CRYPTO WARS E BLOQUEIO DE APLICATIVOS: O DEBATE SOBRE REGULAÇÃO JURÍDICA DA CRIPTOGRAFIA NOS ESTADOS UNIDOS E NO BRASIL

CRYPTO WARS AND APP BLOCKING: THE DEBATE ON ENCRYPTION REGULATION IN THE UNITED STATES AND BRAZIL

Carlos Augusto Liguori Filho
Universidade de São Paulo – USP – (São Paulo, SP, Brasil)
Fundação Getulio Vargas de São Paulo (São Paulo, SP, Brasil)

João Pedro Favaretto Salvador
Fundação Getulio Vargas de São Paulo (São Paulo, SP, Brasil)

Recebimento: 14 maio 2018
Aceitação: 30 ago. 2018

Como citar este artigo / How to cite this article (informe a data atual de acesso / inform the current date of access):

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**, Curitiba, PR, Brasil, v. 63, n. 3, p. 135-161, set./dez. 2018. ISSN 2236-7284. Disponível em: <https://revistas.ufpr.br/direito/article/view/59422>. Acesso em: 22 dez. 2018. DOI: http://dx.doi.org/10.5380/rfdufpr.v63i3.59422.

RESUMO
O presente artigo tem como objetivo principal descrever e analisar os debates públicos sobre regulação jurídica da criptografia e acesso governamental a dados criptografados nos Estados Unidos e no Brasil, identificando pontos de convergência e divergência. Conforme a utilização de mecanismos criptográficos para fins privados – para comunicação *online* e armazenamento de dados – foi se tornando cada vez mais comum, autoridades passaram a enfrentar diversas dificuldades em relação à obtenção de dados no contexto de investigações criminais. Este cenário ensejou debates acerca da necessidade de uma regulação jurídica da criptografia, impondo possíveis restrições à sua utilização. De um lado, facilitaria o acesso por autoridades; de outro, poderia gerar enormes consequências em relação à segurança e privacidade de cidadãos. Nesse sentido pretende-se, em primeiro lugar, descrever como o debate foi conduzido nos Estados Unidos na década de 1990 e na década de 2010 – o que ficou conhecido como as *crypto wars*. Em seguida, será apresentado o debate no Brasil, motivado pelos sucessivos bloqueios do aplicativo WhatsApp entre 2015 e 2016. Por fim, será realizada uma análise sobre diferenças e semelhanças entre os debates, apontando para possíveis consequências de suas particularidades.

PALAVRAS-CHAVE
Criptografia. Privacidade. Direito e tecnologia. Proteção de dados. Poderes de investigação.

ABSTRACT
This article aims to describe and analyze the debate on the legal regulation of cryptography and government access to encrypted data in the United States and Brazil, identifying similarities and differences between them. As the use of encryption mechanisms for private purposes (such as online communications and data storage) became more and more common, government authorities faced

several difficulties in regard to the collection of data in the context of criminal investigations. This scenario led to debates about the need for a legal regulation of cryptography, imposing possible restrictions on its use. On the one hand, it would facilitate access by authorities, on the other hand, it could have disastrous consequences for the security and privacy of citizens. In this sense, we will firstly describe how the debate was conducted in the United States in the 1990s and in the 2010s – something that became known as the "crypto wars". Then, we will present how the debate was conducted in Brazil, motivated by successive suspensions of the WhatsApp app in the country between 2015 and 2016. Finally, we will analyze the differences and similarities between the debates, pointing to possible consequences of their particularities.

KEYWORDS
Cryptography. Privacy. Law and technology. Data protection. Investigatory powers.

INTRODUÇÃO

A criptografia é algo fundamental em diversos aspectos de nossas interações com a tecnologia. Ela é essencial para o devido funcionamento da internet, uma vez que permite o tráfego seguro e privado de dados entre partes, além de garantir a autenticação da identidade das partes envolvidas nestas operações. Sem ela, por exemplo, determinadas atividades como transações bancárias e compras *online* seriam inerentemente inseguras e, consequentemente, pouco atraentes para os usuários.

Nos últimos tempos, a adoção da criptografia tornou-se também um grande atrativo para o usuário comum, cada vez mais preocupado com sua privacidade e com a segurança de suas informações e atividades – *online* e *offline*. Esta preocupação justifica-se de um lado pelo constante desenvolvimento e aprimoramento de ataques *hacker* em serviços de uso cotidiano[1] e, de outro, pelo receio do próprio poder de vigilância de governos e empresas privadas sobre cidadãos e usuários, evidenciado após as informações e documentos divulgados por Edward Snowden, ex-empregado da *National Security Agency* estadunidense, em 2013[2], que revelaram ao mundo a extensão da capacidade tecnológica de vigilância do governo norte-americano.

Nesse contexto, as preocupações com o resguardo de dados, fraudes, invasão de sistemas, privacidade dos usuários, entre outras, tornaram-se um diferencial positivo para diversos provedores de aplicação no Brasil e no mundo, que passaram a adotar mecanismos sofisticados de criptografia forte como o padrão básico de segurança em seus serviços, o que se costumou chamar de criptografia

[1] Em 2016, a plataforma "Dropbox" sofreu um ciberataque e cerca de 68 milhões de usuários tiveram seus dados divulgados. Fonte: <https://goo.gl/CqhU5a>. O serviço de *e-mail* do Yahoo, por sua vez, já foi atacado pelo menos três vezes, sendo a última em 2014. Fonte: <https://goo.gl/Z9oWra>. Acessos em: 5 maio 2018.
[2] "Snowden NSA Files Decoded". Guardian. (01/11/13). <https://goo.gl/MEmVl5>. Acesso em: 5 maio 2018.

by default (PELL, 2016, p. 225). Exemplos disso são serviços de *e-mail*, como o ProtonMail, aplicativos de mensagem instantânea e VoIP, como o Telegram e o WhatsApp, e até mesmo sistemas operacionais, como o iOS[3] – tendo este último adotado a criptografia *by default* para proteger dados contidos nos iPhones.

Alguns tipos de criptografia, como a chamada criptografia ponta a ponta, impossibilitam que até mesmo o provedor de aplicação, responsável pelo funcionamento do serviço, seja capaz de acessar determinados conteúdos. Se, por um lado, isso garante mais proteção e segurança aos usuários (mesmo àqueles sem muito conhecimento de segurança da informação), por outro prejudica a capacidade técnica de autoridades governamentais, em casos de investigação criminal conduzidas ou viabilizadas por meio da utilização desses serviços.

Esse cenário ensejou um debate sobre a necessidade ou não de regular, por meio do Direito, o desenvolvimento, implementação e utilização da criptografia, de forma a viabilizar o acesso a dados por autoridades de investigação em determinados casos, resguardando, assim, a segurança pública. A questão é que esta restrição pode gerar severas consequências na integridade dos sistemas criptográficos, fragilizando sua segurança e potencialmente viabilizando violações à privacidade (novamente) por parte de criminosos e governos.

Nos Estados Unidos, esse debate surge na década de 1990, no início da popularização da internet como principal meio de comunicação e da popularização de instrumentos criptográficos para uso privado nas interações *online* – estas ficaram conhecidas como *crypto wars*. Após um desfecho nos anos 2000, o debate é retomado com força em 2015, após a dificuldade de acesso, pelo governo estadunidense, ao iPhone de um dos responsáveis pelo atentado terrorista em San Bernardino. No Brasil, o debate surge pela primeira vez após os diversos bloqueios do aplicativo WhatsApp em 2015 e 2016, envolvendo a dificuldade de acesso a conteúdo de conversas na plataforma e sua criptografia ponta a ponta.

Nesse sentido, pretende-se com o presente artigo descrever e analisar o debate sobre a regulação jurídica da criptografia e acesso governamental a dados criptografados nos Estados Unidos e no Brasil, apontando diferenças, semelhanças e possíveis consequências de sua condução.

[3] "Apple expands data encryption under iOS 8". Ars Technica. (18/09/14). <https://goo.gl/ahR5Jh>. Acesso em: 7 maio 2018.

1 PANORAMA DAS *CRYPTO WARS* ESTADUNIDENSES

O conflito entre o uso de criptografia e o poder de investigação das autoridades do governo americano é intimamente ligado ao processo de popularização do uso dessa tecnologia.

Do fim da Segunda Guerra Mundial até o início dos anos 90, quem detinha o poder sobre as principais ferramentas criptográficas dos Estados Unidos era a Agência de Segurança Nacional *(National Security Agency*, ou NSA). Este órgão do Departamento de Defesa exercia dois papéis complementares essenciais para o sucesso de operações militares: na ofensiva, a NSA interceptava e decodificava mensagens enviadas por forças estrangeiras e por outros alvos de investigação; na defensiva, a agência desenvolvia e utilizava o estado da arte da tecnologia criptográfica para proteger as forças armadas, o governo e indústrias de grande importância (SWIRE; AHMAD, 2012, p. 433).

Ao longo dos anos, contudo, o avanço das tecnologias de informação permitiu a difusão de ferramentas eficientes de criptografia desenvolvidas por entes privados, resultando na corrosão do papel dominante da NSA. A criptografia, que antes era uma ferramenta de segurança de uso quase inteiramente militar e diplomático, foi gradativamente disponibilizada para usuários comuns, ainda que exigisse deles considerável conhecimento técnico para sua implementação em sistemas de comunicação.

