ISSN 1413-3873

Revista do Ministério Público
do Estado do Rio de Janeiro

Repositório autorizado de jurisprudência
do Egrégio Supremo Tribunal Federal
Registro nº 25/99, de 22/04/1999
DJU nº 72, de 16/04/1999, p.1

Repositório autorizado de jurisprudência
do Egrégio Superior Tribunal de Justiça
Registro nº 37 – Portaria nº 1, de 26/10/1998
DJU de 05/11/1998, p.137 - Registro retificado
Portaria nº 9, de 14/06/1999 – DJ 22/06/1999

nº 79 jan./mar. 2021

Acesso a dados criptografados no contexto de investigações criminais: o "estado da arte"

Access to encrypted data in the context of criminal investigations: the "state of the art"

Gustavo Eloi Razera*

Sumário

Resumo

Pretende-se com o presente artigo descrever e analisar o debate brasileiro a respeito do acesso judicialmente autorizado a dados criptografados para instrução de investigações criminais e a regulação jurídica da criptografia. Os argumentos apresentados no âmbito da audiência pública conjunta que precedeu o julgamento da ADI 5.527 e da ADPF 403 – palco principal da disputa acerca da imposição de limites ao uso da criptografia – foram reunidos e submetidos à análise crítica, privilegiando-se a abordagem consequencialista, com foco em possíveis impactos sociais. Uma vez admitida a premissa da inviabilidade técnica da interceptação de mensagens "às claras" em aplicativos que adotam a criptografia *end to end*, passou-se ao exame das propostas de regulação e respectivas objeções, assumindo-se uma tendência de uso progressivo de técnicas de encriptação e, diante disso, a necessidade premente de modernização dos órgãos de persecução, com o objetivo de manter, no longo prazo, a capacidade investigativa.

Abstract

This article is intended to describe and analyze the Brazilian debate regarding the judicially authorized access to encrypted data for the instruction of criminal investigations and the legal regulation of cryptography. The arguments presented at the joint public hearing that preceded the trial of ADI 5,527 and ADPF 403 – the main stage of the dispute over the imposition of limits on encryption – were brought together and submitted to critical analysis, with emphasis on the consequentialist approach, focusing on possible social

* Promotor de Justiça do Ministério Público do Estado do Paraná.

impacts. Once the premise of the technical unfeasibility of intercepting the "plaintext" in applications that adopt end to end cryptography was admitted, the proposals for regulation and the respective objections were examined, assuming a tendency of progressive use of encryption techniques and, in face of this, the pressing need for modernization of the law enforcement agencies as in order to maintain, in the long term, the capacity to investigate.

Palavras-chave: Criptografia. *WhatsApp*. Investigação criminal. Dados privados. Segurança.

Keywords: *Cryptography. Whatsapp. Criminal investigation. Private data. Security.*

1. Introdução

A "criptografia é uma técnica de preservação da privacidade, entendida classicamente como o direito de ser deixado em paz, ou de proteger uma certa informação pessoal" (ARANHA, 2017, p. 131)[1]. Implementada por meio de algoritmos matemáticos, *ela permite codificar dados de uma mensagem*, tornando-a ininteligível para um possível adversário.

Nas comunicações digitais, o emprego da criptografia já existe há um bom tempo, mas o acesso até então era restrito a poucas pessoas que detinham conhecimento técnico especializado para a sua implementação.

Esse quadro começou a se modificar significativamente em 2013, quando Eduard Snowden, ex-empregado da Agência de Segurança Nacional dos EUA (NSA), divulgou documentos que evidenciaram que o órgão do Departamento de Defesa possuía acesso a informações em massa dos usuários das mais conhecidas empresas de tecnologia para fins de inteligência[2].

As revelações de Snowden influenciaram o comportamento de pessoas, empresas e governos ao redor do mundo, erigindo, sobretudo, uma demanda acentuada por privacidade nas comunicações *online*. A proteção de dados do usuário tornou-se, assim, um grande ativo de mercado, o que acabou por transformar o cenário tecnológico.

Diante da demanda por privacidade, os provedores passaram a implementar a criptografia forte como padrão básico de segurança do serviço, chamada criptografia *by default*, um sistema criptográfico que se encontra ativo sem a necessidade de realização de qualquer comando pelo usuário. Até então, ainda que a adoção da

[1] Audiência Pública Conjunta, Marco Civil Da Internet, ADI 5.527 e Bloqueio Judicial do WhatsApp, ADPF 403. Ata. Disponível em: <https://bit.ly/3c3jDli>. Acesso em: 17 set. 2020.

[2] Sobre as revelações de Eduard Snowden a respeito do programa secreto de vigilância e espionagem americano ver: MACASKILL, E. et al. NSA files: decoded. *The Guardian*. Disponível em: <https://bit.ly/2ZHLvXt>. Acesso em: 17 set. 2020.

criptografia estivesse ao alcance do usuário, ela era opcional e, na maioria dos casos, exigia uma atitude proativa.

Evidentemente, o advento da criptografia forte por padrão de segurança representou clara e importante mudança, que intensificou os problemas de investigação, afinal a capacidade de monitoramento e de interceptação de mensagens é tida como uma das principais formas de se apurar ilícitos, por vezes a única.

Não demorou muito para que autoridades se insurgissem contra as empresas de tecnologia. Foi o caso do então diretor do *Federal Bureau of Investigation* (FBI), James Comey, responsável por uma das mais célebres falas contrárias ao uso da criptografia forte *by default*, ao afirmar que, por impedir o acesso a dados em repouso e a dados de comunicações em trânsito, a sua adoção desenfreada tornou inviável o trabalho investigativo, fenômeno que ele chamou de "*Going Dark*"[3].

Com a utilização, mais comum a cada dia, de mecanismos criptográficos para comunicação *online* e armazenamento de dados, as frequentes dificuldades enfrentadas no contexto de investigações criminais ensejaram debates em diversos países a respeito da necessidade de impor restrições à criptografia[4].

2. A regulação jurídica da criptografia, debate brasileiro

No Brasil, o debate a respeito da regulação da criptografia surge pela primeira vez no Judiciário, após sucessivas decisões judiciais determinando bloqueios do aplicativo *WhatsApp*[5]. Em um intervalo de apenas oito meses, entre 2015 e 2016, o serviço de mensagens instantâneas e chamadas de voz *WhatsApp* teve suas atividades suspensas por três vezes: (i) em dezembro de 2015, por ordem de um juiz do Estado de São Paulo; (ii) em fevereiro de 2016, por um juiz do Estado de Alagoas; e (iii) em julho de 2016, por ordem de uma juíza do Estado do Rio de Janeiro.

