

REGULAÇÃO JURÍDICA DA CRIPTOGRAFIA: UMA PERSPECTIVA COMPARADA ENTRE O CASO FBI V APPLE E OS BLOQUEIOS DO WHATSAPP NO BRASIL

Rodrigo Gomes Paixão (IC) e Maria Edelvacy Marinho (Orientador)

Apoio: PIBIC CNPq

RESUMO

O debate segurança versus privacidade é questão controvertida desde o advento da internet. Com as novas dinâmicas de comunicação introduzidas pelos serviços de mensagens, o alcance destas ferramentas foi ampliado. Essas novas dinâmicas também trouxeram consigo uma consequente maior necessidade de aumentar da segurança desses meios, visto o aumento do número de usuários, o que fez com que a criptografia, tecnologia de segurança, passasse a se difundir como alternativa. Isso levou as autoridades investigativas a começar seus primeiros movimentos contrários à criptografia, dado o receio de perder a poder de acesso a dados e informações e parte de sua capacidade de investigação para fins criminais. Com os escândalos oriundos da divulgação de dados da NSA por Edward Snowden, houve uma movimentação reativa do mercado e da comunidade científica. Com isso a criptografia forte se consolidou como o principal método de segurança de dados privados. Isso também intensificou o debate sobre sua regulação judicial e o acesso a dados no contexto de investigações criminais. Tal contexto, de certa forma, é uma constante no debate internacional sobre a regulação da criptografia e guarda uma série de pontos em comum. Há, também, algumas diferenças consideráveis. A partir disso, a presente pesquisa buscou apresentar e traçar as semelhanças e diferenças entre o caso FBI v Apple, que ocorreu nos EUA, e os bloqueios do WhatsApp no Brasil. O ponto comum a estes casos é o fato de a criptografia ter sido um empecilho às investigações estatais nos dois países.

Palavras-chave: Criptografia. Privacidade. Segurança.

ABSTRACT

The security versus privacy debate has been a controversial issue since the advent of the Internet. With the new communication dynamics introduced by messaging services, the reach of these tools has expanded. These new dynamics also brought with them a consequent greater need to increase the security of these means, given the increase in the number of users, which caused encryption, a security technology, to become widespread as an alternative. This led investigative authorities to begin their first moves against encryption,

for fear of losing the power to access data and information and part of their investigative capacity for criminal purposes. With the scandals stemming from Edward Snowden's release of NSA data, there has been a reactive movement from the market and the scientific community. As a result, strong encryption has established itself as the primary method of securing private data. This has also intensified the debate about its judicial regulation and access to data in the context of criminal investigations. This context is, to some extent, a constant feature of the international debate about the regulation of encryption and has several common points. There are also some considerable differences. From this, the present research sought to present and trace the similarities and differences between the FBI v Apple case, which occurred in the USA, and the WhatsApp blockades in Brazil. The common point between these cases is the fact that encryption has been a hindrance to state investigations in both countries.

Keywords: Cryptography. Privacy. Security.

1. INTRODUÇÃO

Em dezembro de 2015, o Departamento Federal de Investigação americano (Federal Bureau of Investigation, no original em inglês – “FBI”) capturou um iPhone 5c de Syed Rizwan Farook, um dos atiradores responsáveis por um ataque terrorista reivindicado pelo Estado Islâmico que matou 14 pessoas e deixou outros 22 feridos em San Bernardino, Califórnia. Durante as investigações, o FBI tentou obter acesso aos dados armazenados naquele telefone, mas não o fez pelo fato de ele estar bloqueado por uma senha numérica, empecilho imposto pelo software de segurança adotado pelo aparelho.

Com isso, iniciou-se uma série de novas medidas, também malsucedidas, para tentar viabilizar o acesso. Esta sequência de fatos desencadeou um intenso debate nos Estados Unidos da América (EUA) sobre o equilíbrio entre a manutenção da segurança nacional e a proteção da privacidade dos utilizadores. No mesmo mês da captura do celular pelo FBI, mais especificamente no dia 16 de dezembro de 2015, foi proferida no Brasil a primeira decisão de bloqueio do aplicativo de conversas WhatsApp que foi efetivamente implementada¹.

Apesar de o processo correr em segredo de justiça, segundo informações da imprensa brasileira, a decisão foi proferida porque o Facebook, controlador do WhatsApp, havia se recusado a obedecer a um requerimento que ordenava a disponibilização de informações e dados a respeito de um homem preso por latrocínio, tráfico de drogas e associação ao Primeiro Comando da Capital (PCC) em 2013. Outras duas decisões de bloqueio aconteceram em maio e julho de 2016, com motivações semelhantes.

As situações ocorridas no Brasil nos EUA estão intimamente conectadas. Além do fato de as intervenções judiciais se darem em virtude da alegada necessidade de acesso a dados como forma de viabilizar investigações criminais, as tecnologias de segurança adotadas pelo WhatsApp e pela Apple são semelhantes: ambas se munem de criptografia para defesa das informações de seus usuários. A criptografia, na realidade, é o ponto chave desse debate.

Ainda, embora seja questão jurídica, tal debate diz respeito à sociedade civil como um todo. A relevância moral e social dada às espécies de crimes cometidos, o caráter tecnológico e atual da questão e a importância da criptografia no dia a dia - por ser uma tecnologia presente em transferências bancárias, e-mails, em aplicativos de mensagens e

¹ Ordenada no dia 16 de dezembro de 2015, esta foi a segunda decisão que determinava o bloqueio do WhatsApp no país, mas a primeira a ser efetivamente cumprida. Em fevereiro de 2015 houve a primeira decisão de bloqueio, determinada pelo juiz Luiz de Moura Correia do Tribunal de Justiça do Piauí, que não foi implementada.

nos próprios smartphones - faz restar claro que a discussão não repousaria apenas sobre o âmbito legal.