Essa manifestação do progresso técnico mostrou-se uma excelente notícia para aqueles que pediam meios de comunicação protegidos contra agentes mal-intencionados, mas não para os antigos detentores do monopólio da criptografia, que demonstraram preocupação. Diante da erosão que o uso amplo de criptografia poderia exercer sobre sua habilidade de monitorar criminosos e entidades estrangeiras, as agências de inteligência (especialmente a NSA) ativamente tentaram impedir esse processo, inclusive emitindo ordens de sigilo e revogando o financiamento de pesquisadores e desenvolvedores da área (LEVY, 2002).

O fracasso dessas ações foi evidenciado pela continuação do desenvolvimento privado de criptografia no início dos anos 90. Um importante exemplo que atesta a dificuldade vivenciada pelo governo americano nesse período foi o desenvolvimento do sistema de chave pública PGP (*Pretty Good Privacy*) pelo ativista e engenheiro de *software* Phil Zimmerman. O programa foi publicado por seu desenvolvedor na internet já em 1991, burlando os rígidos regimes de exportação de ferramentas de criptografia em vigência nos anos 90 e sedimentando a dificuldade de se deter a difusão da tecnologia para particulares dentro e fora dos Estados Unidos[4].

[4] Cf. Philip R. Zimmermann, **Why I Wrote PGP** (1999), disponível em: <https://goo.gl/Uix30S>. Acesso em: 23 abr. 2018.

A situação crítica levou a então recém-estabelecida administração de Bill Clinton a propor políticas públicas diretamente voltadas para a manutenção dos poderes de investigação das autoridades de inteligência. Os vigorosos embates e debates que se seguiram, entre governo, empresas e comunidade científica americana sobre regulação da criptografia são hoje referidos como "*crypto wars*"[5].

1.1 CRYPTO WARS 1.0: LIÇÕES DOS ANOS 90

O governo americano adotou duas estratégias para tentar controlar a difusão do uso de criptografia durante os anos 90. Em primeiro lugar, defendeu a elaboração de um sistema de "guarda de chaves" (*Key Escrow),* cuja finalidade era garantir que a comunicação entre dispositivos fabricados no país pudesse ser interceptada mesmo com o amplo uso de criptografia forte (SWIRE; AHMAD, 2012, p. 435). Paralelamente, o governo também manteve regulações que limitavam consideravelmente a venda de produtos de criptografia para fora do país (DIFFIE; LANDAU, 2005).

O desafio de qualquer regime de exportação é encontrar um ponto de equilíbrio entre as regulações que buscam limitar a capacidade de outros países de desenvolverem tecnologia militar (restringindo a exportação destes produtos) e a preservação da competitividade internacional das empresas domésticas (estimulando a exportação destes) (DIFFIE; LANDAU, 2005, p. 5). Esse desafio obriga a entidade reguladora a estabelecer critérios de diferenciação entre produtos de uso militar (de exportação restrita) e produtos de uso civil (de exportação muitas vezes promovida). Justamente porque a criptografia foi por muito tempo ferramenta de uso quase exclusivamente militar, seu regime de exportação até a metade dos anos 90 era bastante restrito.

Com a popularização da criptografia para uso de particulares, contudo, classificá-la como apenas produto de uso militar ou civil se tornou uma tarefa difícil. A criptografia utilizada para proteger uma mensagem entre militares de alta patente se tornou extremamente semelhante àquela adotada para proteger uma transferência bancária ou uma mensagem de *e-mail* entre particulares. Mesmo quando passou a ser considerada produto de uso duplo (tanto civil quanto militar), contudo, a tecnologia em suas implementações mais fortes permaneceu classificada como "munição" ("*Munition"*) e, em decorrência disso, teve sua exportação consideravelmente limitada pelo *International Traffic in Arms Regulation* (ITAR)[6]. A exportação de produtos nessa categoria exigia

[5] "Guerras Criptográficas", em tradução livre.
[6] Conjunto de regulações de exportação de produtos militares de responsabilidade do Departamento de Estado dos EUA. Disponível em: <https://goo.gl/BwO93e>. Acesso em: 25 abr. 2018.

licenças individuais emitidas pelo Departamento de Comércio. Essa exigência restringia o poder de venda de empresas privadas dedicadas a desenvolver sistemas de criptografia cada vez mais complexos, visto que a rápida evolução da tecnologia significava uma grande diversidade de produtos que precisariam ser individualmente licenciados, sob o risco constante de recusa (SWIRE; AHMAD, 2012, p. 438).

Além de exercer controle por meio de regimes de exportação, o governo americano buscou também controlar o uso doméstico de criptografia, na tentativa de manter seu poder de vigilância e investigação em território nacional. Nessa linha, a mais relevante tentativa de implementação de um sistema de guarda de chaves foi a iniciativa *Clipper Chip*, divulgada pela Casa Branca em abril de 1993[7]. A iniciativa se manifestou da seguinte forma: o governo desenvolveu um chip que poderia ser adquirido e implementado em dispositivos de comunicação por empresas fabricantes. O produto, argumentava o governo, era mais seguro, mais conveniente e mais barato do que outros disponíveis na época. Contudo, ao mesmo tempo que esse chip implementaria funções criptográficas presumivelmente fortes nos dispositivos[8], as chaves criptográficas associadas a cada *chip* seriam enviadas para entidades associadas ao governo no momento da fabricação.

Cada metade das chaves seria armazenada em um de dois bancos de dados de guarda, administrados por entidades independentes entre si. Quando autorizados por uma ordem judicial específica, os administradores dos bancos de dados revelariam as chaves para as agências de investigação, permitindo a interceptação da comunicação apenas entre dois ou mais dispositivos utilizados por suspeitos e equipados com o *Clipper Chip*. Dessa forma, segundo o governo, a privacidade de usuários não investigados não seria violada.

A proposta foi a principal responsável por inflamar o debate sobre criptografia nos anos 90. Não se sabe se o governo esperava por essa reação, mas sua iniciativa foi recebida de forma bastante negativa pela comunidade científica e pelas empresas fabricantes. Ainda que o produto tivesse sido anunciado como o equilíbrio ideal entre a segurança das comunicações e a capacidade de acesso pelo Estado, os anos que se seguiram ao anúncio do *Clipper Chip* foram caracterizados pela exposição de suas falhas de segurança e pelo surgimento de novos sistemas de criptografia mais baratos e

[7] Cf. **Statement by the Press Secretary**, Office of the Press Secretary, The White House, The Clipper Chip Initiative (Apr. 16, 1993). Disponível em: <https://goo.gl/KnLbWT>. Acesso em: 25 abr. 2018.

[8] Naquela época as informações transmitidas por boa parte dos dispositivos ainda não eram criptografadas em termos de *software*. O algoritmo criptográfico era implementado fisicamente em *chips* instalados no *hardware* do dispositivo, como era o caso do *Clipper Chip* (RICE, 2017, p. 38).

confiáveis (BARR, 2016, p. 311). O resultado foi a não adoção do produto pelas empresas ou a não implementação em dispositivos em escala significativa.

São várias as causas que podem ser atribuídas ao fracasso do *Clipper Chip* e, por consequência, das subsequentes propostas de guarda de chaves, mas uma merece destaque: a desconfiança da comunidade científica em relação à promessa de segurança feita pelo governo[9]. Desde seu anúncio, o algoritmo de criptografia inserido no *Clipper Chip*, o "Skipjack", foi mantido em sigilo. A prática, conhecida como "security by obscurity", é criticada por especialistas, uma vez que impede a realização de testes que comprovem a solidez da base matemática do algoritmo (RICE, 2017, p. 39). Mesmo com o sigilo, contudo, o governo não foi capaz de evitar críticas técnicas a respeito de seu *chip* criptográfico.

Em 1994, o criptógrafo e então pesquisador da AT&T, Matt Blaze, descobriu e tornou pública uma série de falhas técnicas ocorridas no processo de implementação do algoritmo no *chip* (BLAZE, 1994). De acordo com Blaze, um defeito grave do produto permitia que o sistema fosse burlado, de forma que o acesso governamental às comunicações seria impossível mesmo em posse da chave obtida por meio de ordem judicial. A descoberta do criptógrafo foi imortalizada na capa da edição de 12 de junho de 1994 do jornal The New York Times, ficando claro seu impacto para o resultado das *Crypto Wars* dos anos 90[10].

Mais tarde, em maio de 1997, um grupo de profissionais e estudiosos da criptografia publicou uma detalhada crítica, não mais ao *Clipper Chip* em específico (iniciativa que já estava em estado de abandono), mas a todas as propostas de guarda de chave e acesso à comunicação criptografada que ainda povoavam o imaginário governamental (ABELSON et al., 1997). O relatório, intitulado "*The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption*", listava diversos problemas inerentes à adoção de sistemas de guarda de chaves, recomendando ao governo o abandono de tais iniciativas. Por sua completude, as conclusões dos estudiosos merecem atenção.

Em síntese, os especialistas apontaram, em primeiro lugar, que a infraestrutura de guarda de chaves proposta pelo governo traria necessariamente um grande risco à segurança dos dispositivos interceptáveis, visto que a introdução de um novo caminho para o acesso à comunicação sempre traz consigo novas vulnerabilidades. Além disso, a concentração das chaves em bancos de dados tornaria esses centros alvos de grande valor para terceiros mal-intencionados (ABELSON et al., 1997, p. 10).

