JOTA

O zap e a toga

Mapeamento do debate sobre bloqueio de aplicativos e criptografia no STF

Carlos Augusto Liguori Filho

15 de Junho de 2017 - 12h12

Audiência pública que discute bloqueio judicial do WhatsApp *Foto: Carlos Moura/SCO/STF (02/06/2017)*

BLOQUEIO | CRIPTOGRAFIA | DESTAQUES | PROTEÇÃO DE DADOS | STF | WHATSAPP

Nos dias 2 e 5 de junho foi conduzida no Supremo Tribunal Federal uma audiência pública que visava debater aspectos técnicos e jurídicos relativos a bloqueio de aplicativos por descumprimento de ordem judicial. A audiência pública contou com diversos especialistas das áreas jurídicas e técnicas, além dos principais envolvidos nos bloqueios: órgãos de investigação e persecução criminal e o próprio Whatsapp, Inc.

Retomando rapidamente o cenário: em 2015 e 2016, o Whatsapp foi bloqueado no Brasil em três ocasiões distintas como sanção pelo descumprimento de ordens judiciais que solicitavam o fornecimento do conteúdo de mensagens trocadas por usuários da plataforma. Estas ordens judiciais haviam sido obtidas no contexto de investigações criminais (todas correndo sob sigilo), com ao menos uma delas envolvendo uma suposta rede de tráfico de drogas interestadual cujas comunicações ocorria por meio do aplicativo.

Os três bloqueios compartilharam algumas características em comum: (i) todos eles foram autorizados por juízes de primeira instância; (ii) todos eles foram rapidamente revertidos em instâncias superiores. De forma a evitar possíveis bloqueios futuros, algumas ações foram ajuizadas perante o Supremo Tribunal Federal, instigando a corte a dar uma resposta final com relação à legalidade dos bloqueios.

Uma destas ações, a Arguição de Descumprimento de Preceito Fundamental (ADPF) 403, ajuizada pelo

Partido Popular Socialista (PPS), foi apreciada liminarmente pelo STF em julho de 2016 e restabeleceu o serviço quando do terceiro bloqueio. Ao deferir o pedido, o Ministro Lewandowski identificou uma possível violação do direito à comunicação (Art. 5º, IX da Constituição) e a ADPF seguiu para julgamento no plenário.

Devido ao fato de que as questões envolvidas no caso "extrapolam os limites estritamente jurídicos e exigem conhecimento transdisciplinar a respeito do tema", o STF entendeu ser necessária a convocação de audiência pública para uma discussão mais aprofundada dos bloqueios. Optou-se por conduzir a audiência conjuntamente com outra ação ajuizada no Tribunal, a Ação Direta de Inconstitucionalidade (ADI) 5537, de autoria do Partido da República (PR), uma vez que, no entendimento dos Ministros, a discussão presente nas duas ações teria relação "íntima e ínsita".

O que foi analisado na audiência pública?

Tanto a ADI quanto a ADPF sugerem que o bloqueio do aplicativo seria inconstitucional. Diferem, no entanto, nas razões apontadas desta inconstitucionalidade.

De relatoria da Ministra Rosa Weber, a **ADI 5537** alega que os dispositivos legais utilizados para justificar juridicamente o bloqueio do aplicativo são inconstitucionais. Os dispositivos em questão são os incisos III e IV do Artigo 12 da Lei nº 12.965/14, também conhecida como Marco Civil da Internet (MCI), que diz:

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

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

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

Os atos previstos no Artigo 11 consistem em: "*operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações*". De acordo com o alegado na **ADI 5537**, a possibilidade de bloqueio advinda da leitura dos dispositivos iria diretamente contra o direito fundamental de livre comunicação previsto na constituição (Art. 5º, IX), de onde surgiria sua inconstitucionalidade.

Por sua vez, de relatoria do Ministro Edson Fachin, a **ADPF 403** alega inconstitucionalidade da própria decisão de bloqueio como sanção a descumprimento de ordem judicial. Alega-se que a decisão, além de desproporcional, violaria o supramencionado direito fundamental de comunicação. Pede-se, na ação, que não haja futuras ordens de bloqueio de aplicativos como as já realizadas.