Por isso, pretendeu-se averiguar o que os casos revelam sobre o debate entre a liberdade e privacidade (livre iniciativa e o poder dever dos estados) e como os judiciários brasileiro e americano reagiram a isso, buscando semelhanças e diferenças entre os ocorridos. O objetivo foi compreender quais os rumos da regulação da criptografia, guiada pelo Estado e pela sociedade civil, além de entender como os casos estudados reverberaram no meio jurídico nacional e americano.

Dada a importância jurídica do tema quanto aos direitos fundamentais e humanos, buscou-se valorar os fatos – pedidos de acesso excepcional pelas autoridades para fins de investigação e persecução penal e a defesa de tais direitos, como o sigilo das comunicações privadas e a própria liberdade de expressão e comunicação.

Para tal, primeiro foi apresentado o contexto da relação entre criptografia e direito e como aquela ganhou repercussão jurídica para, em seguida, relatar os casos estudados. Estes serão denominados na presente pesquisa como *caso WhatsApp* (conjunto de situações ocorridas no Brasil) e *caso FBI v Apple* (conjunto de situações ocorridas nos EUA). Assim, tais casos foram detalhados para que, posteriormente, fosse possível estabelecer suas semelhanças e diferenças.

Como a regulação judicial da criptografia aconteceu de forma distinta no Brasil e nos EUA, foi necessário realizar uma divisão diferente nos tópicos referentes aos respectivos casos. Mais especificamente quanto ao caso brasileiro, pelo Supremo Tribunal Federal (STF) ter convocado uma Audiência Pública para fins de esclarecimentos quanto à criptografia, o tópico referente ao caso *WhatsApp* tratará tanto da referida audiência como dos votos proferidos pelos ministros da Suprema Corte brasileira.

Como já dito, uma vez apresentados os casos, buscou-se averiguar o que eles nos mostram sobre o conflito entre o direito à liberdade e o poder dever do Estado de assegurar outros direitos fundamentais.

Assim, transitar-se-á entre a regulação judicial da e a regulação jurídica da criptografia para, por fim, responder a seguinte pergunta de pesquisa: “se, e como os casos analisados ditaram as tendências da regulação judicial da criptografia nos Estados Unidos da América e no Brasil?”.

2. DESENVOLVIMENTO DO ARGUMENTO

2.1. Histórico da relação entre a Criptografia e o Direito

Para compreender com maior propriedade os porquês das repercussões no Brasil e nos Estados Unidos dos casos tratados e a relação entre a criptografia e o Direito, é preciso, primeiramente, entender o que é a criptografia em si e, em seguida, esmiuçar um pouco o debate da segurança v. privacidade.

Criptografia nada mais é que uma tecnologia de segurança usada com o fim de cifrar (codificar) dados, tornando-os ininteligíveis² para os que não detêm a chave capaz de decifrá-los (PAIXAO, 2020, p.11).

Para Iphones, por exemplo, quaisquer usuários que não saibam a senha do dispositivo celular não são capazes de acessar seu conteúdo interno. Quanto ao WhatsApp, por sua vez, terceiros não partes de uma conversa privada ou em grupo são incapazes de saber o conteúdo das mensagens. Disto, já se nota inicialmente que, apesar de ambos se munirem da criptografia, as espécies dessa tecnologia adotadas pelo WhatsApp e pelo Iphone são distintas.

Uma vez definido o que é criptografia, parte-se ao debate segurança v. privacidade. Nos Estados Unidos, ele surgiu na década de 1990 com as denominadas “CryptoWars”. Essas “Guerras Criptográficas” foram assim nomeadas por conta dos conflitos existentes entre os defensores da privacidade e o governo americano, especialmente a NSA.

Isto aconteceu em um período em que a internet começou a se estabelecer como principal meio de comunicação (LIGUORI FILHO, 2018, p. 3). Com os progressos técnicos, o uso da criptografia também se difundiu e se popularizou por se mostrar uma forma eficiente de se proteger de ataques maliciosos de hackers.

Já nesse primeiro momento, houve uma primeira reação legal ao uso da criptografia, estabelecendo, portanto, suas primeiras relações com o direito. O governo americano reagiu ao uso da tecnologia tentando controlar sua difusão no país. Houve uma primeira tentativa por meio da implementação de um sistema de depósito de chaves chamado “Chip Clipper”, que viabilizava às entidades responsáveis pela aplicação da lei e aos agentes de segurança nacional o poder de acessar comunicações de texto simples. (SWIRE; AHMAD, 2012, p. 435).

Tal tentativa fracassou, entretanto, pois foi, já à época, muito criticada pela comunidade científica não só por supostas falhas de caráter técnico (LIGUORI FILHO, 2018, p.7), mas também porque o governo americano manteve em sigilo o algoritmo usado no Chip Clipper, o que gerou grande desconfiança.

² Algo impossível de ser compreendido ou de difícil compreensão.

Além disso, houve reação regulatória pelos EUA, visando diminuir também a exportação da criptografia, como forma de assegurar ao estado americano certo monopólio. Tais regulações, inicialmente, visavam dificultar sua venda e controlar os usos da tecnologia para fins não militares (DIFFIE; LANDAU, 2005). Apesar desses esforços, a criptografia continuou a se popularizar, principalmente para o uso de particulares³.

Pode-se dizer, entretanto, que quando foram divulgados documentos por Edward Snowden, ex-funcionário da Agência Nacional de Segurança americana (LIGUORI FILHO, 2018, p. 10)⁴, os debates sobre a violação de dados e da privacidade dos usuários em toda a comunidade internacional teve um de seus auge em relevância.

Com isso, houve o questionamento de que se as plataformas têm acesso aos dados dos usuários, elas são inseguras para comunicações privadas. A reação do mercado a esse sentimento de insegurança foi a chamada criptografia *by default* (criptografia por padrão), criptografia forte que visava conferir maior poder aos sistemas de proteção de dados dos usuários (LIGUORI FILHO, 2018, pág. 2).

A partir desse momento, diversas aplicações passaram a sair de fábrica já programadas para usar tal criptografia forte. Essas novas modalidades não só tornavam ininteligível determinado conteúdo, mas sequer permitiam que a própria empresa obtivesse acesso as informações dos usuários. Ou seja, para alcançar a segurança de seus consumidores, as próprias empresas renunciaram à capacidade de deter acesso aos dados privados deles.