[9] Outra causa que pode ser mencionada, mas que exerceu menor influência, é o fato de que o Clipper Chip foi proposto quando a criptografia por *hardware* estava sendo substituída na indústria pela criptografia por *software*, consideravelmente mais barata (RICE, 2017, 39).

[10] Cf. LEVY, Steven. Battle of the Clipper Chip. **The New York Times,** 12 jun. 1994. Disponível em: <https://goo.gl/HKA4dK>. Acesso em: 26 abr. 2018.

Qualquer falha nos protocolos de segurança de um banco de dados (como vazamentos de informação por funcionários e outras violações de deveres de confidencialidade) teria grande impacto na segurança de um número enorme de dispositivos.

Em segundo lugar, apontaram para a enorme complexidade da hipotética infraestrutura de guarda. Ainda que fosse possível a construção de um sistema transparente, esse sistema seria extraordinariamente complexo e difícil de ser implementado, visto que introduziria novas entidades, chaves, requisitos operacionais e interações que lidariam com a manipulação de informação sensível (ABELSON et al., 1997, p. 10).

Por fim, foram destacados os altíssimos custos associados à construção e manutenção de um sistema de custódia de alta complexidade, incluindo custos de controle de informação sensível por longos períodos, custos de fiscalização pelo governo, custos de atualização de protocolos de segurança e custos de comunicação necessários para o cumprimento do número substancial de ordens judiciais que seriam emitidas (ABELSON et al., 1997, p. 16). De acordo com os estudiosos da área, o governo teria fracassado em sua missão de propor um modelo de guarda de chaves que se mostrasse viável do ponto de vista econômico.

A desconfiança da comunidade científica muito contribuiu para a rejeição dos sistemas de guarda de chaves pelas empresas de tecnologia, mas a disputa não acabava aí. O governo ainda mantinha seu modelo de controle de exportação de criptografia e os debates inflamados pelo *Clipper Chip* acabaram trazendo esse problema de volta para os holofotes.

O modelo de controle de exportações vigente à época não só diminuía a disponibilidade de criptografia forte no exterior como também limitava sua disponibilidade nos próprios Estados Unidos. Isso porque as fabricantes americanas precisavam escolher entre produzir e vender criptografia fraca em ambos os mercados (interno e externo), ou desenvolver duas linhas de produtos: uma mais forte, destinada ao mercado interno, e outra mais fraca, destinada à exportação (SWIRE; AHMAD, 2012, p. 438). A escolha pelo segundo caminho, ainda que facilitasse o processo de exportação, implicava maiores custos de pesquisa e desenvolvimento.

Com o aumento da concorrência de empresas europeias e asiáticas tanto no mercado externo quanto no interno (visto que os produtos trazidos de fora dos Estados Unidos não estavam sujeitos às regras americanas de exportação), o peso da regulação ficou cada vez mais claro e a pressão política por uma reforma ficou mais intensa. Pequenas flexibilizações ocorreram com o passar do tempo[11],

[11] Na primeira metade dos anos 90, o governo determinou que chaves criptográficas de até 40-bits poderiam ser exportadas livremente. Contudo, essa flexibilização não teve qualquer impacto, já que em 1992 um computador pessoal era capaz de

mas até o fim da década nenhuma alteração considerável havia sido aprovada pelo Congresso ou pela administração[12].

Em 1996, o Conselho Nacional de Pesquisa (*National Research Council*) publicou o resultado de um estudo sobre política de criptografia encomendado pela administração Clinton 18 meses antes (DAM; LIN; NATIONAL RESEARCH COUNCIL [U.S.], 1996). O relatório final causou surpresa ao contrariar as políticas de guarda de chave e de controle de exportação defendidas pelo governo. A conclusão do Conselho foi que as vantagens do uso amplo de criptografia superavam as desvantagens, e que a política nacional de criptografia dos Estados Unidos era incapaz de cumprir os requisitos de segurança de uma sociedade de informação. Ainda, concluíram que as políticas de exportação prejudicavam o uso doméstico de criptografia forte, recomendando que elas fossem consideravelmente flexibilizadas.

As *crypto wars* ainda não estavam vencidas, contudo. Em sentido contrário ao movimento de flexibilização do uso e comércio de criptografia, foi proposto em 1997 um projeto de lei predominantemente elaborado pelo *Federal Bureau of Investigation* (FBI) e pelo *House Intelligence Committee* (comitê legislativo permanente que trata de assuntos relacionados às agências de inteligência americana), que visava atribuir responsabilidade criminal àqueles que fabricassem ou distribuíssem produtos de criptografia que impedissem a interceptação pelo governo. Em reação a essa proposta, um grupo de professores de Direito de diversas universidades publicou uma carta aberta direcionada ao Congresso Americano contendo uma crítica detalhada nos moldes daquela que expôs os riscos de segurança da guarda de chaves poucos meses antes[13]. Diante de tal reação, o projeto, que representava um dos últimos esforços de conservação do poder de investigação do governo nos anos 90, não prosperou.

Em setembro de 1999, a administração Clinton finalmente declarou a derrota de suas pretensões de controle restrito do uso e da exportação de criptografia forte. Em uma mudança completa de sua política de criptografia, representantes do Departamento de Defesa e da Secretaria

decifrar uma mensagem criptografada dessa forma em tempo moderado. Em 1998, o governo passou a permitir a exportação de chaves de até 56-bits. Naquela época, contudo, já havia um consenso na comunidade científica de que as chaves deveriam ter no mínimo 128-bits para serem consideradas seguras (DIFFIE; LANDAU, 2005, p. 12).

[12] Em 1996, vários membros do Congresso propuseram projetos de lei que visavam à diminuição do poder do Executivo de controlar a exportação de criptografia. Os projetos (que em conjunto viriam a ser conhecidos como SAFE, ou *Security and Freedom through Encryption*), porém, não tinham apoio suficiente para reverter um prometido veto presidencial (DIFFIE; LANDAU, 2005, p. 12).

[13] A carta assinada por trinta e um professores de diversas universidades americanas pode ser acessada pelo endereço arquivado em: <https://goo.gl/uEuG8N>. Acesso em: 26 abr. 2018.

de Comércio anunciaram[14] que o governo iria remover boa parte dos controles de exportação tão criticados, sob o fundamento de que a competitividade da indústria americana merecia ser preservada[15]. Além disso, um dos objetivos declarados da nova política era o de assegurar que os cidadãos americanos tivessem acesso à forma mais forte de proteção disponível para suas comunicações, indicando que novas políticas de guarda de chaves (ou semelhantes) não seriam adotadas nos anos seguintes. De fato, diante da aparente derrota das autoridades investigativas, as *crypto wars* só seriam retomadas com força após mais de uma década.

1.2 CRYPTO WARS 2.0: NOVOS VELHOS PROBLEMAS

Se nos anos 90 a preocupação das autoridades de investigação americanas foi resultado da erosão de seu monopólio do uso de criptografia, nos últimos anos foi a decisão das grandes empresas de tecnologia de levar criptografia para as massas, inclusive para usuários que não desfrutavam de qualquer conhecimento técnico, que gerou comoção.

Ainda que o uso de criptografia tivesse sido bastante disseminado após a remoção dos limites de exportação, essa disseminação sempre acabava esbarrando na falta de conhecimento técnico do público leigo, que por desconhecimento ou desinteresse raramente empregava a ferramenta. Até esse momento, ainda que as empresas de tecnologia equipassem os dispositivos de comunicação com ferramentas de criptografia, o funcionamento dessas ferramentas era opcional e, na maioria dos casos, exigia uma atitude proativa do usuário. O uso difundido da criptografia, portanto, ainda era restrito a determinadas aplicações (como serviços de comércio eletrônico e transações bancárias) ou a usuários mais sofisticados.

Em 2014 esse cenário mudou. Acontecimentos de impacto global, como o vazamento de informações confidenciais da NSA pelo ex-funcionário Edward Snowden em 2013 (que denunciou o poder de vigilância ainda exercido pelo governo americano)[16] e a divulgação não consensual de fotos íntimas de celebridades que utilizavam serviços de armazenamento de dados da Apple[17], levaram as empresas de tecnologia a repensarem suas políticas de criptografia. A fabricante do iPhone, de forma

[14] As transcrições das declarações do Secretário de Comércio e dos representantes do Departamento de Defesa podem ser lidas, respectivamente, em: <https://goo.gl/1mBJjq> e em: <https://goo.gl/nJ3BVK>. Acesso em: 26 abr. 2018.
[15] O regime de controle prévio foi substituído por um regime de relatórios posteriores, aplicável apenas para a exportação de produtos que utilizam chaves de mais de 64-bits.
[16] MACASKILL, E. et al. **NSA files decoded**: Edward Snowden's surveillance revelations explained. The Guardian Disponível em: <https://goo.gl/MEmVl5>. Acesso em: 27 abr. 2018.
[17] Jennifer Lawrence nude photos leaked "after iCloud hack". **BBC Newsbeat**, 1 set. 2014. Disponível em: <https://goo.gl/2tcR4o>. Acesso em: 27 abr. 2018

pioneira, atualizou o sistema operacional de seus celulares (iOS) para tornar a criptografia configuração padrão[18].