Apesar de parecer quase completamente jurídica, a discussão sobre a legalidade dos bloqueios envolve diretamente aspectos técnicos. Se, em um primeiro momento, o Whatsapp apenas não armazena conteúdos de comunicações dos usuários em seus servidores, a possibilidade técnica de acesso a estes conteúdos se modificou drasticamente em abril de 2016, quando o serviço implementou a chamada **criptografia ponta-a-ponta** em seu sistema.

De forma simplificada, esta ferramenta técnica torna o conteúdo das mensagens legível apenas para o remetente e seu destinatário (as "pontas" da comunicação), uma vez que a chave para decifrar o conteúdo é gerada e está contida exclusivamente em seus celulares. Neste sentido, ainda que a empresa armazene o conteúdo das conversas em seus servidores, este conteúdo somente será legível para os usuários que possuem a chave.

Com este cenário em mente, os Ministros buscavam também compreender os limites técnicos da tecnologia e as consequências jurídicas e sociais de sua adoção ou rejeição.

A seguir serão expostos, em síntese, três principais pontos do debate na audiência pública: (i) legalidade do bloqueio; (ii) possibilidade técnica do fornecimento das informações; e (iii) consequências da implementação de mecanismos de acesso excepcional em sistemas criptografados para fins de investigação policial.

Sobre a legalidade dos bloqueios

Debruçando-se especificamente sobre o conteúdo das ações analisadas, alguns expositores defenderam a **legalidade do bloqueio** como sanção e a proporcionalidade dessa medida nos casos concretos. Reiteraram, nesse sentido, que a sanção é claramente prevista nos já mencionados dispositivos do Marco Civil da Internet e que sua aplicação foi necessária devido à ausência de cooperação do Whatsapp no fornecimento das informações solicitadas em investigações criminais. O Departamento da Polícia Federal afirmou que a colaboração do aplicativo era fundamental para a investigação, uma vez que não há investigação criminal na atualidade que não envolve a utilização do serviço por criminosos para a comunicação.

De forma semelhante, o Ministério Público Federal insistiu na legalidade do bloqueio, entendendo que só seria ilegal a sanção se o serviço pudesse ser enquadrado como serviço de caráter público ou essencial. Os serviços essenciais, estabelecidos na Lei nº 7.783/89, estariam sujeitos ao chamado princípio da continuidade (ou permanência), que impede sua total interrupção. Devido à multiplicidade de meios de comunicação, o entendimento apresentado pelo MPF foi que o serviço em questão não era essencial e que, por isso, com base no MCI e no caso concreto, a medida de bloqueio foi legal e proporcional.

Em sentido diametralmente oposto, o Instituto de Tecnologia e Sociedade do Rio (ITS) defendeu a absoluta **ilegalidade do bloqueio**. O Instituto, que participou do caso também como *amicus curiae*, defendeu a constitucionalidade dos dispositivos do Art. 12 (objeto da ADI), mas negou a constitucionalidade de sua interpretação. Na visão do Instituto, o dispositivo não viabiliza em nenhuma hipótese o bloqueio do serviço pelos provedores de conexão à internet, apenas a suspensão das atividades de "*operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações*", atividades estas que são realizadas pelo próprio aplicativo, nada tendo a ver com a infraestrutura da rede.

Ademais, o ITS afirma que as sanções previstas no artigo seriam aplicáveis apenas caso o provedor de aplicação não respeitasse os deveres impostos pelos artigos 10 e 11 do MCI, quais sejam, "a preservação da intimidade, da vida privada, da honra e da imagem" e a "privacidade, proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros". Este posicionamento é também compartilhado pelo Instituto Brasileiro de Defesa do Consumidor (IDEC).

Além disso, o Instituto aponta também para a desproporcionalidade da aplicação da sanção e para uma evidente violação do direito à comunicação, fundamentando-se, principalmente, no fato de que a decisão de um único juiz de primeira instância atingiu mais de 100 milhões de brasileiros.