Houve, ainda, uma ordem de bloqueio em fevereiro de 2015, da Justiça do Piauí, e outra em maio de 2016, por um juiz de Sergipe, ambas cassadas antes da implementação.

---

[3] O discurso do Diretor do FBI recorre às consequências da disseminação de criptografia forte para as investigações e as relaciona aos impactos na segurança pública, destacando as dificuldades na prevenção e repressão a crimes e, sobretudo, ataques terroristas. 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://bit.ly/32DztQN >. Acesso em: 17 set. 2020.

[4] Para uma visão abrangente acerca de como os demais países têm enfrentado o tema regulação da criptografia, confira-se o resultado da pesquisa realizada pelo Centro de Ensino e Pesquisa em Inovação (CEPI) da FGV Direito SP "Criptografia e Direito: uma perspectiva comparada". Disponível em: < https://bit.ly/33zN0rS >. A pesquisa buscou mapear o debate internacional sobre acesso a dados criptografados por autoridades de investigação e privacidade, identificando tendências e modelos regulatórios de criptografia ao redor do mundo. Os dois principais produtos da pesquisa são: a *Criptopédia* e *o CryptoMap*, site e mapa interativo que compilam de forma prática as informações a respeito dos 40 países estudados.

[5] Informações detalhadas sobre o histórico de bloqueios de aplicações de Internet no Brasil desde 2007 podem ser consultadas no portal Bloqueios.Info, do Internetlab. Disponível em: http://bloqueios.info/pt/linha-do-tempo/.

O juiz subscritor dessa última ordem é o mesmo que, em março de 2016, chegara a ordenar a prisão do diretor do *Facebook* no Brasil por descumprir decisão judicial[6].

Os bloqueios se deram como sanção ao provedor de aplicação, por não fornecer o conteúdo das mensagens de usuários investigados.

Inicialmente, a resistência em cumprir as decisões judiciais veiculava os mais variados argumentos, como o fato da empresa ter sede no exterior e servidores em outros países, ou das intimações judiciais terem sido endereçadas ao *Facebook,* que supostamente não teria representação legal ou contratual para responder pelo *WhatsApp*. Somente mais tarde sobreveio o argumento principal: a incapacidade técnica de cumprir a decisão, em virtude do modelo criptográfico implementado.

No entanto, não havia consenso acerca do protocolo criptográfico adotado pelo *WhatsApp* e o provedor era pouco transparente a respeito.

Alicerçados em interpretação conferida a dispositivos do Marco Civil da Internet (Lei nº 12.965, de 23 de abril de 2014), os bloqueios foram contestados no Supremo Tribunal Federal mediante ações de controle concentrado de constitucionalidade: (i) a Ação Direta de Inconstitucionalidade (ADI) nº 5.527, sob a relatoria da Min. Rosa Weber, questiona dois artigos da Lei nº 12.965, de 23 de abril de 2014, mais precisamente o art. 10, em seu § 2º[7], e o art. 12, em seus incisos III e IV[8]; e (ii) a Arguição de Descumprimento de Preceito Fundamental (ADPF) nº 403, sob a relatoria do eminente Ministro Luiz Edson Fachin, discute a constitucionalidade de decisões que determinaram o bloqueio do *WhatsApp*.

Para dirimir as questões técnicas envolvidas no julgamento destas ações, os Ministros convocaram audiência pública conjunta[9], que contou com a contribuição *de 30 expositores, entre eles representantes do Ministério Público Federal, da Polícia Federal, do Conselho Federal da Ordem dos Advogados do Brasil, do Comitê Gestor da Internet no Brasil, e de inúmeras entidades civis, acadêmicos e até mesmo do cofundador do* WhatsApp.

A partir da participação plural e do aporte das diversas perspectivas dos atores envolvidos, houve notória expansão do tema proposto pelas ações de controle concentrado,

[6] Diego Jorge Dzodan, vice-presidente do *Facebook* na América Latina, teve a prisão decretada pelo juiz da Comarca de Lagarto, Sergipe, após a rede social não fornecer o conteúdo de mensagens trocadas por meio do aplicativo *WhatsApp,* descumprindo ordem judicial nesse sentido. A prisão ocorreu no dia 01.03.2016 e no dia seguinte foi reformada em sede de liminar em *habeas corpus*. (FAGUNDES, I.; SENRA, R. *Executivo do Facebook é libertado em SP*. BBC Brasil, São Paulo, 02 de março de 2016. Disponível em: < https://bbc.in/2FEcRqn >. Acesso em: 17 set. 2020).

[7] 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. […] § 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.

[8] Art. 12. Sem prejuízo das demais sanções cíveis, criminais ou administrativas, as infrações às normas previstas nos arts. 10 e 11 ficam sujeitas, conforme o caso, às seguintes sanções, aplicadas de forma isolada ou cumulativa: […] III - suspensão temporária das atividades que envolvam os atos previstos no art. 11; ou IV - proibição de exercício das atividades que envolvam os atos previstos no art. 11.

[9] A audiência pública para o julgamento das ações de controle concentrado ADI 5.527 e ADPF 403 foi realizada entre os dias 02 e 05 do mês de junho de 2017. A gravação audiovisual encontra-se disponível em: https://www.youtube.com/watch?v=3TNsQCNIOO0&t=8s.

que originariamente pretendiam discutir a constitucionalidade da imposição das sanções judiciais de bloqueio a aplicativos de Internet, e passaram a pautar o debate em torno do funcionamento da criptografia e limites do direito frente a ela.

3. A criptografia *end to end* e a (in)capacidade técnica de promover interceptação

A chamada criptografia *end to end* ou de ponta a ponta é uma técnica criptográfica que importa na cifragem do dado em trânsito do início ao fim da comunicação, o que impossibilita a revelação de seu conteúdo no caminho, até mesmo pelo provedor que viabiliza a troca das mensagens[10].

Do ponto de vista da técnica criptográfica, qualquer entidade que está no canal de comunicação, e mesmo aquela que possui o controle parcial ou total dele, é vista como adversário. Por isso faz completo sentido para o projetista do protocolo de comunicação encarar-se como um possível adversário – inclusive porque ele pode ser comprometido por um terceiro – e projetar o mecanismo de forma que ele próprio não tenha capacidade de interceptar mensagens (ARANHA, 2017, p. 130)[11].

Para melhor entender o contexto da implementação desse protocolo criptográfico pelas empresas de tecnologia, é importante voltar ao programa de vigilância (*surveillance*) americano revelado por Snowden, PRISM.

O PRISM, segundo as publicações que se encontravam na imprensa à época, coletava conteúdo de comunicações e metadados de usuários, mediante acesso direto da NSA aos servidores de grandes empresas que proveem comunicações privadas na *web*, incluindo *Google, Microsoft, Facebook, Yahoo* e *Apple,* isso tudo sem contar com mandados individuais de monitoramento[12].