O novo sistema operacional utilizava criptografia para codificar o conteúdo do dispositivo sem a necessidade de ativação da função pelo usuário. O acesso ao conteúdo criptografado dessa forma era exclusivo ao próprio usuário do iPhone, de forma que nem a empresa era capaz de reverter o processo. Ocorre que, por consequência, a Apple deixou para trás não só seus problemas com privacidade, mas também sua capacidade técnica de atender a ordens judiciais de desbloqueio de celulares apreendidos.

Para o horror das autoridades investigativas americanas, outras gigantes da tecnologia, como a Google[19], passaram prontamente a adotar aquilo que passou a ser denominado *criptografia by default* (PELL, 2016, p. 225), ou seja, a implementação de mecanismos sofisticados de criptografia forte como o padrão básico de segurança de seus serviços. Pouco mais tarde, aplicativos de mensagem instantânea, como Telegram e WhatsApp, passaram a implementar em seus serviços a chamada criptografia ponta a ponta, ferramenta técnica que torna o conteúdo das mensagens acessível apenas ao remetente e ao destinatário (as "pontas" da comunicação), uma vez que a chave usada para criptografar o conteúdo é gerada e fica contida exclusivamente em seus celulares (LIGUORI FILHO, 2017). Assim como no caso da Apple, a Google, o Telegram e o WhatsApp acabaram por deixar de lado sua capacidade técnica de interceptação. O palco estava armado para uma ressurgência ainda mais intensa das *crypto wars*.

E as *crypto wars* de fato foram retomadas. Não demorou muito para que autoridades se insurgissem contra as decisões das empresas de tecnologia. Foi o caso do então diretor do FBI, James Comey, que, poucos meses após o anúncio feito pela Apple, realizou uma das mais importantes falas contrárias ao uso da criptografia forte como padrão de segurança[20]. O ex-diretor do FBI afirmou que a adoção desenfreada de criptografia forte seria extremamente prejudicial para autoridades de investigação, uma vez que as impediria de ter acesso tanto a dados estáticos (no caso da criptografia em sistemas operacionais em dispositivos) quanto a dados de comunicações em trânsito (no caso de aplicativos de mensagem) no contexto de investigações criminais. A consequência disso, de acordo

[18] Apple expands data encryption under iOS 8, making handover to cops moot. **Ars Technica**, 18 set. 2014. Disponível em: <https://goo.gl/ahR5Jh>. Acesso em: 27 abr. 2018.
[19] Newest Androids will join iPhones in offering default encryption, blocking police. **The Washington Post**, 18 set. 2014. Disponível em: <https://goo.gl/Shmhkd>. Acesso em: 27 abr. 2018.
[20] COMEY, James. **Going Dark**: Are Technology, Privacy, and Public Safety on a Collision Course? Brooklings Institution, Washington, D. C., 16 out. 2014. Disponível em: <https://goo.gl/Rj2pGR>. Acesso em: 23 abr. 2018.

com Comey, seria que o poder de investigação do Estado ficaria "nas trevas", fenômeno que ele chamou de "*going dark*"[21].

A solução para isto, de acordo com o diretor, seria a regulamentação, pela via legislativa, do acesso às informações necessárias para a investigação – no caso de serviços que utilizam criptografia, isso só seria possível com a implementação obrigatória de medidas de acesso excepcional para o poder público, como um *backdoor*[22]. Para ele, meios alternativos de investigação não forneciam as informações essenciais que estavam contidas no conteúdo das comunicações criptografadas.

A reação ao posicionamento do FBI veio quase tão rápida quanto a declaração de Comey. Em 2015, diversos estudiosos e profissionais da criptografia (muitos deles veteranos das *crypto wars*) elaboraram crítica análoga àquela publicada em 1997 contra as propostas de guarda de chaves. Nesse novo relatório (intitulado "*Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications"*), os estudiosos apontaram para inúmeros riscos inerentes à obrigação jurídica de inserção de mecanismos de acesso excepcional em serviços e dispositivos, que afetariam a segurança e privacidade de milhões de usuários que os utilizam regularmente. Ademais, alegaram também que o constante desenvolvimento tecnológico, para além de permitir a elaboração de técnicas complexas de criptografia, viabilizou também diversas outras formas de investigação e vigilância que poderiam e deveriam ser utilizadas sem o mesmo impacto na segurança dos usuários. Nesse sentido, com essas tecnologias, não apenas não estaríamos vivendo "nas trevas", como teríamos nas mãos as ferramentas para viver uma "era de ouro da vigilância" (*golden age of surveillance)* (ABELSON et al., 2015, p. 24-26).

Em dezembro de 2015, o debate, que até então era majoritariamente travado entre o FBI e a comunidade científica, passou a envolver também o Poder Judiciário. Em meio à investigação de um ataque terrorista em San Bernardino[23], a polícia estadunidense não conseguiu, em um primeiro momento, em razão da criptografia dos seus sistemas operacionais, acessar os dados armazenados em *smartphones* de suspeitos.

---

[21] Ainda que Comey tenha popularizado o uso da expressão para designar o problema de acesso às comunicações criptografadas, o termo foi usado pela primeira vez pelo FBI em 2011, quando a Conselheira Geral Valerie Caproni testemunhou para o *House Judiciary Committe* em audiência. Nesse testemunho, a metáfora do *"going dark"* foi usada para fazer referência ampla aos desafios de interceptação decorrentes de novas tecnologias. Cf. VALERIE CAPRONI. **Going Dark**: Lawful Electronic Surveillance in the Face of New Technologies. 17 fev. 2011, Sec. House Judiciary Committee. Disponível em: <https://goo.gl/UnVzF1>. Acesso em: 27 abr. 2018.

[22] Um *backdoor* é um mecanismo ou ponto de acesso em um dispositivo de comunicação ou rede que permite que o criador do *software* ou *hardware* acesse conteúdo ou informações sem a permissão ou conhecimento do usuário (PELL, 2016, p. 609).

[23] Apple challenges "chilling" demand to decrypt San Bernardino shooter's iPhone. **The Guardian**, 17 fev. 2016. Disponível em: <https://goo.gl/G9XAkE>. Acesso em: 27 abr. 2018.

Diante de sua suposta incapacidade de obter as informações necessárias para dar continuidade às investigações[24], o FBI levou a questão para o Judiciário, pleiteando que a Apple fosse obrigada a desenvolver um sistema operacional que pudesse ser acessado no contexto de investigações – por meio de *backdoors*. A Apple resistiu, alegando que o mecanismo fragilizaria a segurança de seus aparelhos e comprometeria a privacidade de seus usuários[25]. A ação judicial foi abandonada quando o FBI declarou ter conseguido, com a ajuda de um terceiro, desbloquear o iPhone apreendido e obter as informações necessárias para o prosseguimento da investigação[26]. Não revelou, contudo, a técnica que permitiu o desbloqueio.

Até a elaboração deste artigo, diversos representantes das autoridades de investigação se manifestaram sobre o tema, mantendo a pressão sobre o Legislativo e as empresas de tecnologia. Da mesma forma, diversos membros da comunidade científica ofereceram resposta às propostas de implementação obrigatória de *backdoors*[27]. Entre o fim 2017 e o começo de 2018, tanto o atual diretor do FBI, Christopher Wray, quanto o *Deputy Attorney General*, Rod J. Rosenstein, manifestaram-se publicamente pedindo por uma legislação que obrigasse as empresas de tecnologia a implementar criptografia somente de maneira que garantisse o acesso excepcional pelas autoridades de investigação.

Rosenstein[28] pediu por uma legislação que determinasse um "uso responsável da criptografia", obrigando as empresas a manterem um banco de chaves de acesso excepcional que pudessem ser fornecidas às autoridades em contexto de investigação. Pediu, ainda, que a criptografia ponta a ponta fosse abandonada. Wray[29], semelhantemente, pediu por uma "solução responsável", voluntária ou legislativa, em que as empresas mantivessem a capacidade de fornecer as comunicações de seus clientes investigados às autoridades. Além de repetir as "sugestões" de Rosenstein, Wray

[24] Em março de 2018 o *Office of the Inspector General* (OIG) do Departamento de Justiça dos Estados Unidos publicou relatório com resultados de inquérito que buscava avaliar a precisão das declarações feitas pelo FBI a respeito de sua capacidade de desbloquear o iPhone. O relatório indicou que, ao contrário do que foi originalmente alegado, o FBI não tinha esgotado suas capacidades de investigação antes de levar o problema para o Poder Judiciário. O relatório está disponível em: <https://goo.gl/1z5pTX>. Acesso em: 27 abr. 2018.

[25] Apple Fights Order to Unlock San Bernardino Gunman's iPhone – **The New York Times**. Disponível em: <https://goo.gl/CuzZ6J>. Acesso em: 8 maio 2018.

[26] FBI may have found way to unlock San Bernardino shooter's iPhone without Apple. **The Guardian**, 22 mar. 2016. Disponível em: <https://goo.gl/Me2tzf>. Acesso em: 8 maio 2018.

[27] Em 2016, por exemplo, um relatório publicado pelo Berkman Center for Internet & Society da Universidade de Harvard se uniu ao coro dos que questionavam a própria premissa de que as autoridades estariam *"going dark"*, concluindo que as novas tecnologias oferecem uma série de oportunidades de investigação que não estariam sendo devidamente aproveitadas pelo FBI (GASSER et al., 2016).