Como o exemplo, a criptografia de ponta a ponta usada pelo WhatsApp, que deixa as mensagens indecifráveis durante todo o percurso da conversa. A segurança tecnológica passou a ser um produto tão desejado que outras “gigantes” como o Google, a Apple e implementaram o uso da criptografia com esse fim, o que também ajudou a ditar uma tendência, dada a credibilidade e confiança que paira sobre estas empresas⁵. O custo da

³ Antes, a tecnologia era classificada como de uso ou militar, ou civil, o que perdeu o sentido com a popularização (SWIRE; AHMAD, 2012, p. 435). A partir desse momento, apesar de inúmeros sistemas passarem a usar a criptografia (e-mails, sites, aplicativos), o público comum não tinha ciência proativa disso. Melhor explicando, os usuários usavam a criptografia – ou sistemas que detinham tal tecnologia - não por se sentirem mais seguros ou por julgarem que aquela era a melhor forma de se proteger, mas porque os sistemas que eles usavam se muniam da tecnologia, tendo eles ciência disso ou não.

⁴ Nestes, Snowden revelou quão grande era a capacidade de vigilância do governo estadunidense, informando que ele pirateava empresas de telefonia chinesas para recolher mensagens de texto e que espionava escritórios diplomáticos de outros países, obtendo acesso a e-mails e documentos internos, por exemplo. Além disso, havia indícios de que um dos alvos da espionagem era Dilma Rousseff, presidente do Brasil à época, o que efervesceu a questão no país.

⁵ A Apple, fabricante do Iphone foi vanguardista, atualizando o sistema operacional de seus dispositivos, o IOS, para adotar a criptografia como sua configuração padrão, de forma que o usuário não precisasse ser proativo em sua ativação, ou seja, ela seria usada independente da vontade dele. O WhatsApp, por sua vez, passou a adotar a chamada criptografia de ponta-a-ponta. Nela, a mensagem é codificada em sua origem, ou seja, quando é enviada pelo emissor. Ela, por sua vez, só será decifrada no destino, quando o receptor a recebe, de forma que apenas as “pontas” da conversa têm acesso ao conteúdo decifrado

segurança como norte, porém, como dito, foi a renúncia à própria capacidade de interceptação de dados de seus clientes.

Tais fatos também amplificaram também a disseminação e a defesa do uso da criptografia entre os usuários comuns, indivíduos que se viam preocupados com as possibilidades de terem seus dados sequestrados. Assim, a tendência após Snowden rumou em direção à criptografia muito em virtude da privacidade do consumidor (RYDER, 2016, pág. 904), mas também como uma forma das próprias empresas de tecnologia se defenderem.

Isso desencadeou uma nova questão na relação entre a criptografia e o direito. A renúncia à capacidade técnica de obter dados dos seus clientes resultou também na incapacidade de cumprir com ordens judiciais que reivindicavam tais dados para investigações.

Ou seja, mesmo que a empresa quisesse colaborar, ela não seria capaz de entregar esses dados para agências de vigilância, segurança e espionagem. Estas requeridas maior segurança e privacidade - que conferiram também maior proteção de direitos fundamentais – acabaram por dificultar as investigações e, conseqüentemente, violar outros direitos fundamentais segundo os órgãos de persecução penal.

Esta situação foi chamada de *Going Dark* – expressão popularizada numa palestra dada pelo diretor do FBI James Comey em que ele reclamava de as autoridades de segurança ficarem no “escuro” por não conseguirem o acesso a informações para investigação criminal (LIGUORI FILHO, 2020, p. 9). Ele começou, ali, a defender a fragilização dessas criptografias por meio de *backdoors* e acessos excepcionais, formas que viabilizassem o que os dados fossem obtidos.

O caráter absoluto dessas tecnologias de segurança passou a ser questionado, dada a necessidade de perseguir o bem comum e assegurar que alguns direitos não sejam violados em nome de outros. Além disso, houve grande preocupação dos órgãos de investigação com a perda do seu poder de acesso à informação e investigação e os entes particulares. Esse contexto é pano de fundo do acontecido no Brasil e nos Estados Unidos da América. Os conflitos entre viabilizar investigações criminais e ao mesmo tempo garantir a segurança as informações dos usuários deu base aos ocorridos.

2.2. Caso FBI v Apple

Como descrito, em 2015, o FBI capturou o iPhone de um dos atiradores responsáveis por um ataque terrorista em San Bernardino, mas não conseguiu interceptar os dados ali presentes. O Departamento de Investigação Americano requisitou auxílio da Apple e, com a recusa, pleiteou uma ordem judicial para obrigá-la a fazê-lo.

Ao solicitar a ordem, o governo americano trouxe um memorando com algumas informações, dentre as quais a de que a Apple havia codificado seus sistemas com uma função *auto-erase*. Dessa forma, o dispositivo celular, que estava protegido (“bloqueado”) com a senha numérica determinada pelo usuário, teria seu conteúdo permanentemente destruído caso ocorressem 10 tentativas erradas de introdução da senha.

Por isto, o uso de ataques de força bruta⁶, por exemplo, seria inviável e o FBI não conseguiria fazer tentativas para determinar a senha. Dessa forma, a ajuda da Apple se tornara fundamental. O pedido acatado pela Corte Americana, entretanto, foi ineficiente. A Apple se recusou a obedecê-lo e Timothy Cook, Diretor Executivo, (ou, do inglês, Chief Executive Officer CEO) da empresa de tecnologia, afirmou em carta aberta que não obedeceria a ordem. Para se justificar, Cook afirmou que as implicações daquela ordem iam muito além das questões jurídicas, tendo repercussão para a sociedade atual como um todo.

Ele ressaltou a importância da criptografia para os smartphones e concluiu que ela reverbera de forma tão impactante no meio social que acatar a ordem significaria comprometer a segurança das informações dos usuários e inclusive colocar em risco, inclusive, sua segurança pessoal⁷.