Por fim, vale mencionar ainda o posicionamento da Associação Internetlab, que afirmou que **o bloqueio seria ilegal no caso em questão, mas que poderia ser legal em outros casos**. A Associação indicou que um eventual bloqueio de uma plataforma cuja atividade é incompatível com o ordenamento jurídico brasileiro (por exemplo, uma que fosse dedicada precipuamente a atividades ilícitas) seria permitido, mas que o bloqueio como sanção ao não cumprimento de ordem judicial é desproporcional e ilegal.

Sobre a possibilidade técnica de cumprimento das ordens judiciais

Apesar de tratar de diversas controvérsias legais, o principal motivo para a convocação da audiência pública orbitou a possibilidade técnica do Whatsapp de fornecer as informações solicitadas no âmbito da investigação criminal. A empresa fundamentalmente aponta duas peculiaridades técnicas de seu serviço que têm impacto direto na viabilidade do fornecimento das informações: (i) por um lado, diz que **o Whatsapp não armazena o conteúdo das conversas de seus usuários em seus servidores**; e (ii) por outro lado, afirma que, devido à utilização de **criptografia ponta-a-ponta,** mesmo que houvesse uma obrigação de armazenamento destas conversas, seus conteúdos estariam criptografados e as chaves para decriptação só estariam acessíveis para os remetentes e destinatários das mensagens, uma vez que esta chave é gerada e armazenada apenas nos próprios aparelhos celulares. O fornecimento das informações seria, portanto, tecnicamente impossível.

Sobre o **primeiro ponto**, pertinente foi a observação do Núcleo Direito, Incerteza e Tecnologia da Faculdade de Direito da USP, de que o Marco Civil da Internet não obriga, em nenhum momento, que os provedores de aplicação armazenem o conteúdo de mensagens trocadas por seus usuários. A lei obriga

apenas que seja realizado o armazenamento de dados de registro e acesso às aplicações pelo prazo de 6 meses (Art.15, *caput*). Diante disso, o Whatsapp estaria agindo de forma perfeitamente legal ao não armazenar as informações exigidas no âmbito das investigações.

O **segundo ponto** relaciona-se especificamente ao armazenamento de conversas após ordem judicial específica que obrigue a empresa a fazê-lo. Devido às peculiaridades da criptografia adotada pelo Whatsapp (baseada em um protocolo aberto, o Signal), foi unanimidade entre os especialistas técnicos presentes na audiência pública que, até o presente momento (e assumindo que não ocorreram falhas na implementação da ferramenta), não é possível "quebrar" a criptografia do serviço. Como o Whatsapp não consegue obter as chaves criptográficas, não seria possível sequer "espelhar" conversas em outros dispositivos acessíveis pelas autoridades investigativas. No entanto, é importante destacar que esses mesmos especialistas alegam que é possível que uma vulnerabilidade que permita essa "quebra" possa ser encontrada futuramente.

Frente a este cenário, a solução apontada por alguns expositores (MPF, PF, OAB e AMB) seria uma alteração no sistema do Whatsapp como um todo, de forma a implementar **mecanismos de acesso excepcional** (os chamados *backdoors*) para que autoridades tenham acesso aos conteúdos das conversas quando necessário para investigações criminais.

Sobre a implementação de mecanismos de acesso excepcional para fins de investigação judicial

Caso o Whatsapp alterasse por completo a estrutura de seus serviços, seria sim possível a implementação de um *backdoor* para fins de investigação policial; o debate, neste ponto, transcende a possibilidade técnica de implementação, e passa a tratar das consequências desta implementação para a segurança dos usuários e para o modelo de negócio das empresas de aplicativos.

Os especialistas da comunidade técnica, também de forma unânime, apontaram para diversos **perigos da implementação de** *backdoors* no serviço de comunicação. Uma vez que o *backdoor* é disponibilizado às autoridades, é possível (e provável) que cibercriminosos se apropriem deste mecanismo e tenham acesso aos conteúdos das conversas da totalidade dos usuários do serviço. Ademais, além de comprometerem a segurança de todos os usuários comuns (entendimento destacado também por expositores da área jurídica, como ITS, Internetlab, IDEC, e CTS-FGV) principalmente aqueles não investigados, eventuais mudanças no sistema seriam facilmente identificáveis por investigados versados em tecnologias, o que as tornaria ineficientes.