[28] OFFICE OF PUBLIC AFFAIRS, FEDERAL BUREAU OF INVESTIGATION. **Deputy Attorney General Rod J. Rosenstein Delivers Remarks on Encryption at the United States Naval Academy**. Disponível em: <https://goo.gl/KUnjZz>. Acesso em: 23 abr. 2018.

[29] WRAY, Christopher. **Raising Our Game**: Cyber Security in an Age of Digital Transformation. Disponível em: <https://goo.gl/egjCdq>. Acesso em: 23 abr. 2018.

divergiu em um ponto: para ele, o sistema de guarda de chaves deveria ser administrado por terceiros, ou seja, nem pela empresa, nem pelo governo.

É importante destacar que, diferentemente do caso dos anos 90, em que a política de criptografia foi anunciada publicamente e colocada a escrutínio da comunidade científica e da sociedade civil, os pedidos de regulação feitos pelas autoridades a partir de 2014 pecaram pela falta de clareza. Nem Comey, nem Wray e nem Rosenstein foram especialmente claros em relação às reformas legislativas que deveriam ser implementadas, ou aos detalhes técnicos dos mecanismos de acesso excepcional que propunham.

Ainda assim, é possível elencar algumas diferenças claras entre as novas propostas e as dos anos 90. Em primeiro lugar, ao contrário da iniciativa *Clipper Chip*, a inclusão de *backdoors* ou de um novo sistema de guarda de chaves não seria opcional, mas sim determinada por lei. Em segundo lugar, também ao contrário da iniciativa *Clipper Chip*, a implementação de um *backdoor* moderno ultrapassa a mera adição de um componente novo ao dispositivo, exigindo uma alteração no código desenvolvido pelas empresas de tecnologia, fator esse que atraiu a atenção de teóricos da liberdade de expressão (BARR, 2016, p. 313).

O que se repete, contudo, é a dinâmica do debate. Assim como nos anos 90, as novas propostas de regulação governamentais têm sido duramente criticadas pela comunidade científica pela insegurança que decorreria de sua implementação. Ainda que mais genéricas, as propostas de imposição de *backdoors* ou de novas modalidades de guarda de chaves não têm convencido os especialistas em segurança de informação, como também foi o caso das propostas da administração Clinton. Em fevereiro de 2018, Riana Pfefferkorn, pesquisadora especialista em criptografia ligada ao *Center for Internet and Society* da Universidade de Stanford, publicou relatório em que analisou as possíveis consequências da regulação desejada por Wray e Rosenstein. Sua conclusão, novamente, foi que a aprovação de legislação nesse sentido não seria uma atitude sábia do governo dos Estados Unidos (PFEFFERKORN, 2018, p; 16).

Diante da grande quantidade de manifestações vindas de ambos os lados do debate nos primeiros meses de 2018, é extremamente difícil, no momento em que se elabora este artigo, prever um final certo e próximo para as *crypto wars* estadunidenses. Ainda que seja tentador tal exercício de futurologia, devemos voltar nossos olhos para o debate sobre regulação da criptografia que ocorre em terras brasileiras. Como será demonstrado a partir de agora, as autoridades investigativas brasileiras também entraram em conflito com a popularização do uso de criptografia forte por particulares nos últimos anos, conflito esse que pode ser analisado por suas semelhanças e diferenças com aquele relatado até o momento.

2 *CRYPTO WARS* À BRASILEIRA

Ao contrário do cenário estadunidense, o debate público sobre acesso a comunicações criptografadas e regulação jurídica da criptografia no Brasil surgiu e se intensificou de forma exponencial somente nos últimos anos, à época das *crypto wars 2.0*. Seu catalisador foram os sucessivos bloqueios do aplicativo de mensagens WhatsApp em território nacional, ocorridos no período entre 2015 e 2016, após a empresa descumprir obrigação do fornecimento do conteúdo de mensagens no contexto de investigações criminais.

De maneira semelhante ao caso Apple v. FBI, um dos motivos elencados pelo WhatsApp para justificar o não fornecimento dos dados foi sua própria incapacidade técnica de acessá-los, uma vez que havia implementado criptografia ponta a ponta em seu sistema. De qualquer modo, com o descumprimento, o serviço foi bloqueado, afetando milhões de usuários no País.

A questão da legalidade dos bloqueios foi levada, em junho de 2017, ao Supremo Tribunal Federal, que convocou uma audiência pública para debater aspectos jurídicos e técnicos dos bloqueios de aplicativos, acesso a comunicações criptografadas e limites técnicos da criptografia.

No entanto, antes desse período específico grande parte dos trabalhos brasileiros sobre a relação entre direito e criptografia focavam no potencial de sistemas criptográficos em garantir a integridade e segurança de transações *online* (como em compras pela internet e *internet banking*) e em autenticar documentos (MARCACINI, 2002). Ademais, estudiosos do direito à privacidade apontavam também para a importância da criptografia como ferramenta de autotutela da privacidade e da proteção de dados pessoais na internet (LEONARDI, 2012).

Após os escândalos Snowden, que desencadearam a promulgação do Marco Civil da Internet (MCI, Lei nº 12.965/14) em 2014, os debates acerca dos direitos dos usuários de internet e proteção de dados pessoais intensificaram-se, culminando na elaboração de diversos projetos de lei para proteção de dados pessoais, que tramitam no Congresso Nacional até os dias de hoje (SOUZA; LEMOS, 2016, p. 25)[30]. No entanto, esse mesmo MCI foi utilizado para justificar os bloqueios de aplicativos como sanção e, posteriormente, acender o debate sobre regulação jurídica da criptografia no Brasil. Vale, portanto, descrever rapidamente alguns pontos relativos ao MCI, de modo a melhor apresentar a idiossincrática construção deste debate.

[30] A saber, trata-se dos seguintes projetos de lei: PL 4060/2012; PL 5276/2016 e PLS 330/2013.

2.1 O MARCO CIVIL DA INTERNET E OS BLOQUEIOS DE APLICATIVO

Assim como nos Estados Unidos, as divulgações de Edward Snowden em 2013 impactaram de forma direta a questão da privacidade e proteção de dados no território brasileiro. De fato, dentre os documentos divulgados pelo *whistleblower*, constavam indícios de que a então presidenta Dilma Rousseff havia sido alvo de espionagem por parte da NSA[31]. Ao contrário dos EUA, no entanto, a reação à espionagem e vigilância de dados não ocorreu apenas no âmbito do mercado, com a lógica da criptografia *by default*, mas também na esfera legislativa.

Uma das reações a este escândalo ocorreu no texto do Marco Civil da Internet – à época ainda um Projeto de Lei, nº 2.126/11, que tramitava no Congresso Nacional após consulta pública realizada nos anos de 2009 e 2010. Ao texto foram acrescidos dispositivos específicos para proteção de dados pessoais e privacidade (no artigo 7º) e, em maio de 2014, a lei foi sancionada pela presidenta Dilma (SOUZA; LEMOS, 2017). A lei estabelece diversos princípios, direitos e deveres em relação ao uso da internet no Brasil – em relação a usuários, provedores de aplicação e provedores de conexão.

Ainda que não trate especificamente da restrição ou promoção da criptografia, o Marco Civil estabelece determinadas obrigações a provedores, de aplicação na internet em relação a, de um lado, a proteção dos registros, dados pessoais e comunicações privadas dos usuários[32], e, de outro lado, a obrigação do fornecimento destes conteúdos – sempre mediante ordem judicial[33] – e sanções para o descumprimento dessas obrigações.

Entre as sanções por descumprimento de ordem judicial, o art. 12 estabelece a "*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*".

As atividades mencionadas no artigo 11 consistem em "*operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet*". Nesse sentido, a partir de uma interpretação específica dos supramencionados incisos do Artigo 12[34], o aplicativo de mensagens WhatsApp foi sucessivamente

[31] Documentos da NSA apontam Dilma Rousseff como alvo de espionagem. **G1**, 9 set. 2013. Disponível em: <https://goo.gl/A5dYuw>. Acesso em: 3 abr. 2018.

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

[33] "Art. 10 […] § 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no **caput**, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º. § 2º O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7º."

[34] Não é consensual a interpretação do artigo 12 que possibilita o bloqueio dos aplicativos como sanção. Neste sentido, ver SOUZA; BRANCO, 2016.

bloqueado em território nacional, após não cumprir ordem judicial de fornecimento do conteúdo da conversa de determinados usuários. A questão que deriva desse cenário é espelho daquela debatida nas *crypto wars* estadunidenses: o que deve acontecer se o provedor de aplicações não for tecnicamente capaz de fornecer esses conteúdos?

2.2 BLOQUEIOS DO WHATSAPP EM 2015 E 2016

Entre dezembro de 2015 e julho de 2016, o aplicativo de mensagens WhatsApp foi bloqueado em todo o território nacional em três ocasiões distintas[35]. De forma geral, os bloqueios foram decretados como sanção ao não cumprimento de determinadas ordens judiciais, que solicitaram que o aplicativo fornecesse o conteúdo de conversas de seus usuários a órgãos de investigação[36]. Vale dizer, os casos judiciais por trás de todas essas ordens de bloqueio estão em segredo de justiça, não sendo possível precisar as situações fáticas que ensejaram os pedidos de fornecimento de dados, mas ao menos dois casos tratavam, de forma geral, de tráfico de drogas[37].