O FBI, em contrapartida, primeiro afirmou que a Apple era, sim, capaz de modificar seu sistema (*autoerase*) para apenas um dispositivo e que, ao não o fazê-lo, ela contribuía para que o processo demorasse demasiado tempo para permitir o acesso ordenado pelo tribunal. Isso seria um problema dado o imediatismo que algumas investigações demandam.

Para além do apresentado o debate perpassou fundamentalmente pelo “All Writs Act” (AWA), Estatuto federal dos EUA que assegura que os tribunais americanos possam emitir quaisquer mandados necessários para que seja alcançado o fim racional de direito de acordo com os usos e princípios da lei.

A partir desse estatuto, o FBI argumentou, primeiramente, quanto a proximidade da Apple com o tema da interceptação de dados e quanto a ausência de onerosidade excessiva à Apple em caso de cumprimento da ordem - a Suprema Corte americana já havia decidido que tal regra não poderia ser usada quando o terceiro obrigado tiver como consequência um ônus desproporcional⁸, que é o argumentado pela maioria da comunidade científica, dados os riscos apresentados.

⁶ Ataques de força bruta são espécies de *hacking* (meios de burlar a segurança de um sistema) por meio de sucessivas tentativas até que se acerte a senha (chave), e, assim, conseguir as informações e dados desejados.

⁷ Leia na íntegra em: <https://www.apple.com/customer-letter/>

⁸ Disponível em: <https://www.theguardian.com/technology/2016/feb/24/apple-v-the-fbi-why-1789-all-writs-act-is-the-wrong-tool>

Porém, o argumento mais relevante à presente pesquisa foi quanto à essencialidade do auxílio da Apple para que o mandado fosse cumprido. O FBI trouxe que nenhum outro teria a capacidade de ajudar o governo a impedir que o mandado seja obstruído que não ela, uma vez que ela não só é a criadora do design do software, mas é sua única detentora e vendedora.

Além disso, contrapondo o exposto por Tim Cook em sua manifestação pública, o FBI alegou que viabilizar o acesso nesse específico caso não daria ao governo o poder de acessar os aparelhos de qualquer um sem que houvesse um mandado ou autorização judicial. Pelo contrário, a ordem permitiria, inclusive, que a Apple se mantivesse em custódia do software ao longo de todo o procedimento.

Tem-se, então, o panorama do caso *FBI v Apple*. Houve um embate público e judicial entre a empresa de tecnologia e as autoridades investigativas, o que também aconteceu no caso WhatsApp como veremos a seguir. Com a descrição desse caso, traçaremos os pontos distintos e em comum para estabelecer relações entre ambos.

2.3. Caso WhatsApp

Como dito, a primeira decisão de bloqueio do aplicativo de conversas WhatsApp que foi efetivamente implementada⁹ ocorreu no mesmo mês da captura do Iphone pelo FBI no caso americano. A juíza Sandra Regina Nostre da 1ª Vara Criminal de São Bernardo do Campo¹⁰ determinou o bloqueio do aplicativo em todo o Brasil como punição pelo descumprimento de ordens judiciais que exigiam a cessão de dados de um usuário.

O referido processo corre em segredo de justiça, mas, de acordo com informações da imprensa brasileira, o bloqueio do WhatsApp se deu porque o Facebook se recusou a obedecer a um requerimento da Justiça que ordenava a disponibilização de informações e dados a respeito de um homem preso por latrocínio, tráfico de drogas e associação ao Primeiro Comando da Capital (PCC) em 2013.

Em maio do ano seguinte (2016), houve novo bloqueio do WhatsApp em todo o país, também resultado do descumprimento de ordens de interceptação da dados. Dessa vez os alvos da investigação foram 36 usuários que estavam supostamente envolvidos em uma organização criminosa que patrocinava o tráfico interestadual de drogas.

⁹ Ordenada no dia 16 de dezembro de 2015, esta foi a segunda decisão que determinava o bloqueio do WhatsApp no país, mas a primeira a ser efetivamente cumprida. Em fevereiro de 2015 houve a primeira decisão de bloqueio, determinada pelo juiz Luiz de Moura Correia do Tribunal de Justiça do Piauí, que não foi implementada.

¹⁰ Cabe comentário sobre uma curiosa coincidência. O atentado terrorista e a questão do primeiro bloqueio do WhatsApp no Brasil, para além das apenas duas semanas de diferença, guardam semelhança quanto aos nomes dos locais em que os fatos aconteceram: São Bernardo (do Campo) e São Bernardino (EUA).

Estas foram duas das três primeiras decisões de bloqueio que afetaram o aplicativo de mensagens sendo as duas primeiras a efetivamente serem executadas (PAIXÃO, 2020, p. 8). Cabe ressaltar que alguns meses depois desses eventos, em julho de 2016, a juíza Daniela Barbosa Assumpção de Souza da 2ª Vara Criminal de Duque de Caxias, Rio de Janeiro, determinou a quarta decisão de bloqueio contra o WhatsApp e a terceira a ser implementada com sucesso.

O debate, inicialmente, repousou sobre uma suposta inviabilidade técnica de se conseguir acesso às mensagens. Nas primeiras instâncias, o WhatsApp respondeu às ordens de bloqueio ora mencionadas afirmando não ser possível o acesso às mensagens por conta da tecnologia adotada pelo aplicativo, a criptografia de ponta a ponta.

O caso foi levado à Suprema Corte por meio da Arguição de Descumprimento de Preceito Fundamental (ADPF) 403 e da Ação Direta de Inconstitucionalidade (ADI) 5527 para que se debatesse questões de constitucionalidade. No âmbito dessas ações, o Supremo convocou a Audiência Pública nº 21 com o objetivo de responder alguns questionamentos técnicos sobre a criptografia, como será visto a seguir.

2.3.1. Audiência Pública nº 21

Em 27 de outubro de 2016 o Ministro Edson Fachin junto da ministra Rosa Weber convocou audiência pública nº 21 no âmbito da ADPF 403 e da ADPF 403, com o objetivo de discutir aspectos técnicos da suspensão do WhatsApp por decisões judiciais no Brasil. Dessa forma, foram selecionados dentre os 182 pedidos de participação, 23 especialistas para participar dos debates.

