inocentes; iv) redução da segurança; v) WhatsApp colocado em disparidade econômica; vi) repercussão internacional

Todos eles apareceram nos votos dos ministros. Destaco que o min. Edson Fachin, no tópico "Alegações mais relevantes trazidas na audiência pública" fez um panorama geral do exposto, citando os expositores e, de certa forma,

englobando todas essas consequências.

Isso prova que o caráter técnico do debate apareceu nos votos dos ministros apesar da natureza jurídica da Ação Direta de Inconstitucionalidade e da Arguição de Descumprimento de Prefeito Fundamental.

Apesar de os votos dos ministros relatores não configurarem um entendimento colegiado, eles iniciaram uma tendência: a constitucionalidade da criptografia e, por consequência, a inconstitucionalidade dos bloqueios judiciais e sanções impostas ao WhatsApp. Ambos votaram dessa forma.

No que concerne os diálogos entre os votos, em dado momento da análise do proferido pelo ministro relator, repliquei uma pergunta para buscar relação com o voto da ministra Weber: Cabe ao Estado obrigar os desenvolvedores acriar essa alternativa?

Ela, que levantou a questão, também não a responde expressamente, mas, em nova concordância com o relator, defende que é função do Estado assegurar que não haja afrouxamento de liberdades. Corrobora, então, a concordância por, ao longo de seu voto, explicitar que viabilizar o enfraquecimento da criptografia configuraria em maiores quantidades de direitos violados.

Os ministros seguiram o entendimento majoritário exposto na audiência pública, mas não deixaram de sopesar o lado negativo da manutenção da criptografia da forma atual. O min. Edson Fachin, por exemplo, cita comodesvantagem a dificuldade que os órgãos de segurança possuirão para investigar crimes nas plataformas digitais, em especial, aplicativos de comunicação que se munem da criptografia de ponta a ponta.

Ele frisa, ao final de seu voto, que o fato de votar a favor da constitucionalidade dessa tecnologia não isenta as empresas de buscarem medidas para evitar as práticas de ilícitos em suas plataformas.

Ambos trazem aos votos tanto exposições da audiência como dispositivos legais nacionais e internacionais, além de textos externos – em comum, ambos trouxeram os artigos 17 e 19 do Pacto Internacional sobre Direitos Civis e Políticos, no âmbito das Nações Unidas e citaram David Kaye,

Relator Especial das Nações Unidas sobre a promoção e a proteção do direito à liberdade de opinião e de expressão.

Um ponto interessante sobre afinidades entre os votos dos dois ministros foi que, apesar de toda a relevância da criptografia e da audiência para o debate, estes foram pontos minoritários nos dois votos. A min. Rosa Weber, em 36 páginas de argumentação, separou 6 para falar da "questão da criptografia" e o min. Edson Fachin separou aproximadamente 9 páginas das 76 de seu voto para tratar sobre a audiência pública especificamente. Apesar disso, eles não deixaram de tratar dos temas em algumas oportunidades em outros espaços de seus votos.

Ilustrados todos esses pontos, conclui-se que os votos de Edson Fachin, ministro relator da ADPF 503 e Rosa Weber, ministra relatora da ADI 5527 dialogaram com as exposições feitas na audiência pública n.21 em inúmeros âmbitos, assumindo alguns argumentos como verdadeiros e apropriando-se deles, usando outros como fundamentação para seus próprios argumentos e discordando de alguns, sem negar sua relevância.

De tal forma, é possível afirmar que a sociedade civil, representada em suas diversas facetas pelos expositores da audiência reverberou no mundo jurídico, sob a ótica dos votos dos relatores no que tange à criptografia e sua futura regulação judicial.

BIBLIOGRAFIA:

BRASIL. Lei nº 12.965, de 23 de abril de 2014. *Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil*. Brasília. 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

Definidos participantes e cronograma da audiência pública sobre WhatsApp e Marco Civil da Internet (2017). Disponível em: http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=341437

Dicionário Houaiss da língua portuguesa. Rio de Janeiro: Objetiva, 2009.

FERRAZ JÚNIOR, T. S. (1993). *Sigilo de dados*: o direito à privacidade e os limites à função fiscalizadora do Estado. *Revista Da Faculdade De Direito, Universidade De São Paulo*, *88*, 439-459. Recuperado de http://www.revistas.usp.br/rfdusp/article/view/67231

LIGUORI FILHO, Carlos Augusto; SALVADOR, João Pedro Favaretto. *Crypto wars e bloqueio de aplicativos: o debate sobre regulação jurídica da criptografia nos estados unidos e no brasil*: o debate sobre regulação jurídica da criptografia nos Estados Unidos e no Brasil. **Revista da Faculdade de Direito Ufpr**, [s.l.], v. 63, n. 3, p. 135-161, 22 dez. 2018. Universidade Federal do Paraná. http://dx.doi.org/10.5380/rfdufpr.v63i3.59422

Questionados artigos do Marco Civil da Internet que permitem bloqueio de aplicativos, (2016). Disponível em: http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=317478&caixaBusca=N

Partido pede que STF suspenda decisão judicial que bloqueou WhatsApp, (2016). Disponível em: https://www.conjur.com.br/2016-jul-19/partido-stf-suspenda-decisao-bloqueou-whatsapp

PFEFFERKORN, Riana. *The Risks of "Responsible Encryption*". [s.l.] The Center for Internet and Society, fev. 2018.

Suspensão do bloqueio do WhatsApp, (2016). Disponível em: http://www.omci.org.br/jurisprudencia/97/suspensao-do-bloqueio-do-whatsapp

Relatora entende que aplicativos de mensagens não podem ser obrigados a fornecer dados criptografados (2020). Disponível em: https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=444265&ori=1

Relatores consideram inconstitucional quebra do sigilo de comunicação em aplicativos de mensagens, (2020). Disponível em: https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=444384&ori=1

SUPREMO TRIBUNAL FEDERAL. Tribunal Pleno. ADPF 403-DF, Rel. Min. Edson Fachin, j. 28/05/2020, Disponível em: http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADPF403voto.pdf

SUPREMO TRIBUNAL FEDERAL. Tribunal Pleno. ADI 5527-DF, Rel. Min. Rosa Weber, j. 27/05/2020. Disponível em: http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI5527voto.pdf