O **primeiro bloqueio** do aplicativo ocorreu em 16 de dezembro de 2015, a partir de uma decisão expedida pela juíza Sandra Marques, da 1ª Vara de São Bernardo do Campo[38]. O bloqueio do aplicativo perdurou por mais de 10 horas, até o Tribunal de Justiça de São Paulo acatar um pedido de liminar elaborado pelo WhatsApp e suspender o bloqueio.

O **segundo bloqueio** ocorreu em dois de maio de 2016, após ordem do juiz Marcel Montalvão, da Comarca de Lagarto, em Sergipe. Neste caso, em específico, a ordem de bloqueio foi disponibilizada[39], e a investigação judicial em questão tratava-se de uma suposta rede interestadual de tráfico de drogas que utilizava o aplicativo como forma de comunicação. O juiz requereu a suspensão do aplicativo pelo prazo de 72 horas, mas uma nova liminar foi apresentada pelo WhatsApp e o bloqueio foi suspenso após cerca de 24 horas. Vale dizer, ainda, que em março do mesmo ano,

[35] Cf. o portal Bloqueios.Info, do Internetlab, para acesso a informações mais detalhadas e outros documentos relativos aos bloqueios de aplicativos no Brasil. Disponível em: <bloqueios.info> Acesso em: 15 abr. 2018.
[36] De forma geral, cf. ABREU (2017).
[37] Sobre o primeiro bloqueio, cf. Drogas e PCC: entenda o que levou ao bloqueio do WhatsApp. **Jornal A Tarde**, 17 dez. 2015. Disponível em: <https://goo.gl/bmQir3>; segundo bloqueio, cf. Motivo de novo bloqueio do WhatsApp é o mesmo que levou executivo do Facebook à prisão. **BBC Brasil**, 2 fev. 2016. Diponível em: <https://goo.gl/Y9VTDY>. Acessos em: 17 abr. 2018.
[38] Cf. <https://goo.gl/ysPvw6>. Acesso em: 18 abr. 2018.
[39] Cf. **Decisão de suspensão do aplicativo 'WhatsApp'**. Processo nº 201655090143/SE. Juiz de Direito Marcel Maia Montalvão. Proferida em 26 de abril de 2016. Disponível em: <https://goo.gl/buCNwi>. Acesso em: 18 abr. 2018.

uma outra sanção havia sido imposta ao Facebook Brasil (empresa do mesmo grupo econômico do WhatsApp) em resposta ao não fornecimento de dados: a prisão do vice-presidente da empresa[40].

Logo após este segundo bloqueio, duas ações foram ajuizadas no Supremo Tribunal Federal em relação ao bloqueio de aplicativo como modalidade de sanção ao descumprimento de ordem judicial: (i) a **ADPF 403**[41], que afirma que a própria possibilidade de bloqueio de aplicativo como sanção seria inconstitucional por si só, violando o direito constitucionalmente garantido à livre comunicação; e (ii) a **ADI 5527**[42], que alega que os dispositivos do MCI utilizados para embasar os bloqueios (incisos III e IV do artigo 12) seriam inconstitucionais.

Por fim, o **terceiro bloqueio** ocorreu em 19 de julho de 2016, após ordem judicial expedida pela juíza Daniela Barbosa, da 2ª Vara Criminal do Rio de Janeiro, Comarca de Duque de Caxias. O bloqueio durou apenas quatro horas, uma vez que o pedido de liminar que solicitava a suspensão dos bloqueios de forma geral, contido na inicial da ADPF 403, fora concedido pelo Ministro Ricardo Lewandowski[43].

Ao longo das decisões de bloqueio, a questão da criptografia foi abordada de forma direta. A última decisão judicial que solicitou o bloqueio, por exemplo, tratou diretamente da necessidade de impor uma solução técnica para viabilizar o acesso de autoridades judiciais a conteúdo criptografado. Nas palavras da juíza Daniela Souza[44]:

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

Dois pontos em comum podem ser identificados em relação a todas as solicitações de bloqueio: em primeiro lugar, todas as ordens de bloqueio foram concedidas por juízes da primeira instância; em segundo lugar, todas foram imediatamente revertidos em instâncias superiores. Com o ajuizamento das duas ações no STF, foi repassada a esta Corte a função de dar uma resposta final em relação à constitucionalidade dos bloqueios (LIGUORI FILHO, 2017).

[40] Polícia prende vice-presidente do Facebook na América Latina em SP. **G1**, 1 mar. 2016. Disponível em: <https://goo.gl/wO6FY2>. Acesso em: 19 abr. 2018.
[41] A petição inicial referente à **ADPF 403** está disponível em: <https://goo.gl/VYZJqX>. Acesso em: 16 abr. 2018.
[42] A petição inicial referente à **ADI 5537** está disponível em: <https://goo.gl/ZnJAS9>. Acesso em: 20 abr. 2018.
[43] **Medida Cautelar na Arguição de Descumprimento de Preceito Fundamental 403/SE**. Min. Ricardo Lewandowski. Disponível em: <https://goo.gl/p73pQT>. Acesso em: 20 abr. 2018.
[44] Cf. **Inquérito Policial n. 062-00164/2016**, PJERJ, 2a Vara Criminal de Duque de Caxias, Relatora: Daniela Barbosa Asumpção de Souza. Decisão proferida em 19/06/2016.

Dois foram os principais motivos alegados pelo WhatsApp para o não fornecimento dos conteúdos de conversas de seus usuários: (1) de um lado, a empresa não armazena o conteúdo das conversas de seus usuários, e não haveria dispositivo legal que a obrigue a isto; (2) de outro lado, a partir de abril de 2016, o aplicativo passou a utilizar **criptografia de ponta a ponta** em seus serviços; como já mencionado, isso significa que somente o emissor e o destinatário conseguem acessar o conteúdo em *plaintext*, sendo tecnicamente impossível, dentro desse sistema, que o aplicativo tenha acesso a esses conteúdos.

Devido à natureza técnica e similaridade entre o conteúdo das ações supramencionadas, o STF convocou uma audiência pública conjunta. Ainda que o objeto principal das ações trate da constitucionalidade dos bloqueios de aplicativos – seja de forma geral, seja relacionada aos dispositivos do Marco Civil –, a Decisão de Convocação da Audiência Pública optou por priorizar a discussão técnica em relação à possibilidade técnica de fornecimento dos dados e sistemas criptográficos[45].

Nesse sentido, o debate sobre regulação da criptografia no Brasil (i) derivou de um debate anterior sobre a constitucionalidade de uma modalidade de sanção por descumprimento de ordem judicial; (ii) foi judicializado no Supremo Tribunal Federal; e (iii) contou com uma audiência pública específica, com participação de diversos setores da sociedade, na qual se enfatizaram os limites técnicos e jurídicos da regulação da criptografia.

2.3 AUDIÊNCIA PÚBLICA NO STF E REGULAÇÃO DA CRIPTOGRAFIA

Nos dias dois e cinco de junho de 2017, a audiência pública foi realizada no Supremo Tribunal Federal para debater aspectos jurídicos e técnicos sobre os bloqueios de aplicativos como forma de sanção e, de forma geral, a questão do acesso a dados criptografados no contexto de investigações criminais. Trinta expositores[46] de diferentes setores da sociedade (academia, terceiro

[45] As perguntas que constaram na convocação 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 [sic] no aplicativo para outro celular/*smartphone* ou computador, permitindo que se implementasse ordem judicial de interceptação em face de um usuário específico?". Disponível em: <https://goo.gl/RLsC33>. Acesso em: 16 abr. 2018.

[46] As seguintes instituições participaram da audiência pública: Polícia Federal; WhatsApp Inc.; MPF, Facebook NIC.br, University of Washington-Tacoma; Instituto de Computação da Unicamp; Departamento de Engenharia de Computação

setor, empresarial, governo e comunidade técnica) contribuíram nos dois dias de audiência, totalizando cerca de nove horas de exposições.

Não é objeto do presente artigo mapear de forma detalhada todos os tópicos e posições debatidos ao longo das sessões[47], mas sim identificar e expor de forma breve os principais pontos de discussão acerca da regulação jurídica da criptografia na audiência. Nesse sentido, podemos apontar três aspectos principais do debate: possibilidade técnica, constitucionalidade dos bloqueios e proporcionalidade da imposição de medidas restritivas no sistema criptográfico – três pontos que aproximam o conteúdo do debate brasileiro ao estadunidense.

Em relação à **possibilidade técnica** do acesso a dados no contexto de sistemas dotados de criptografia forte (como a criptografia ponta a ponta), o debate centrou-se na possibilidade de "quebra" deste tipo de criptografia, de forma a viabilizar o cumprimento das ordens judiciais. De forma geral, os especialistas técnicos[48] reiteraram a inexistência de falhas de segurança no protocolo Signal, utilizado pelo WhatsApp, corroborando a tese da impossibilidade técnica de acesso ao conteúdo criptografado no sistema atual.