Conforme expresso nos arts. 13, XVII, e 21, XVII, do Regimento Interno do STF, as audiências públicas tem como fim ouvir o depoimento de pessoas com experiência e autoridade em determinada matéria. Como dito, os casos possuem além da relevância jurídica, repercussão social. Dessa forma, viabilizar a participação popular em um caso de interesse público e introduzi-la ao debate de maneira formal relevante se fez necessário,

Para que esclarecimentos técnicos no que concerne à criptografia fossem prestados, os Ministros estabeleceram perguntas norte¹¹. Assim, professores universitários, cientistas,

¹¹ As perguntas foram: 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)? 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?

procuradores, juízes e outros especialistas, tanto favoráveis como contrários à questão do acesso excepcional, bem como interessados na questão da criptografia se manifestaram – destaque-se, Brian Acton, um dos fundadores do WhatsApp.

A partir das apresentações, algumas possibilidades de obter tais dados foram apresentadas. O argumento levantado nas primeiras instâncias sobre a impossibilidade técnica foi questionado pelas autoridades investigativas também na audiência. Assim, apresentaram alternativas para a implementação dos acessos excepcionais, dentre as quais, as mais frequentes foram o uso de *backdoors* e o ataque *man-in-the-middle*.

Explicando melhor, e diferenciando os dois conceitos, o ataque *man-in-the-middle* seria, literalmente, colocar um “homem” no meio da conversa, entre o emissor e o destinatário. De forma mais técnica, seria colocar um passo a mais no processo de troca de mensagens, de forma que entre seu envio e seu recebimento, ela poderia ser acessada por um intermediário. Assim, quando um indivíduo enviase sua mensagem, antes de chegar ao receptor, ela seria acessada por um intermediário que acompanharia a comunicação.

Os *backdoors*, por sua vez, seriam uma espécie de entrada secreta cujo acesso só seria possível pelas autoridades governamentais. Para isso, seria necessário estabelecer uma falha na criptografia que viabilizasse o uso de uma “chave-mestra”, ou programar uma intervenção que viabilizasse que eventuais mensagens fossem interceptadas antes de serem cifradas (ou logo após serem decifradas).

Thiago Guimarães, representante da Universidade de Brasília na Audiência Pública nº 21 expôs que o intermediário se passaria como “dois interlocutores, de forma a poder optar apenas acompanhar a comunicação dos usuários, passando-se por eles, replicando as mensagens, de forma a continuar invisível”.

As possibilidades apresentadas não foram tidas como inviáveis por si só, mas alguns participantes expuseram pontos prejudiciais em aplicá-las. Brian Acton, por exemplo, disse que seria, sim, possível o uso do referido ataque *man-in-the-middle*, porém com alguns empecilhos. Um deles seria que, em virtude do sistema de verificação do código de segurança usado pelo aplicativo, a interceptação seria facilmente detectável, pois o usuário seria notificado do ocorrido, bastando apenas que ele conferisse as chaves.

Usuários comuns não se preocupariam com isso, provavelmente, mas isso pode não valer para usuários criminosos. Acton expôs ainda que quanto maior o número de conversas, maior a chance de a notificação acontecer: “se nós tivermos cinquenta conversas, a chance de uma dessas conversas ligar essa notificação aumenta muito”. Em conversas de grupos, então, a interceptação seria facilmente perceptível. Acton trouxe que com o maior o número de conversas, a chance de a notificação aumenta o que,

consequentemente, aumenta a possibilidade de descoberta.

Apesar do afirmado, foi um argumento frequente entre os defensores de tais acessos a possibilidade de construir um *backdoor* apenas para o WhatsApp dos celulares dos investigados, por ser considerada uma medida mais simples e efetiva.

Isto porque, segundo eles, ela não violaria os direitos de todos os usuários, mas apenas serviria para que a investigação prosseguisse. O indivíduo suspeito teria sua conta violada e seria investigado sem que quaisquer danos a terceiros ocorressem. Assim, em situações como as descritas – investigados por atentados terroristas, tráfico de drogas e pornografia infantil - a investigação seria possível sem que eles soubessem do feito ou que tivessem seus dispositivos apreendidos fisicamente.

Isto, por sua vez, seria extremamente positivo dado o caráter imediato que tais casos exigem - esperar a apreensão do dispositivo físico poderia fazer com que muitas das informações cruciais para a investigação fossem perdidas, ou que não fossem acessadas a tempo, o que poderia tornar seus danos irreparáveis.

O Delegado Felipe Alcântara trouxe nova questão ao alegar que a apreensão de um celular em detrimento da interceptação de dados imediata pode ser um obstáculo a uma das principais ferramentas investigativas, que é a ação controlada, espécie de flagrante postergado, na qual se espera o momento mais adequado para a prisão. Ou seja, ao longo da investigação haveria a interceptação e, por meio dela, a possibilidade de flagrante, que seria feita no melhor momento para que maiores provas fossem obtidas.

Este flagrante, intencionalmente postergado, acabaria sendo retardado ou até mesmo inviabilizado com o fato de as autoridades investigativas não terem a prerrogativa de, em momento oportuno, acessar as informações requeridas.

Outros pontos foram levantados na audiência pública, mas estes foram os que mais guardaram relação com os trazidos no caso *FBI v Apple*, como veremos a seguir, sendo, portanto, mais relevantes para a presente pesquisa. Tanto os argumentos favoráveis e contrários aos acessos excepcionais foram ouvidos pelos ministros da Suprema Corte brasileira e considerados antes que estes proferissem seus votos. De tal forma, passaremos à análise dos votos.

2.3.2. Votos dos Ministros do Supremo Tribunal Federal

O Supremo, apesar de passados cinco anos da propositura da ação, ainda não terminou seu julgamento – os Relatores da ADI 5527 e da ADPF 403, respectivamente, a ministra Rosa Weber e o ministro Edson Fachin, proferiram seus votos. Já o ministro

Alexandre de Moraes, que votaria a seguir, pediu vista do processo no dia 28 de maio de 2020.