---

[10] "Calcular e armazenar chaves criptográficas apenas nas pontas da comunicação simplifica uma aplicação criptográfica porque torna evidente quais são os principais pontos que exigem proteção, reduzindo a ameaça de pontos intermediários ou atacantes internos que operam o serviço e desfrutam de acesso privilegiado." (ARANHA, Diego de Freitas. O que é criptografia fim a fim e o que devemos fazer a respeito? *In*: DONEDA, Danilo; MACHADO, Diego (org.). *A criptografia no direito brasileiro*. São Paulo: Thomson Reuters Brasil, 2020, RB-1.3. E-book).

[11] Audiência Pública Conjunta, Marco Civil Da Internet, ADI 5.527 e Bloqueio Judicial do WhatsApp, ADPF 403. Ata. Disponível em: <https://bit.ly/3c3jDli>. Acesso em: 17 set. 2020.

[12] Extrai-se de matéria publicada no *The Washington Post*: "*The top-secret PRISM program allows the U.S. intelligence community to gain access from nine Internet companies to a wide range of digital information, including e-mails and stored data, on foreign targets operating outside the United States. The program is court-approved but does not require individual warrants. Instead, it operates under a broader authorization from federal judges who oversee the use of the Foreign Intelligence Surveillance Act (FISA).*" (*NSA slides explain the PRISM data-collection program*. *The Washington Post*. Washington D. C., 10 de julho de 2013. Disponível em: < https://wapo.st/2ZM9k0g >. Acesso em: 17 set. 2020). Tradução livre: O programa ultrassecreto PRISM permite que o centro de inteligência dos EUA obtenha acesso a uma ampla gama de informações digitais de nove empresas de Internet, incluindo *e-mails* e dados armazenados, sobre alvos operando fora dos Estados Unidos. O programa detém autorização judicial, mas não requer mandados individuais. Em vez disso, opera sob uma autorização mais ampla de juízes federais que supervisionam o uso do *Foreign Intelligence Surveillance Act* (FISA).

Tão logo o programa veio a público, as empresas listadas se apressaram em negar seu envolvimento com a agência de inteligência americana[13]*. Apesar disso, predominou na opinião pública a versão que sustentava a existência de uma espécie de colaboração secreta entre as empresas de tecnologia e o Governo. Isso fez com que os usuários passassem a desconfiar dos provedores, o que provocou relevante incremento na demanda por privacidade.*

Para responder à crise de confiança que pairava sobre eles, em virtude da aventada colaboração com os órgãos governamentais, os provedores passaram a implementar um protocolo criptográfico com característica especial, ponta a ponta / fim-a-fim / *end to end*, projetado para que as mensagens em seu conteúdo compreensível possam ser capturadas apenas nas pontas da comunicação (remetente e destinatário), o que impede que o próprio provedor recupere o seu conteúdo, ou "quebre", por assim dizer, a criptografia.

Com isso as empresas lograram transmitir aos usuários a ideia de que, mesmo que o Estado exija, o provedor de aplicação (responsável pelo fornecimento do serviço) não poderá informar o teor das suas comunicações, tornando-se, assim, insuscetível a ingerências e pressões externas.

Esse protocolo criptográfico de ponta a ponta vem se tornando mais comum a cada dia no mercado para aplicativos de troca segura de mensagens. Em abril de 2016 o WhatsApp *passou a adotar o protocolo* Signal[14]*, que por meio do emprego de criptografia assimétrica*[15]*, combinando o uso de chaves públicas e chaves privadas, garante que apenas emissor e destinatário (as "pontas" da comunicação) tenham acesso ao conteúdo inteligível das mensagens.*

Além disso, prevendo a hipótese de ataque exitoso às chaves criptográficas, o WhatsApp *adota o recurso denominado* forward secrecy[16]*, por meio do qual uma nova chave*

---

[13] Os pronunciamentos oficiais das empresas mencionadas podem ser consultados em: LEE, Timothy B. Here's everything we know about PRISM to date. *The Washington Post*. Washington D. C., 12 de junho de 2013. Disponível em: < https://wapo.st/3mEg4qX >. Acesso em: 17 set. 2020.

[14] No dia 05 de junho de 2016 o *Signal* anunciou a completa integração de seu protocolo criptográfico ao aplicativo de mensagens *WhatsApp*, e com ele a criptografia de ponta a ponta. (*WHATSAPP'S Signal Protocol integration is now complete*. Disponível em: < https://signal.org/blog/whatsapp-complete/ >. Acesso em: 17 set. de 2020).

[15] *"Ao tempo que na criptografia simétrica a mesma chave é utilizada para encriptar e desencriptar um arquivo qualquer, no método de criptografia assimétrica apenas o destinatário possui a chave capaz de efetivar a desencriptação. A encriptação é realizada por meio de um software específico, que recebe basicamente dois arquivos: o arquivo a ser encriptado e um outro, que é a chave pública do destinatário. Como se vê, este tipo de criptografia dispensa o envio prévio de uma chave secreta para o destinatário. Entretanto, é necessário que o destinatário disponibilize previamente sua chave pública em algum local para que o remetente a utilize para encriptar o arquivo a ser remetido"* (Brasil, Ministério Público Federal, Câmara de Revisão Criminal, 2. Roteiro de Atuação: Crimes Cibernéticos. 3ª edição. Brasília – DF, 2016, p. 302. E-book).

[16] *"Com o* forward secrecy, *uma nova chave é negociada a cada transação e as chaves de longo prazo são usadas somente para autenticação. Essas chaves de transação (ou sessão) são descartadas após cada transação – o que reduz significativamente a exposição de uma entidade que tenha sido comprometida. Quando um sistema com* forward secrecy *é usado, invasores que infringem uma rede e obtêm acesso às chaves só conseguirão desencriptar dados a partir do momento da violação até que esta seja descoberta e corrigida; os dados históricos permanecem seguros. Além disso, como as chaves de sessão são destruídas imediatamente após a conclusão de cada transação, o invasor deve inserir-se no processo de cada transação em tempo real para conseguir obter as chaves e comprometer os dados." (ABELSON, Harold et al.* Chaves Embaixo do Tapete*: exigências de acesso a todos os dados e comunicações*

é gerada a cada mensagem e, portanto, caso o atacante consiga comprometer a criptografia de uma mensagem, mesmo assim não terá acesso ao conteúdo de mensagens passadas[17].