Em face disso, tratou-se da possibilidade de alteração do mecanismo do WhatsApp de forma a viabilizar o fornecimento de dados. Neste sentido, discutiu-se a **constitucionalidade** (e legalidade, de forma geral) desta possível imposição para fins de investigação policial. De um lado, apontando-se para a necessidade de acesso às provas como forma de manutenção da segurança pública; de outro, indicando a importância da integridade de sistemas criptográficos para a manutenção de diversos direitos fundamentais no âmbito digital, como privacidade e liberdade de expressão (ABREU, 2017, p. 35).

e Sistemas Digitais da POLI–USP; Insper; Assespro; Internetlab; ITS Rio; MCTIC; Febratel; Laboratório de Pesquisa Direito Privado e Internet da Universidade de Brasília – UnB; AMB; CTS-FGV; CPQD; IASP; Ibidem; NDIT-USP; Idec e Centro de Competência em Software Livre IME-USP.

[47] Neste sentido, cf. LIGUORI FILHO (2017) para um mapeamento resumido e a própria transcrição oficial da Audiência para um panorama mais detalhado. Disponível em: <https://goo.gl/sZ2Qqc>. Acesso em: 16 abr. 2018.

[48] Anderson Nascimento, professor da Universidade de Washington: "[…] depois de estudado, por diversos grupos ao redor do mundo, o entendimento da comunidade científica de criptografia é que o Signal, como se encontra hoje, o protocolo em si, é seguro. […] [O] entendimento da comunidade, no momento, é que não existe uma vulnerabilidade aparente no protocolo. Então não podemos quebrar a criptografia forte.". Marcos Simplício, professor de ciência da computação da POLI-USP: "[…] a comunidade científica fez várias auditorias do WhatsApp, em si, e do protocolo *signal*. Então, é consenso na comunidade que, dificilmente, seria fácil trocar o protocolo que está sendo executado ali - logo, existe, sim, uma certa auditoria do próprio protocolo, pelo menos até onde se sabe -, e que não tem nenhuma porta dos fundos já no aplicativo. Não foi inserido jamais algo dessa natureza, também conforme as várias análises que foram feitas por pessoas independentes aí da comunidade científica". Transcrição disponível em: <https://goo.gl/sZ2Qqc>. Acesso em: 17 abr. 2018.

Diretamente relacionado à constitucionalidade, abordou-se de forma superficial, ainda, a **proporcionalidade** da imposição deste tipo de medida ante outros direitos que podem vir a ser prejudicados em consequência desta imposição.

De um lado, colocou-se que o direito à segurança pública se sobreporia ao direito à privacidade dos usuários, afirmando que o sistema não poderia viabilizar "um paraíso digital, em que criminosos possam cometer infrações penais, violando direitos fundamentais tão importantes quanto o direito à privacidade"[49]. Em oposição a essa visão, apontou-se para diversas outras formas de investigação menos prejudiciais, como análise de metadados, infiltração policial e o chamado *government hacking*, em que a própria autoridade de investigação explora vulnerabilidades preexistentes em sistemas – ainda que este último deva ser tratado com bastante cautela.

O caso é bastante emblemático: uma decisão do STF que venha a julgar constitucional a medida de bloqueio e obrigue o fornecimento dos conteúdos das conversas compartilhadas pelo serviço – que utiliza criptografia ponta a ponta – pode gerar consequências diretas na adoção de criptografia forte por estes serviços.

As decisões, no entanto, não necessariamente esgotarão o debate. Caso o tribunal entenda pela constitucionalidade da medida sancionatória, não necessariamente os aplicativos que utilizam criptografia forte serão obrigados a inserir mecanismos de acesso excepcional para autoridades de investigação policial; assim como uma decisão contra os bloqueios não implicará uma "blindagem jurídica" da criptografia. No entanto, ela pode (e provavelmente irá) orientar os futuros rumos do debate.

Enquanto a decisão não se materializa, autoridades brasileiras começaram a investigar a possibilidade técnica de quebra da criptografia do serviço[50], a indicar a intenção de elaborar projetos para regulação do mecanismo[51] e até mesmo a questionar a constitucionalidade deste tipo de criptografia[52].

Na Câmara dos Deputados, o **PL 9.808**[53] foi apresentado em março de 2018. De autoria do deputado João Campos, o projeto propõe a inclusão de dois parágrafos (5º e 6º) no art. 10 do MCI. O

[49] Cf. Ministério Público defende aplicação de sanções previstas no Marco Civil da Internet ao WhatsApp, **STF Notícias**, 2 jun. 2017. Disponível em: <https://goo.gl/9SPRiJ>. Acesso em: 10 abr. 2018.
[50] MPF Investiga se a criptografia do WhatsApp permite a quebra de sigilo por parte das autoridades judiciais do país. **MPF - Sala de imprensa**, 3 maio 2016. Disponível em: <https://goo.gl/rzONw6>. Acesso em: 5 maio 2018.
[51] Governo elabora projeto para regular acesso às informações do WhatsApp. **O Globo**, 19 jul. 2016. Disponível em: <https://goo.gl/Er1D5B>. Acesso em: 10 abr. 2018.
[52] MPF investiga possível inconstitucionalidade da criptografia do WhatsApp. **Tecmundo**, 6 maio 2016. Disponível em: <https://goo.gl/nqeJp1>. Acesso em: 10 abr. 2018.
[53] Inteiro teor do projeto de lei disponível em: <https://goo.gl/M74muw>. Acesso em: 20 abr. 2018.

primeiro deles garantiria à autoridade policial o direito de acessar os conteúdos de dispositivo móvel sem autorização judicial, em casos de "situação flagrante de crimes definidos em lei como hediondo, tráfico de drogas ou terrorismo". O segundo parágrafo proposto[54] propõe explicitamente uma abordagem regulatória restritiva à criptografia, obrigando, de forma ampla, que os aplicativos de comunicação forneçam "chave criptográfica" para acesso aos conteúdos. No entanto, a simples leitura do dispositivo não fornece respostas para situações em que o fornecimento da chave é tecnicamente impossível por parte do provedor de aplicação, como na criptografia ponta a ponta.

Curiosamente, de outro lado, em meados de 2016 foi sancionado o decreto regulamentador do Marco Civil da Internet, o **Decreto n. 8771/16**. Ainda que ele não estabeleça nenhum mecanismo de regulação do desenvolvimento da criptografia e tampouco prescreva obrigações oponíveis a provedores de aplicação ou usuários sobre utilização da mesma, ele aborda a técnica em seu artigo 13, IV, recomendando a adoção de sistemas de encriptação por provedores de aplicação na guarda, armazenamento e tratamento de dados pessoais e comunicações privadas:

> Art. 13. Os provedores de conexão e de aplicações devem, na guarda, armazenamento e tratamento de dados pessoais e comunicações privadas, observar as seguintes diretrizes sobre padrões de segurança:
> […]
> IV - o uso de soluções de gestão dos registros por meio de técnicas que garantam a inviolabilidade dos dados, como **encriptação** ou medidas de proteção equivalentes. (Grifo nosso).

No momento da elaboração deste artigo, a vertente judicial das *crypto wars* brasileiras encontra-se em uma espécie de pausa temporária até a iminente decisão do Supremo Tribunal Federal.

3 QUESTÕES IMPORTANTES PARA OS PRÓXIMOS PASSOS

Após a exposição de ambos os conflitos, é tentador compará-los com profundidade para além das semelhanças e diferenças já mencionadas. De forma a adequar a análise às finalidades do presente artigo, porém, nos limitaremos a apontar algumas questões que devem ser levadas em consideração

[54] "§ 6º - No caso do parágrafo anterior, **em se tratando de dados criptografados, poderá o delegado de polícia requisitar, diretamente aos provedores de internet, provedores de conteúdo e autores de aplicativos de comunicação, o fornecimento de chave criptográfica que permita o acesso aos dados e conteúdos de comunicação privada de dispositivo móvel**, sem prejuízo do desenvolvimento e emprego, pelas polícias judiciárias, de técnicas e ferramentas tecnológicas que atinjam esse fim específico, incluindo a utilização de dispositivos que possibilitem o acesso a conteúdo anterior à criptografia por meio de aplicativos, sistemas ou outras ferramentas". (Grifo nosso).

por aqueles que buscam respostas para o conflito brasileiro comparando-o com a experiência estadunidense.

Nos referimos a ambos os debates como *crypto wars* pois os conflitos que os motivaram são extremamente semelhantes: em ambos os países a popularização do uso de sistemas de criptografia forte se tornou um obstáculo para autoridades que investigam crimes e exercem atividades de inteligência. Mais recentemente, o conflito gira em torno do uso de ferramentas que impedem que dados sejam obtidos mesmo com a anuência da empresa desenvolvedora do dispositivo ou do serviço de comunicação criptografado. Nesse sentido, muitos dos argumentos favoráveis ou contrários à limitação da adoção de criptografia forte por empresas de tecnologia são aplicáveis a ambos os conflitos, mas algumas divergências e omissões merecem destaque.

Em primeiro lugar, as preocupações externadas pelas autoridades de cada país divergem em alguns pontos. Como evidencia o caso Apple v. FBI, as autoridades estadunidenses declararam oposição principalmente ao uso de criptografia de dados estáticos, ou seja, aquela que protege informações contidas em um dispositivo, e não em fluxo de comunicações. Ainda que nos anos 90 o governo americano tenha temido a perda de sua capacidade de interceptar comunicações (daí a preferência por iniciativas como o *Clipper Chip*), a principal preocupação demonstrada após 2014 é a de que órgãos como o FBI possam perder permanentemente sua capacidade de extrair informações de dispositivos já apreendidos no contexto de uma investigação.