Em pesquisa elaborada por mim em 2020, tracei as relações estabelecidas entre os votos e os argumentos dos expositores. De tal forma, neste tópico será restrito ao apontamento dos principais argumentos dos ministros.

2.3.2.1. Ministra Rosa Weber

A ministra argumentou principalmente que a redução da segurança contraporaria a defesa de direitos fundamentais como a proteção da liberdade de expressão e sigilo das informações. Numa perspectiva mais jurídica, a ministra traz que a Constituição deve ser fluida, acompanhando os avanços da tecnologia ao questionar qual seria o sentido de uma Constituição que protege o sigilo das comunicações telegráficas, mas não o de comunicações realizadas por aplicações de internet ou qualquer outro meio.

Ao defender a criptografia, ela faz menção a outro valor constitucional pétreo, afirmando que tal tecnologia merece proteção por permitir que indivíduos exerçam seus direitos de liberdade de opinião e expressão na área digital.

Assim, Weber conclui seu argumento sobre a questão da criptografia afirmando que ela o acesso do Estado ao conteúdo das comunicações é uma exceção à regra que é a proteção do sigilo das comunicações, iniciando, assim, os rumos iniciais da regulação judicial da criptografia no Brasil

2.3.2.2. Ministro Edson Fachin

O ministro Edson Fachin, por sua vez, seguiu, de forma geral, o entendimento de Weber e da comunidade científica. Ele afirmou ser contraditório enfraquecer a segurança da internet em nome da segurança pública, pois o risco causado pelo uso da criptografia de ponta a ponta não compensa as potenciais consequências da implementação do acesso excepcional.

Disso, chegou a três conclusões que corroboravam ser inconstitucional proibir as pessoas de utilizarem a criptografia ponta-a-ponta, pois isso impactaria desproporcionalmente os mais vulneráveis, com menores possibilidades de ter sua segurança e privacidade garantidas.

Na primeira, ele trouxe a liberdade de expressão como um dos direitos defendido pela criptografia. Assim, afirmou que ela atua para assegurar a proteção necessária à tal direito fundamental numa sociedade democrática. Na segunda conclusão, ele traz que não só a sociedade civil, mas todos os órgãos do Estado reconhecem que a criptografia garante a privacidade de suas comunicações no meio digital (PAIXÃO, 2020, p. 58).

Dessa forma, ele argumentou que deve haver uma colaboração mútua desses grupos com fins de alcançar um ambiente digital seguro. Por fim, ele conclui que, apesar das dificuldades técnicas advindas do uso da criptografia para a apuração de crimes, os órgãos de investigação devem depender da autorização do próprio usuário do serviço (PAIXÃO, 2020, p. 59).

Como dito inicialmente, apenas os ministros relatores julgaram a questão da criptografia, de forma que este entendimento, apesar de sugerir uma tendência, não é ainda o consolidado no país. Temos, portanto, um início de regulação judicial da criptografia, apesar de não termos ainda uma regulação jurídica por não haver disposições legais que explicitamente tratem da tecnologia¹².

2.4. Semelhanças e Diferenças entre os casos

Uma vez levantadas algumas das peculiaridades dos casos, é interessante traçar semelhanças e diferenças entre eles. Isto porque o fato de terem acontecido em contextos e momentos distintos com motivações diferentes faz com que a forma de regular a criptografia em cada país seja também possa diferir.

O fim do debate é a regulação em si, mas antes disso, os debates e argumentos são os pontos base para que o caminho até esse fim seja traçado. E um dos panos de fundo comuns aos casos é que, como visto, desde o início, os sistemas de segurança enfrentaram oposições.

Não só hackers e agentes maliciosos, mas sofreram também represálias das autoridades estatais. O Estado, na qualidade de ente cujo fundamento é ser garantidor de direitos, argumentou majoritariamente contra o caráter absoluto dessas tecnologias de segurança, dada a necessidade de perseguir o bem comum e assegurar que alguns direitos não sejam violados em nome de outros.

Ou seja, a preocupação em 1990, nos Estados Unidos era, de certa forma e nas duas perspectivas (estatal e privada) a mesma que havia internacionalmente em 2014 e em 2017¹³ no Brasil. O Estado tradicionalmente preocupado com a perda do seu poder de acesso à informação e investigação e os entes particulares preocupados com a garantia da segurança e privacidade.

Entretanto, tanto o FBI como a maioria dos expositores favoráveis na Audiência Pública nº 21 do STF, fizeram questão de deixar claro que não requeriam que fosse criado ou providenciado um “*backdoor*” para todos os dispositivos, mas apenas para os

¹² Apesar disso, alguns projetos de lei foram apresentados, mas não avançaram com a tramitação. São eles o Projeto de Lei do Senado nº 330, de 13 de agosto de 2013, o Projeto de Lei nº 4060, de 13 de junho de 2012 e o projeto de lei nº 5276, de 13 de maio de 2016.

¹³ Ano em que aconteceu a Audiência Pública nº 21

investigados.

Ainda assim, foi levantado pelo procurador de Justiça Vladimir Aras, Representante do Ministério Público a necessidade de se alterar o design de aplicativos que se munem da criptografia para que fosse possível o acesso em casos de “absoluta necessidade diante critérios de proporcionalidade adequadas”. E essa linha argumentativa é comum não só nos casos analisados.

Como exemplo, em declaração conjunta da Europol¹⁴ e da Enisa¹⁵, foi dito que em casos de crimes graves, os órgãos de aplicação da lei deveriam ter respaldo legal para violar os mecanismos de segurança de dados, de forma que a legislação deve estipular de forma expressa as condições para que isso ocorra coletiva (Europol and Enisa, pág. 1, 2016). Eles também afirmaram que os direitos de um indivíduo precisam ser avaliados com cuidado quando comparados com os de outro.

Isso se mostra afim ao trazido por Aras, apesar de mais explícito, e sobre a ausência de um direito absoluto quando comparado a outro. O argumento, neste caso, foi o da proporcionalidade entre o caráter intrusivo da medida investigativa e o crime cometido – crimes mais graves demandariam medidas mais invasivas para que os objetivos de persecução sejam atingidos.