Após a realização de diversas auditorias independentes, é consenso na comunidade científica que o protocolo Signal *é seguro e também a sua implementação feita pelo* WhatsApp *se deu de forma adequada.*

Desse modo, a partir da adoção do protocolo Signal *e da criptografia* end to end *pelo* WhatsApp*, passou a se tornar tecnicamente inviável a interceptação do conteúdo das mensagens às claras (*plaintext*), isto é, de forma inteligível.*

Estabelecida a premissa da inviabilidade técnica, a interceptação da mensagem para fins de investigação criminal exigiria o rebaixamento dos níveis de segurança adotados, mediante a implementação de falhas intencionais, chamadas de backdoor.

---

pelo governo geram insegurança. Tradução: SALES, R. et al. Instituto de Tecnologia e Sociedade do Rio (ITS Rio). Rio de Janeiro, 2018, p. 17. Disponível em: < https://bit.ly/35Nxuvc >. Acesso em: 17 set. 2020).

[17] A respeito do atual funcionamento do protocolo criptográfico do *WhatsApp*, vale recorrer à didática exposição do cofundador da empresa durante os debates da Audiência Pública, Brian Acton (2017, p. 31): "Num nível geral, todas as mensagens enviadas através do *WhatsApp* são garantidas, quanto à segurança, com um cadeado e uma chave. Só o emissor e o receptor é que têm as chaves necessárias para destrancar e ler as mensagens de *WhatsApp*. Como vou explicar, em maior detalhe, nós também acrescentamos outras características ao nosso sistema para que ele seja o estado da arte. Por exemplo, em vez de submeter todas as mensagens à criptografia de um usuário, com o mesmo cadeado e a mesma chave, no nosso sistema esse cadeado e essa chave mudam a cada mensagem. Incluímos também uma característica que dá, aos usuários, o poder de verificar a identidade e confirmar que outros não estejam lendo as suas mensagens. Observando a tela, os senhores poderão ver que a Ana instalou o *WhatsApp* no telefone dela. Ao fazer isso, o telefone dela gerou um par de chaves relacionadas matematicamente. Uma, é uma chave privada, armazenada unicamente no telefone dela. E a outra, é uma chave pública, que o telefone dela manda para o servidor de *WhatsApp*, para que o Bernardo, ou qualquer outra pessoa, possa usar. Da mesma maneira, o Bernardo instalou o *WhatsApp* no telefone dele, que manda também chaves públicas para o servidor para que a Ana possa usar para mandar mensagens para ele. Então, agora, a Ana quer mandar uma mensagem para o Bernardo. Em primeiro lugar, ela pede a chave pública do Bernardo, do servidor. E, depois, o telefone dela constrói o que nós chamamos de sessão. A sessão é o início de uma conversa criptografada. Para isso, o Bernardo e a Ana passam por uma troca compartilhada de chaves. Este método permite que dois usuários criem uma chave compartilhada para criptografia, através de um canal que não é seguro. O tipo de troca de chaves que nós usamos evita que uma terceira parte, incluindo o próprio *WhatsApp*, obtenha informação que permita a leitura da mensagem. Isso ocorre porque apenas os dois telefones, dos dois usuários, têm a informação correta para criptografar e retirar a criptografia das suas mensagens. Uma vez que a sessão é criada, eles podem começar a se comunicar com segurança e cada um dos seus telefones cria chaves de mensagens singulares com base num cálculo matemático. Portanto, se a Ana quer mandar uma mensagem para o Bernardo, o telefone dela vai criptografar a mensagem usando a chave. O sistema de criptografia do *WhatsApp* garante que cada mensagem tenha a sua própria chave de mensagem, que muda para toda a mensagem que é enviada. Portanto, como se pode observar pelo diagrama, depois que a mensagem é submetida à criptografia no telefone da Ana, o servidor transfere a mensagem para o Bernardo sob a forma criptografada. O servidor não consegue ler a mensagem, porque não tem a chave correta. Apenas o Bernardo é que tem a chave certa, armazenada apenas no telefone dele e em nenhum outro lugar. Quando a mensagem chega no telefone do Bernardo, o telefone dele tira a criptografia, usando a versão dele da chave de mensagem, armazenada apenas no telefone dele. Os dois lados da comunicação, nesse caso, a Ana e o Bernardo, usam o que nós chamamos de *ratchet* criptográfico. Especificamente um algoritmo de *ratchet* duplo, esse *ratchet* ou catraca garante que uma nova chave de sessão e uma nova chave de mensagem sejam sempre modificadas e recalculadas à medida que as mensagens fluem entre os dois usuários. É uma proteção importante, conhecida na comunidade de segurança como sigilo futuro. Isso significa que se as chaves de qualquer única mensagem forem comprometidas, as chaves não podem ser utilizadas para voltar e retirar a criptografia de mensagens já transmitidas." (Audiência Pública Conjunta, Marco Civil Da Internet, ADI 5.527 e Bloqueio Judicial do *WhatsApp*, ADPF 403. Ata. Disponível em: <https://bit.ly/3c3jDli>. Acesso em: 17 set. 2020).

Assim, a principal questão em debate no âmbito da audiência pública, e tema a ser enfrentado pelo Supremo nas ações de controle concentrado *(ADI 5.527 e ADPF 403)*, não é (i) se o *WhatsApp* (e outros aplicativos de *instant messenger*) teria a obrigação de colaborar com a investigação criminal, cedendo o teor das mensagens de um usuário específico em caso de decisão judicial, pois, dado o modelo criptográfico adotado, isso é impossível; mas sim (ii) se o próprio *WhatsApp* e as demais empresas de tecnologia estão autorizadas a comercializar produtos que proporcionem ao usuário ambientes de informação inacessíveis aos órgãos de investigação, e mais, se o Estado pode e deve exigir a criação de acessos privilegiados, permitindo a custódia das chaves criptográficas (*key scrow*) a terceiros autorizados.

4. A imposição de limites à criptografia: propostas e objeções

Uma vez que a implementação da criptografia *end to end* impossibilita a realização de interceptações telemáticas (a captura das conversas de alvos específicos em tempo real), e como os provedores de aplicação também não armazenam mensagens pretéritas em seus servidores, não é possível obter nenhum tipo de conteúdo de conversa no âmbito de investigações. A partir daí, a questão que se põe é: deve-se impor aos desenvolvedores de aplicativos de mensagens a obrigação de construírem a arquitetura de seus serviços de modo a permitir interceptações?