Do outro lado, a Polícia Federal foi incisiva na **necessidade da implementação destes mecanismos**, insistindo que a persecução criminal no Brasil deve ser ditada pelo Estado e não por empresas de tecnologia. O MPF alegou que não haveria prejuízo (no sentido da perda de usuários) para o modelo de negócio do Whatsapp, uma vez que o aplicativo se popularizou bem antes da implementação da criptografia ponta-a-ponta. Ademais, alegou que este tipo de criptografia inviabiliza por completo as investigações criminais, e que a implementação do backdoor poderia ser realizada de forma segura e controlada. Em um cenário cada vez mais conectado, em que as comunicações são majoritariamente realizadas nestes aplicativos, seria essencial o acesso a essas comunicações para a devida condução da investigação.

Essa alegada dependência do acesso ao conteúdo das conversas pelas autoridades de investigação criminal foi algo bastante questionado por alguns expositores, principalmente aqueles da área técnica. Nesse sentido, foram sugeridas diversas alternativas à imposição de backdoors em sistemas como o do Whatsapp.

Viabilizando a investigação: alternativas aos mecanismos de acesso excepcional

De forma a prezar pela segurança dos dados de usuários e viabilizar a investigação criminal, diversos expositores apresentaram alternativas à imposição de *backdoor* em sistemas criptografados.

No contexto de uma sociedade cada vez mais conectada e adepta à utilização de serviços da internet, uma grande quantidade de informações podem ser extraídas dos chamados **metadados**, que consistem em "informações sobre dados". Nessa categoria se encaixam grande parte dos dados que descrevem outros dados sem evidenciar seu conteúdo. Por exemplo, os dados referentes à data e hora de registro e acesso

às aplicações (cuja guarda é obrigatória pelo MCI), dados referentes à tamanho de imagens, à duração de vídeos etc. Ainda que não signifiquem muito isoladamente, o acesso a grandes quantidades de metadados e a possibilidade de cruzamento desses dados, a inferência e outras técnicas de análise poderiam auxiliar imensamente as investigações criminais se adequadamente manuseadas.

Como exemplo da utilização deste tipo de dado, o Centro de Tecnologia e Sociedade da FGV-Rio apontou que a investigação do assassinato da juíza Patrícia Acioli se utilizou amplamente de imagens de câmeras de segurança e metadados, estes de mais de 3 milhões de celulares que passaram pela área do assassinato, e com a análise destas informações pôde ser concluída com êxito.

Outra alternativa apresentada ao *backdoor* é o chamado *government hacking*. Neste sentido, o próprio governo atua como *hacker*, buscando e explorando vulnerabilidades nos sistemas dos aplicativos investigados, sem o conhecimento destes. A técnica foi (e é) bastante utilizada pelo governo estadunidense.

Embora menos agressiva que a inclusão de *backdoors,* esta modalidade deve ser tratada com cautela, uma vez que se houver o vazamento das vulnerabilidades descobertas, eles ficam suscetíveis ao ataque de hackers antes da possibilidade de seu reparo, conforme apontado pelo IDEC na audiência. O ataque do *ransomware* WannaCry, em maio de 2017, que atingiu diversos órgãos do judiciário brasileiro, só foi possível graças ao vazamento, pela Wikileaks, das vulnerabilidades utilizadas pelo governo dos EUA.

Por fim, uma alternativa menos tecnológica que também foi mencionada na audiência é a própria **infiltração policial** nos grupos de conversa investigados. É uma técnica aparentemente já utilizada neste tipo de investigação.

O que esperar daqui pra frente

Com o término dos dois dias de audiência pública, os julgamentos da ADI 5537 e da ADPF 403 seguem para decisão. O caso é bastante complexo tanto na esfera jurídica quanto técnica, e as decisões do STF afetarão diretamente a segurança das informações de usuários, diversos processos de investigação criminal e até os modelos de negócio de determinados provedores de aplicação.

Carlos Augusto Liguori Filho - Pesquisador do Grupo de Ensino Pesquisa e Inovação da FGV-SP.