Um contraponto a tais argumentos foi levantado por Tim Cook, em sua carta aberta, quando afirmou que esse argumento ignora o básico da segurança digital. Segundo o CEO, ao descobrir como contornar a criptografia de um dispositivo, o detentor desse conhecimento pode contornar a defesa de qualquer outro.

Dessa forma, não haveria como estabelecer um *backdoor* exclusivo à um dispositivo sem que muitos outros fossem violados. Cook disse que o pedido do governo era semelhante a minar décadas de avanços da segurança obrigando os desenvolvedores do software do celular a enfraquecê-lo, uma vez que um dispositivo que não tenha acessos excepcionais é fundamentalmente mais seguro que um que o tenha.

Da mesma forma, foi dito na referida Audiência Pública que violar a conta de um único usuário do WhatsApp seria inviável. Além disso, inserir uma “falha intencional de projeto num protocolo criptográfico”, como dito por Diogo Aranha, professor da Unicamp, seria um retrocesso para fins de segurança.

Uma vez que os desenvolvedores se obrigam a colocar uma falha na tecnologia, ele automaticamente se torna mais frágil. Além disso, ao estabelecer uma variável fixa nos

¹⁴ Serviço Europeu de Polícia responsável pelo tratamento e intercâmbio de informações criminais

¹⁵ Agência Europeia para a Segurança das Redes e da Informação que busca elevar os níveis de segurança nas redes de informação

sistemas criptográficos (imaginemos que todos os softwares de criptografia obrigatoriamente devam ter um acesso excepcional), o próprio desenvolvimento do software ficaria mais complicado e, portanto, teria maiores chances de ser vulnerável.

Esse entendimento foi apresentado como consenso na comunidade científica tanto internacional¹⁶ como presente na audiência: a introdução de *backdoors* é um retrocesso em questão de segurança digital. Eles argumentam que o enfraquecimento obrigatório da criptografia pode ser extremamente prejudicial ao exercício dos direitos fundamentais e da liberdade civil.

Isso também foi dito por Cook em sua carta aberta e foi argumento presente nos votos dos ministros relatores do Supremo Tribunal Federal na ADPF 403 e na ADI 5527. A ministra Rosa Weber, por exemplo, afirmou ser um “inadmissível contrassenso, e mesmo retrocesso [...] limitar dessa maneira o uso de criptografia”. Fachin, por sua vez, como já visto, afirmou que a criptografia atua para assegurar a proteção necessária a direitos essenciais para o Estado Democrático de Direito.

As situações revelam que o debate entre a livre iniciativa e o poder dever dos Estados se caracterizaram mais por serem conflituosos que por buscarem um meio termo. Tanto no caso americano como no brasileiro, houve esse debate e os argumentos levantados, em regra, traziam um caráter de conflito.

Não houve cessões pelas partes, de forma que os órgãos de investigação e persecução penal não renunciaram à possibilidade de não haver acessos excepcionais. Da mesma forma, os contrários a tais acessos traziam que apesar de ser possível, tal possibilidade seria inviável dados as inúmeras consequências que, segundo eles, seriam mais prejudiciais que favoráveis.

Como já dito, a questão da criptografia levanta muitos pontos, seja no âmbito tecnológico, seja no jurídico e no social. Assim, o debate é rico em informações e detalhes, mas também em discordâncias. Por isso que a regulação da criptografia se mostra tão delicada e importante.

3. CONSIDERAÇÕES FINAIS

Apesar das comparações entre o caso *FBI v Apple* e o caso *WhatsApp*, as ações no caso brasileiro ainda não foram julgadas. Diferentemente do dos EUA, em que o caso acabou por perder sua razão pelo fato de o FBI ter conseguido desbloquear o dispositivo

¹⁶ Disponível em: <https://itsrio.org/wp-content/uploads/2018/10/KEYS-UNDER-DOORMATS-1.pdf>

sem a ajuda da Apple, não há como falar em uma pronta regulação da criptografia no Brasil, mas apenas em tendências.

Isso porque apenas os ministros relatores votaram. A tendência ditada foi no sentido contrário aos bloqueios e a favor da manutenção da criptografia forte. Apesar de os ministros não terem votado, não é possível dizer que esses votos não tiveram impacto. Em 2021, a terceira seção do Superior Tribunal de Justiça (STJ) decidiu que uma empresa não pode receber multa por entregar informações se ela alega que usa de criptografia forte¹⁷.

O importante dessa decisão é que ela reconheceu algumas informações que foram pautadas no STF e que são muito pautadas no debate internacional: reconheceu que o argumento de que é impossível tecnicamente quebrar o sigilo em caso de uso de criptografia forte é um argumento válido, a criptografia tem benefícios que superam prejuízos e que ela protege direitos fundamentais como a privacidade, segurança e liberdade de expressão.

Para além disso, foi possível notar que os argumentos principais dos casos são muito semelhantes, tanto como seus pontos contrários. Entretanto, foi pouco levantado em ambos as demais possibilidades de acesso às informações investigadas que não enfraquecessem a criptografia forte. As situações estiveram envoltas de um caráter conflituoso, de forma que não houve muitos indícios da busca de um meio termo entre as partes.

No Brasil, a relação da criptografia com o direito se estabeleceu também com a contestação do caráter absoluto dos direitos fundamentais à privacidade, ao sigilo das comunicações privadas e à liberdade de expressão e comunicação, expressos respectivamente no art. 5º, incisos X, XII, e IX da Constituição Federal Brasileira.

Estes foram levantados de forma mais aprofundada com os votos dos ministros relatores do STF, sendo parte importante do debate no âmbito jurídico. Tais direitos, quando violados, o são por baixo dos panos, de forma que essas violações muitas vezes só são descobertas quando os danos são irreversíveis. Cite-se o caso de Snowden.