Trata-se de regular a criptografia, criando uma obrigação legal para mudança do protocolo criptográfico, com a implementação de uma vulnerabilidade intencional, uma backdoor *que possibilite o acesso de órgãos investigativos ao conteúdo de mensagens trocadas via aplicativo.*

O debate a respeito do acesso governamental a dados criptografados, que no Brasil teve como palco principal a mencionada audiência pública realizada pelo STF, pouco se afastou da tônica da disputa vista nos demais países, onde se tem, de um lado, as autoridades de aplicação da lei pressionando por mecanismos de acesso excepcional obrigatório aos sistemas de criptografia e, de outro, técnicos e acadêmicos do setor argumentando que essa solução compromete a segurança dos sistemas criptográficos e, consequentemente, a privacidade de seus usuários.

A resolução desse conflito passa pela formulação das perguntas corretas, a saber: (i) as soluções que se propõem contra a criptografia são eficazes, isto é, elas de fato resolvem o problema?; e (ii) os benefícios que a pretensa solução vai trazer são maiores do que os seus malefícios? É legítimo que o Estado busque tomar atitudes positivas para reduzir os problemas que a ferramenta aparenta estar causando, mas, para tanto, é elementar, porém necessário, que haja um certo equilíbrio, aferido pelo teste de proporcionalidade sugerido.

As propostas apresentadas pelos órgãos de Estado giram em torno do emprego do chamado "ataque *man-in-the-middle*". A proposição surge sob vários nomes, como chave dourada, porta da frente, porta do lado, *key escrow, backdoor, golden key, mas a ideia comum a todas é promover uma mudança de protocolo criptográfico para inserir*

uma falha intencional e, assim, permitir o acesso do terceiro autorizado, como se fosse mais uma sessão da conversa.

O acesso exclusivo especial, inclusive, já é objeto de projetos de lei que tramitam na Câmara dos Deputados: PL 9.808/18[18] e PL 10.372/18[19]. Ambos pretendem impor ao provedor uma obrigação genérica de fornecimento da chave criptográfica aos órgãos policiais.

Diversas são as objeções apresentadas pela comunidade científica.

A primeira delas diz respeito à proteção desta "porta dos fundos", desse acesso privilegiado. É dizer, além de a técnica criptográfica se preocupar com o canal de comunicação, como originalmente proposto, passaria a ser preciso também se preocupar com esse acesso, essa falha artificial injetada no protocolo criptográfico, que não cumpre o objetivo de segurança, e cujo controle impõe diversos obstáculos do ponto de vista logístico e de projeto (ARANHA, 2017, p. 135)[20].

Proteger essa porta dos fundos e prevenir que o propósito dela seja desvirtuado são desafios que se estabelecem, sobretudo porque esse acesso autorizado, ou essa chave-mestra, se tornaria um alvo extremamente valioso para cibercriminosos e até mesmo governos autoritários[21].

Além disso, com a criação da *backdoor* o operador do serviço precisará proteger o acesso excepcional também contra os seus próprios funcionários, que, até mesmo, podem ser coagidos ou atacados por terceiras partes e forçados a utilizar essa porta dos fundos para outros interesses[22].

---

[18] BRASIL. Câmara dos Deputados. *Projeto de lei nº 9.808, 20 de março de 2018*. Autor: João Campos. Câmara dos Deputados, Brasília, DF, 20 de mar. 2018. Disponível em: < https://bit.ly/3hlz5Vk >. Acesso em: 17 set. 2020.

[19] BRASIL. Câmara dos Deputados. *Projeto de lei nº 10.372, 06 de junho de 2018*. Autor: José Rocha. Câmara dos Deputados, Brasília, DF, 06 de jun. 2018. Disponível em: < https://bit.ly/3myty7y >. Acesso em: 17 set. 2020.

[20] Audiência Pública Conjunta, Marco Civil Da Internet, ADI 5.527 e Bloqueio Judicial do *WhatsApp*, ADPF 403. Ata. Disponível em: <https://bit.ly/3c3jDli>. Acesso em: 17 set. 2020.

[21] "Já no que se refere às dificuldades de manter esse acesso efetivamente 'excepcional', restrito às autoridades e às situações permitidas, ressalta-se o quanto *backdoors* se apresentam como alvos de extremo interesse. Seja pela atuação de hackers maliciosos, pela captura de algum agente com acesso a esses mecanismos ou por outro caminho, frequentemente se argumenta que a ponderação mais adequada aqui não é se a utilização indevida desses sistemas pode ocorrer, mas sim quando ela ocorrerá." (ALIMONTI, Veridiana. Criptografia, direitos e a problemática polarização entre "privacidade individual" e "segurança coletiva". *In*: DONEDA, Danilo; MACHADO, Diego (org.). *A criptografia no direito brasileiro*. São Paulo: Thomson Reuters Brasil, 2020, RB-3.1. E-book).

[22] "Tecnicamente, o mecanismo de interceptação legal pode se manifestar de várias maneiras, como exigir que partes comunicantes forneçam cópia de suas chaves para as autoridades ou forçar os operadores do serviço a montar ataques de espelhamento contra seus próprios usuários. Entretanto, uma característica é comum a todas essas alternativas. Introduzir uma nova ponta artificial na comunicação forçadamente equipada com cópia das chaves criptográficas para capturar mensagens, ainda que com autorização institucional, implica aumentar a superfície de ataque e tornar sistemas menos seguros. Além das pontas originais da comunicação que precisam ser protegidas, um novo ponto de intervenção acessível para um possível atacante agora precisa também ser protegido. […] A tarefa pode parecer simples em primeira análise, mas é importante considerar não apenas atacantes externos ao serviço, mas principalmente seus operadores. Criptografia fim a fim é implementada exatamente para proteger a integridade e sigilo de comunicações contra eventuais ladrões de dados, falsificadores de identidade, espiões e outras classes de criminosos que se infiltram nas organizações. A ameaça interna é preocupação crescente e frequentemente está associada a grandes fraudes, exatamente por fornecer acesso privilegiado aos meandros de um sistema. A ideia torna-se bem mais difícil de implementar ao se considerar que aplicativos de troca segura

Outro desafio não menos preocupante consistiria em harmonizar o acesso de múltiplos órgãos de persecução àquela porta dos fundos – problema que se potencializa no Brasil, com diversas instituições com competências concorrentes e sobrepostas.

A criação de uma *backdoor* não apenas se distancia de qualquer objetivo de segurança para as partes comunicantes, mas também, torna sistemas e procedimentos, necessariamente, mais complexos, criando mais vulnerabilidades.

"Na segurança digital, os dados ou são seguros de todo mundo ou seguros de ninguém" (ACTON, 2017, p. 31)[23], a frase dita pelo representante do *WhatsApp* em sua participação na audiência pública é pedagógica e adverte, qualquer ferramenta que permita ao Estado desabilitar a criptografia de conversas de criminosos investigados também pode ser voltada contra os demais usuários do serviço por partes hostis. Esse não é apenas um risco teórico, basta notar os numerosos e recorrentes ciberataques que fragilizam desde usuários comuns até polícias e agências estatais de inteligência[24].