No Brasil, as autoridades encontraram obstáculo no uso por particulares de serviços de comunicação que adotaram criptografia ponta a ponta, como o WhatsApp. Os bloqueios do aplicativo revelam que em nosso país o foco do debate não é o escrutínio de celulares já apreendidos pelas autoridades, mas a interceptação em tempo real de trocas de mensagens, interceptação essa que se mostra tecnicamente impraticável enquanto persiste a adoção de criptografia ponta a ponta. Importante, portanto, que qualquer trabalho que busque transpor argumentos do debate estadunidense para o debate brasileiro se atente para as diferenças entre essas tecnologias.

Um segundo ponto de divergência entre as *crypto wars* se relaciona justamente a como as autoridades compreendem o funcionamento de ferramentas de criptografia. Nos EUA, as manifestações públicas de James Comey, Christopher Wray e Rod Rosenstein deixaram claro que os atores envolvidos reconhecem que as empresas de tecnologia, ao implementarem ferramentas atualizadas de criptografia em seus dispositivos, abandonaram sua capacidade técnica de cooperar com as autoridades. Assim, o debate estadunidense passou para uma fase seguinte, em que se discute se as empresas devem ou não enfraquecer sua criptografia para satisfazer as necessidades de investigação das autoridades (principalmente por meio da inserção de *backdoors* em seus serviços).

Em terras nacionais o debate ainda é bastante imaturo. Como apontamos anteriormente, a audiência pública convocada pelo STF teve como principal objetivo (evidenciado pelas perguntas feitas aos expositores convidados) a elucidação dos limites técnicos à interceptação que resultam da adoção de criptografia ponta a ponta. Nota-se, assim, que os principais responsáveis pela iminente tomada de decisões relevantes para as *crypto wars* brasileiras ainda não reconhecem que diversos provedores de aplicação não mais detêm a capacidade técnica de fornecer informações criptografadas, questão essa que parece superada no debate estadunidense.

Esse descompasso não só afeta o Judiciário, como também tem reflexos na produção legislativa sobre o tema: o já mencionado PL 9.808/18 falha em trazer qualquer solução para o problema de incapacidade técnica de fornecimento de dados. Desnecessário afirmar que devemos priorizar a superação desse descompasso o quanto antes, permitindo que o debate brasileiro prossiga de forma qualificada e atualizada.

Por fim, merece menção uma questão que tem tido pouco destaque tanto no debate estadunidense quanto no debate brasileiro, mas que, ao nosso ver, deveria despertar maior preocupação por parte dos atores envolvidos. Diferentemente de diversos outros debates regulatórios, cujos efeitos práticos costumam se limitar ao território do Estado regulador, a limitação do desenvolvimento, do uso e do comércio de criptografia em qualquer país provavelmente terá efeitos ao redor do planeta. Exemplo desse fenômeno é o que se denomina "problema do país menos confiável" (*least trusted country problem)* (SWIRE; AHMAD, 2012, p. 457).

Quando lembramos que um mesmo serviço de comunicação costuma ser utilizado em vários países e que as comunicações via internet quase sempre atravessam fronteiras, podemos perceber como a regulação da criptografia em um país pode criar uma falha de segurança que afeta todos os outros que utilizam um mesmo sistema de comunicação. Se um país proíbe criptografia eficaz ou impõe vulnerabilidades aos serviços utilizados em seu território, então a comunicação que parte desse país ou passa por sua infraestrutura estará necessariamente menos segura. Afirma-se, nesse sentido, que um sistema de comunicação internacional é tão seguro quanto o país mais restritivo envolvido permite que ele seja (SWIRE; AHMAD, 2012, p. 459).

Assim, qualquer autoridade com a pretensão de estabelecer limites para o uso, o desenvolvimento ou o comércio de criptografia eficaz deve estar consciente de que suas decisões afetarão mais do que seu território nacional, sua soberania ou sua jurisdição. Se empresas como a Apple forem obrigadas a enfraquecer suas ferramentas de criptografia nos Estados Unidos, então as comunicações que partem de celulares americanos serão menos seguras. Da mesma forma, se uma decisão do STF implicar a restrição à adoção de criptografia ponta a ponta por aplicativos como o

WhatsApp, toda comunicação que partir de um usuário brasileiro será necessariamente menos segura, independentemente da localização do remetente.

4 CONSIDERAÇÕES FINAIS

O debate é complexo e delicado. Independentemente da abordagem, uma eventual regulação do mecanismo, de forma a garantir acesso governamental a dados, poderá gerar efeitos negativos não apenas à segurança e privacidade de usuários sujeitos a ela, mas também àqueles além das fronteiras nacionais. É absolutamente necessário, por parte de legisladores e demais operadores do direito, uma abordagem interdisciplinar do tema para condução dessas discussões, seja para compreender os impactos de uma eventual regulação em outros direitos viabilizados pela criptografia, como privacidade e proteção de dados, seja para compreender os limites da eficácia de determinadas imposições, de modo a não se repetir, novamente, o imbróglio do *Clipper Chip* da década de 1990.

Diversas autoridades governamentais manifestaram-se acerca do debate sobre regulação da criptografia e acesso governamental a dados ao redor do mundo. Alguns, como o Gabinete Holandês, braço principal do Poder Executivo, manifestaram-se contra restrições à criptografia forte, promovendo-a[55]. Outros, como o primeiro ministro australiano, manifestaram-se a favor de restrições[56]. Não há como prever os próximos passos da discussão nos Estados Unidos e tampouco o impacto da futura decisão do STF no Brasil, restando aguardar as cenas dos próximos capítulos.

REFERÊNCIAS

ABELSON, Harold et al. Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications. In **Communications of the ACM**, v. 58, n. 10, p. 24-26, 2015.

ABELSON, Harold et al. **The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption**. 1997.

ABREU, Jacqueline de Souza. Passado, presente e futuro da criptografia forte: desenvolvimento tecnológico e regulação. **Revista Brasileira de Políticas Públicas**, v. 7, n. 3, 2017, p. 25-42.

[55] Dutch Government: Encryption good, backdoors bad. **Ars Technica**, 6 jan. 2016. Disponível em: <https://goo.gl/NrR2zR>. Acesso em: 6 maio 2018.

[56] Coletiva de imprensa realizada por Malcolm Turnbull, primeiro ministro australiano, no dia 14 de julho de 2017. Transcrição completa oficial disponível em: <https://goo.gl/7E6Ca8>. Acesso em: 5 maio 2018.

BARR, Allen Cook. Guardians of Your Galaxy S7: Encryption Backdoors and the First Amendment. **Minnesota Law Review**, v. 101, 2016.

BLAZE, Matt. **Protocol failure in the escrowed encryption standard**. ACM Press, 1994. Disponível em: <https://goo.gl/7Vibh3>. Acesso em: 29 mar. 2018.

DAM, K. W.; LIN, H.; NATIONAL RESEARCH COUNCIL (U.S.) (Ed.). **Cryptography's role in securing the information society**: Kenneth W. Dam and Herbert S. Lin, editors. Washington, DC: National Academy Press, 1996.

DIFFIE, Whitfield; LANDAU, Susan. **The Export of Cryptography in the 20th Century and the 21st**. Palo Alto, 2005. Disponível em: <https://goo.gl/rSQVjm>. Acesso em: 7 abr. 2018.

GASSER, Urs et al. **Don't Panic**. Making Progress on the "Going Dark" Debate. [s.l.] Berkman Center for Internet & Society at Harvard University, 1 Feb. 2016. Disponível em: <https://goo.gl/nCFoHK>. Acesso em: 20 abr. 2018.

LEONARDI, Marcel. **Tutela e Privacidade na Internet**. São Paulo: Saraiva, 2012.

LEVY, Steven. **Crypto**: How the code rebels beat the government – saving privacy in the digital age. New York: Penguin Books, 2002.

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.

MARCACINI, Augusto Tavares Rosa. **Direito e Informática**: uma abordagem jurídica sobre a criptografia. Rio de Janeiro: Forense, 2002.

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.

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

RICE, E. The Second Amendment and the Struggle Over Cryptography. **Hastings Science and Technology Law Journal**, v. 9, n. 1, p. 29–88, 2017.

SOUZA, Carlos Affonso; BRANCO, Sérgio. WhatsApp bloqueado? A culpa não é do Marco Civil da Internet. **Open Democracy**, 2016. Disponível em: <https://goo.gl/nLe8Xe>. Acesso em: 20 abr. 2018.

SOUZA, Carlos Affonso; LEMOS, Ronaldo. **Marco Civil da Internet**: construção e aplicação. Rio de Janeiro: Editar, 2016.

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: 29 mar. 2018.

Carlos Augusto Liguori Filho
Coordenador de projetos e pesquisador no Centro de Ensino e Pesquisa em Inovação da Escola de Direito da Fundação Getúlio Vargas de São Paulo (FGV Direito SP). Doutorando em Filosofia e Teoria Geral do Direito pela Universidade de São Paulo. Mestre em Direito e Desenvolvimento pela FGV Direito SP. *E-mail*: liguori.carlos@gmail.com

João Pedro Favaretto Salvador
Pesquisador no Centro de Ensino e Pesquisa em Inovação da FGV Direito SP. Bacharel em Direito pela Universidade de São Paulo. *E-mail*: jopesfs@gmail.com