O desejo de preservar o sigilo e a integridade dos dados não é recente, mas para que sejam assegurados, é necessário o correto funcionamento das tecnologias que se munem daqueles dados. Com as constantes evoluções digitais e a consolidação de uma sociedade da informação, o dia a dia dos indivíduos está cada vez mais entrelaçado aos adventos das revoluções tecnológicas e, por consequência, mais informações são tanto necessárias para abastecer softwares distintos, como usadas em situações que não eram antes o que, portanto, demanda maior proteção.

Para tal, inúmeras tecnologias que visam proporcionar a segurança requisitada à

¹⁷ Disponível em: <https://www.stj.jus.br/sites/porta/p/Paginas/Comunicacao/Noticias/30122020-Terceira-Secao-afasta-multa-contra-empresa-que-alega-impossibilidade-de-interceptar-mensagens-criptografadas.aspx>

efetivação daqueles direitos, viabilizando serviços, comunicações e outros processos, vêm sendo implementadas - dentre elas, destacamos na presente pesquisa a criptografia.

Suas finalidades são legítimas e necessárias, porém explicitamos no artigo o ônus que carregam. Atividades criminosas têm, muitas vezes, sua investigação dificultada por conta desses meios de segurança o que traz o paradigma: em nome dos direitos humanos e fundamentais protegidos por estas tecnologias, vale violar outros? Nos encontramos, então, diante de um caso de sopesamento. Daí a relevância maior desse debate.

Da mesma forma que a privacidade, a liberdade de expressão e outros direitos fundamentais precisam ser protegidos, outros direitos precisam igualmente. A reflexão sobre como viabilizar a aplicação da lei para que crimes como os trazidos nos casos WhatsApp e FBI v Apple sejam devidamente investigados, sem que, entretanto, cláusulas pétreas sejam desrespeitadas é complicado, mas imprescindível.

Assim, do apresentado, fez-se claro que tanto as manifestações do FBI e das partes relacionadas ao processo americano como as dos expositores da Audiência Pública nº 21 e os ulteriores votos dos ministros relatores da ADI 5527 e da ADPF 403 ditaram as tendências da regulação judicial da criptografia nos Estados Unidos da América e no Brasil respectivamente.

Apesar de suas distinções, algumas semelhanças nas formas de regulação foram encontradas, o que mostra que esse debate não é restrito ao local onde ele ocorre, tendo pontos em comum independente do contexto social e localidade, mas que deve ser considerado também com suas peculiaridades.

4. REFERÊNCIAS

ABELSON, Harold; ANDERSON, Ross. et al. **Keys under doormats: 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), 2018. <http://dx.doi.org/10.1093/cybsec/tyv009>. Disponível em: <<https://itsrio.org/wp-content/uploads/2018/10/KEYS-UNDER-DOORMATS-1.pdf>> Acesso em: 7 mar. 2020.

Concerning an Order Requiring Apple to Create Custom Software to Assist the FBI in Hacking a Seized iPhone. EPIC.org, 2020. Disponível em: <<https://epic.org/amicus/crypto/apple>>. Acesso em: 30 de Agosto de 2020.

DIFFIE, Whitfield; LANDAU, Susan. **The Export of Cryptography in the 20th Century and the 21st**. Palo Alto, 2005. Disponível em: <https://privacyink.org/pdf/export_control.pdf> Acesso em: 7 nov. 2020.

FERRAZ JUNIOR, 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. Disponível em: <http://www.revistas.usp.br/rfdusp/article/view/67231>. Acesso em: 02 abr. 2020.

LIGUORI FILHO, Carlos Augusto, Exploring Lawful Hacking as a Possible Answer to the 'Going Dark' Debate (May 8, 2020). Michigan Telecommunications and Technology Law Review, Vol. 26, No. 2, 2020, Available at SSRN: <https://ssrn.com/abstract=3606601>. Access in: April 04, 2020.

LIGUORI FILHO, Carlos Augusto. **O Zap e a Toga: Mapeamento do debate sobre bloqueio de aplicativos e criptografia no STF.** Jota, 2017. Disponível em: <https://goo.gl/TSxVkW>. Acesso em: 20 abr. 2018.

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. 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>. Disponível em: <https://revistas.ufpr.br/direito/article/view/59422>. Acesso em: 30 mar. 2021

PELL, Stephanie K. **You Can't Always Get What You Want:** How Will Law Enforcement Get What It Needs in a Post-CALEA, Cybsecurity-Centric Encryption Era. North Carolina Journal of Law & Technology, v. 17, n. 4, p. 599–644, maio 2016.

PAIXÃO, Rodrigo Gomes. **O Supremo Tribunal Federal e a regulação judicial da Criptografia:** diálogos entre a Suprema Corte e a Audiência Pública nº21. Acesso em: 21/03/2021. Disponível em <https://sbdp.org.br/publication/o-supremo-tribunal-federal-e-a-regulacao-judicial-da-criptografia-dialogos-entre-a-suprema-corte-e-a-audiencia-publica-no21/>. Acesso em: 20 abr. 2020.

SWIRE, P.; AHMAD, K. **Encryption and Globalization.** The Columbia Science & Technology Law Review, vol. XIII, spring 2012, p. 416-481. Disponível em: <https://goo.gl/knVYc6> Acesso em: 04 mar. 2020.

S. Ryder and N. Le-Khac, **The End of Effective Law Enforcement in the Cloud? - To Encrypt, or Not to Encrypt**, 2016 IEEE 9th International Conference on Cloud Computing (CLOUD), 2016, pp. 904-907, doi: 10.1109/CLOUD.2016.0133. Disponível em: <https://ieeexplore.ieee.org/document/7820370>. Acesso em: 04 mar. 2020

S. Ryder and N. Le-Khac, "The End of Effective Law Enforcement in the Cloud? - To Encrypt, or Not to Encrypt," 2016 IEEE 9th International Conference on Cloud Computing (CLOUD), 2016, pp. 904-907, doi: 10.1109/CLOUD.2016.0133. Available at: <https://ieeexplore.ieee.org/document/7820370>. Access in: April 11, 2020.

Contatos: rod2paixao@gmail.com e maria.marinho@mackenzie.br