Para além das importantes questões relacionadas à segurança desse acesso excepcional, mesmo considerando a hipótese de haver pleno êxito na sua implementação, a eficácia da medida é questionável, sob diversos aspectos.

Supondo a imposição da obrigação ao *WhatsApp* de criar um mecanismo de acesso autorizado para viabilizar a colaboração com investigações policiais, as pessoas podem simplesmente migrar de aplicativo. A propósito, existem centenas de ferramentas de comunicação que utilizam criptografia *end to end* – basta uma busca rápida no *Google* e aparecerão nomes como *Signal, Telegram, Weibo, Confide* – e que servirão de alternativa ao usuário.

---

de mensagens operam em escala global, de forma que coordenar o acesso de centenas de órgãos de investigação em dezenas de países, alguns dos quais não muito democráticos e com interesses diversos, cria uma receita absolutamente perfeita para abusos e reverte todo o efeito crescente de medidas tecnológicas para coibir esforços de vigilância global." (ARANHA, Diego de Freitas. O que é criptografia fim a fim e o que devemos fazer a respeito? *In*: DONEDA, Danilo; MACHADO, Diego (org.). *A criptografia no direito brasileiro*. São Paulo: Thomson Reuters Brasil, 2020, RB 1.4. E-book).

[23] Audiência Pública Conjunta, Marco Civil Da Internet, ADI 5.527 e Bloqueio Judicial do *WhatsApp*, ADPF 403. Ata. Disponível em: <https://bit.ly/3c3jDli>. Acesso em: 17 set. 2020.

[24] O ataque *ransomware* conhecido como *WannaCry* revelou ao mundo que nem mesmo a Agência Nacional de Segurança Americana (NSA) foi capaz de manter as suas ferramentas fora do alcance dos criminosos. O *WannaCry* afetou dezenas de milhares de computadores em mais de 150 países e causou prejuízos a Governos e empresas privadas. Essa praga virtual se baseia numa ferramenta desenvolvida pela própria NSA com a finalidade de proteger a segurança nacional do Estado Americano, ela foi desenvolvida com esse fim nobre, mas, infelizmente, foi utilizada para fins ilícitos, conforme explicou durante a Audiência Pública o Conselheiro Do Comitê Gestor Da Internet No Brasil e professor Demi Getchko (2017, p. 79-80): "O que aconteceu no ataque do *WannaCry*, em maio de 2016? Havia uma falha no sistema. Todos os sistemas de computação, todos os *softwares*, todos os aplicativos têm uma ou várias falhas, que podem ser conhecidas ou não; se são conhecidas, o fabricante devia tentar sanar, mas pode ser que nem ele saiba que a falha existe. Alguém de áreas de governo descobriu a falha e, evidentemente, guardou-a para usar em caso de emergência, para o bem, para examinar atividades estranhas. Evidente que essa chave geral, esse *backdoor* do bem, rapidamente caiu na mão das pessoas do mal e, em pouco tempo, tivemos um enorme ataque de *ransomware*, como se chama. Isso só para pontuar o fato de que não deveríamos colocar os nossos ovos nessa cesta de que determinado acesso privilegiado só é executado pelas pessoas do bem, porque, se há um acesso privilegiado, ele será usado por todo mundo." (Audiência Pública Conjunta, Marco Civil Da Internet, ADI 5.527 e Bloqueio Judicial do *WhatsApp*, ADPF 403. Ata. Disponível em: <https://bit.ly/3c3jDli>. Acesso em: 17 set. 2020).

Então, ao fim e ao cabo, o benefício ao se fazer algo como o "ataque *man-in-the-middle*", mesmo considerando a hipótese de isso ser extremamente seguro, protegido, e que apenas autoridades utilizarão, acabará perdido e, de alguma forma, ter-se-á um dano à livre concorrência, porque os usuários, do criminoso àquele que se preocupa com a própria segurança, buscarão aplicativos considerados seguros[25].

Alternativas a isso poderiam ser cogitadas. A primeira delas, obrigar também os demais aplicativos que oferecem o serviço no Brasil a criar a "porta dos fundos", o que resultaria igualmente inócuo, porque, como sabemos, a *Internet* é global e o usuário pode instalar em seu aparelho uma versão do respectivo aplicativo disponibilizada em outros países que não adotam a mesma abordagem regulatória[26].

Um segundo caminho que se poderia trilhar necessitaria de uma – diga-se, improvável – ordem global para forçar todos os provedores de aplicativo disponíveis a terem algum tipo de *backdoor*, algo análogo a proibir a criptografia forte *end-to-end*, o que, novamente, não resolveria o problema, porque a criptografia é amplamente conhecida e, por mais que os mecanismos sejam complexos de serem entendidos, há diversas implementações prontas sendo oferecidas livre e gratuitamente na Internet[27].

Assim, qualquer tentativa de banir a encriptação forte resultaria infrutífera, pois ela sempre será acessível aos criminosos, afinal, ela é apenas matemática em forma de *software*. Não é possível voltar a um estado de tempo em que a sociedade não mais saiba utilizar a encriptação[28].

---

[25] Sobre as consequências econômicas de eventual regulação da criptografia, alertou o professor Bruno Magrani (2017, p. 61): "A criptografia funciona efetivamente como um diferencial competitivo da seguinte maneira: se uma empresa nacional não oferece um serviço que seja protegido pela criptografia, enquanto uma empresa estrangeira o oferece, esta vai ter efetivamente uma vantagem sobre aquela. Isso para dizer que, se no Brasil a criptografia for considerada ilegal, as empresas nacionais e eventualmente as estrangeiras que operarem no Brasil estarão em desvantagem competitiva com outras empresas que oferecem seus serviços mundialmente, mas que de alguma maneira não se encontram ou não tem nenhuma relação com o país". (Audiência Pública Conjunta, Marco Civil Da Internet, ADI 5.527 e Bloqueio Judicial do *WhatsApp*, ADPF 403. Ata. Disponível em: <https://bit.ly/3c3jDli>. Acesso em: 17 set. 2020).

[26] "[…] a natureza global dos serviços de Internet faz com que a conformidade com as regras de acesso excepcional seja difícil tanto de definir como de aplicar. Se o software vendido no país X copiar todas as chaves para o governo daquele país, os criminosos poderão simplesmente comprar seu software de países que não cooperam; assim, nos Estados Unidos criminosos poderiam adquirir seus softwares da Rússia. E se o software escolher automaticamente quais governos copiar, usando uma técnica como a geolocalização por IP, como evitar ataques baseados na dissimulação de localização? Embora seja possível projetar sistemas de telefonia móvel para que as jurisdições de acolhimento (*host jurisdictions)* tenham acesso ao tráfego (desde que os usuários não recorram ao *VoIP*), essa é uma tarefa muito mais difícil para aplicativos de mensagens de uso geral". (ABELSON, Harold et al. *Chaves Embaixo do Tapete*: exigências de acesso a todos os dados e comunicações pelo governo geram insegurança. Tradução: SALES, R. et al. Instituto de Tecnologia e Sociedade do Rio (ITS Rio). Rio de Janeiro, 2018, p. 25. Disponível em: < https://bit.ly/35Nxuvc >. Acesso em: 17 set. 2020).

[27] A esse respeito, advertiu em sua exposição o professor da Escola Politécnica da USP, Marcos Simplício Júnior (2017, p. 153): "[…] alguém que quiser desenvolver o aplicativo, simplesmente usará esses pacotes prontos, livres, gratuitos na internet, e o desenvolve. Na escola Politécnica, todo ano, temos projetos de formatura que são feitos com algoritmos de criptografias, e alguns deles de mecanismos de comunicação fim a fim. Então, não é difícil, não é caro fazer o seu próprio aplicativo." (Audiência Pública Conjunta, Marco Civil Da Internet, ADI 5.527 e Bloqueio Judicial do *WhatsApp*, ADPF 403. Ata. Disponível em: <https://bit.ly/3c3jDli>. Acesso em: 17 set. 2020).

[28] "[...] qualquer esforço para proibir essa tecnologia seria completamente ineficaz, já que a generatividade e a arquitetura global da internet permitem que aplicações de criptografia forte sejam criadas a qualquer

Outro problema apontado pelos técnicos diz respeito à integridade/confiabilidade da prova obtida. Conforme expôs o professor Diego Aranha (2017, p. 142)[29], não se conhece uma estratégia técnica para permitir interceptação, ou interferência no canal de comunicação, sem permitir também o poder de introduzir mensagens. Na medida em que um terceiro detém a chave criptográfica de um destinatário e determina qual vai ser a chave de um destinatário, ele também pode interferir no canal de comunicação, introduzindo mensagens ou alterando o seu conteúdo[30], o que termina por comprometer o valor probatório do material coletado para fins de investigação[31].

Outra proposta ventilada pelos órgãos de persecução, e presente na própria chamada da audiência pública, consiste na desabilitação da criptografia para usuários específicos, mediante ordem judicial. *Todavia, a única maneira de desativar a criptografia para um usuário específico, mediante ordem judicial, pressupõe o poder de desativar a criptografia para todos os usuários, ou seja*, por mais que os alvos sejam criminosos, a versão sabotada do protocolo criptográfico será usada por todos. *Assim, a solução seria novamente a criação de vulnerabilidades nos protocolos criptográficos, incorrendo nos mesmos problemas acima apontados*.

Prevalece, portanto, aos olhos da comunidade experta, o entendimento de que interferir no funcionamento de técnicas de encriptação para fins de investigação:

---

momento, baixadas de qualquer lugar do mundo e utilizadas por qualquer agente interessado o suficiente para buscá-las; o conhecimento de técnicas de criptografia forte já não é algo que se consiga apagar da memória da humanidade e tirar das mãos de criminosos sofisticados." (ABREU, Jacqueline de Souza. Passado, presente e futuro da criptografia forte: desenvolvimento tecnológico e regulação. *Rev. Bras. Polít. Públicas*. Brasília, v. 7, nº 3, 2017 p.24-42).

[29] Audiência Pública Conjunta, Marco Civil Da Internet, ADI 5.527 e Bloqueio Judicial do *WhatsApp*, ADPF 403. Ata. Disponível em: <https://bit.ly/3c3jDli>. Acesso em: 17 set. 2020.

[30] "[…] a prática recomendada atual consiste em usar frequentemente *encriptação autenticada*, que fornece a *autenticação* (assegurando que a entidade no outro lado da comunicação é quem você espera, e que a mensagem não sofra alteração após o envio), bem como a *confidencialidade* (protegendo a privacidade das comunicações, incluindo dados financeiros, médicos e outros dados pessoais). No entanto, a divulgação da chave para encriptação autenticada a um terceiro significa que o destinatário da mensagem não estará mais provido de garantia técnica para a integridade da comunicação; a divulgação da chave permite que o terceiro não apenas *leia* o tráfego encriptado, mas também *forje* o tráfego para o destinatário e faça com que ele pareça vir do remetente original. Assim, divulgar a chave a um terceiro cria uma nova vulnerabilidade de segurança. Remetendo-nos aos métodos de encriptação dos anos de 1990, com chaves separadas para encriptação e autenticação, isto não apenas dobraria o esforço computacional necessário, mas traria muitas oportunidades para erros de projeto e implementação que viriam a causar vulnerabilidades". (ABELSON, Harold et al. *Chaves Embaixo do Tapete*: exigências de acesso a todos os dados e comunicações pelo governo geram insegurança. Tradução: SALES, R. et al. Instituto de Tecnologia e Sociedade do Rio (ITS Rio). Rio de Janeiro, 2018, p. 18-19. Disponível em: < https://bit.ly/35Nxuvc >. Acesso em: 17 set. 2020).

[31] No RHC nº 99.735 de 2018, o Superior Tribunal de Justiça considerou ilícita a prova colhida por meio de espelhamento das conversas do *WhatsApp*, implementado via *WhatsApp Web*, mediante acesso físico ao aparelho telefônico do investigado. Destaca-se do julgado: "[…] 8. O fato de eventual exclusão de mensagens enviadas (na modalidade 'Apagar para mim') ou recebidas (em qualquer caso) não deixar absolutamente nenhum vestígio nem para o usuário nem para o destinatário, e o fato de tais mensagens excluídas, em razão da criptografia *end-to-end*, não ficarem armazenadas em nenhum servidor, constituem fundamentos suficientes para a conclusão de que a admissão de tal meio de obtenção de prova implicaria indevida presunção absoluta da legitimidade dos atos dos investigadores, dado que exigir contraposição idônea por parte do investigado seria equivalente a demandar-lhe produção de prova diabólica [...]".

(i) torna os sistemas menos seguros; (ii) viola a livre concorrência; e (iii) não traz resultados efetivos.

5. Criptografia é Direito?

Criptografia não é, necessariamente, algo novo ou especial. A encriptação já é utilizada há séculos, é claro que as técnicas mudaram muito ao longo do tempo, junto com suas aplicações[32].

Apesar de ter se popularizado no mercado para aplicativos de troca de mensagens (*WhatsApp, Telegram, Signal* etc.), a criptografia está em todo lugar. É muito provável que todos nós utilizemos criptografia hoje, seja acessando uma conta bancária no sistema financeiro, fazendo uma compra na *Internet* ou mesmo enviando um *e-mail*[33].

Sem criptografia para garantir proteção para essas atividades *online*, ninguém se sentiria efetivamente seguro para desenvolvê-las[34], o que comprometeria, de certa maneira, o próprio desenvolvimento da *Internet*.

É possível afirmar que a sobrevivência de atividades econômicas como o mercado de ações e o comércio eletrônico depende, efetivamente, da criptografia.

Logo, para além de uma ferramenta de segurança, a criptografia é um elemento central para o crescimento econômico de um país.

---

[32] "A preocupação com comunicação privada na presença de adversários é tão antiga quanto a humanidade. Há fartos registros históricos de como povos da Antiguidade já utilizavam técnicas criptográficas para obter sigilo, a começar pela Cifra de César empregada no Império Romano para estratégia militar. A tendência de utilização de criptografia pelo Estado para fins militares foi dominante durante a Idade Média, quando surgiram as primeiras unidades dedicadas a quebrar cifras utilizadas por reinos vizinhos, posteriormente ganhando enorme importância durante as Grandes Guerras. Até esse ponto, as técnicas criptográficas conhecidas sempre exigiam o compartilhamento prévio de um segredo (chave criptográfica) para comunicação confidencial, por isso chamadas simétricas. Após a disseminação de computadores e o advento de novas ideias nos anos 1970, técnicas criptográficas terminaram por se tornar de domínio civil, passando a fundamentar setores inteiros da economia, como comércio eletrônico e gerência de documentos digitais." (ARANHA, Diego de Freitas. O que é criptografia fim a fim e o que devemos fazer a respeito? *In*: DONEDA, Danilo; MACHADO, Diego (org.). *A criptografia no direito brasileiro*. São Paulo: Thomson Reuters Brasil, 2020, RB 1.1. E-book).

[33] "Quando digitamos nossa senha de acesso em variados sites, por exemplo, esse dado não pode ser transmitido em seu estado original pela rede, sob o risco de qualquer intermediário possa enxergá-lo e utilizá-lo indevidamente. Para solucionar a questão, esses dados passam por uma função criptográfica de *hash* e somente a informação resultante desse processo é transmitida adiante. Ela é conhecida no jargão técnico como um *digest* da função *hash* e, como consequência das questões explicadas anteriormente, a única forma de se chegar a um determinado *digest* é digitando sempre o mesmo dado (no caso, a sua senha), para que, então, a partir da mesma função criptográfica de *hash*, seja gerado o *digest* em questão. Ou seja, o que os *sites* armazenam jamais é (ou jamais deveria ser) uma lista em texto puro contendo as senhas de seus usuários, pois isso seria catastrófico no caso de um ataque *hacker* ou de um vazamento. O que se guarda é apenas uma lista de *digests* indecifráveis, cujos dados originais que os geram são desconhecidos do *site*, de seus funcionários e dos múltiplos intermediários que processam essa informação ao longo da internet." (ALEIXO, Gabriel. A criptografia aplicada para além da privacidade. *In*: DONEDA, Danilo (org.). *A regulação da criptografia no direito brasileiro*. São Paulo: Thomson Reuters Brasil, 2019, RR-5.1. E-book).

[34] Para se ter uma ideia, de acordo com dados recentes do Cert Brasil – que pertence ao Comitê Gestor da Internet, o NIC.br –, mesmo com a ampla utilização de técnicas criptográficas *by default*, 875.327 incidentes de segurança foram reportados somente no ano de 2019 (disponível em https://www.cert.br/stats/incidentes/).

A criptografia também, como ferramenta de segurança, é utilizada por diversos governos, exatamente para garantir o sigilo da comunicação sobre assuntos sensíveis, como aqueles relacionados à segurança nacional[35] e à segurança de Estado[36].

Vê-se, portanto, que a defesa da criptografia não diz respeito somente à preservação da privacidade ou intimidade, de modo que o famigerado conflito "privacidade versus segurança pública", na realidade, se apresenta equivocado e desvirtua o debate, na exata medida em que a própria criptografia foi pensada e projetada para tornar a "vida *online"* mais segura.

Frise-se, privacidade e segurança são intimamente relacionadas e caminham lado a lado, não o contrário. Uma vez violada a privacidade, um dos direitos mais impactados é, indubitavelmente, a segurança.

Nessa busca de promover o direito à segurança, a criptografia exerce papel fundamental. A propósito, parece haver uma tendência no Supremo Tribunal Federal para o reconhecimento da encriptação como fonte de segurança, conforme se extrai das conclusões do voto do Ministro Relator da ADPF nº 403, Luiz Edson Fachin (2020, p. 02)[37]:

> 1.1. Premissas [...] Sétima: É contraditório que em nome da segurança pública deixe-se de promover e buscar uma internet mais segura. Uma internet mais segura é direito de todos e dever do Estado. Medidas que, à luz da melhor evidência científica, trazem insegurança aos usuários somente se justificam se houver certeza comparável aos ganhos obtidos em outras áreas.

O voto da Ministra Rosa Weber (2020, p. 27-28)[38], relatora da ADI 5.527, é ainda mais enfático nesse aspecto:

> 15. A questão da criptografia
>
> Embora a ciência da criptografia seja tão antiga quanto a escrita, o desenvolvimento e disseminação de tecnologias criptográficas na

[35] Reconhecendo a importância da criptografia para a defesa de informações sensíveis à segurança nacional, o Governo Federal estabeleceu como ação estratégica para a Estratégia Nacional de Segurança Cibernética (Decreto nº 10.222/2020): "a adoção de soluções nacionais de criptografia [...]".

[36] "Não é à toa que a pesquisa científica sobre criptografia se deu por muito tempo por financiamento de Estados, dentro de entidades estatais, como órgãos militares e serviços secretos. Esses órgãos tinham tanto os incentivos quanto os recursos necessários para isso. Afinal, criptografia é uma técnica crucial para proteger informações sensíveis. Assim, quando o Estado quer garantir a privacidade e a segurança de suas próprias comunicações e dados, a implementação de técnicas de criptografia é imprescindível". (ABREU, Jacqueline de Souza. Passado, presente e futuro da criptografia forte: desenvolvimento tecnológico e regulação. *Rev. Bras. Polít. Públicas*. Brasília, v. 7, nº 3, 2017 p. 24-42).

[37] Supremo Tribunal Federal, ADPF n. 403, Voto Ministro Relator Luiz Edson Fachin. Disponível em < https://bit.ly/3iN3UcT >. Acesso em: 17 set. 2020.

[38] Supremo Tribunal Federal, ADI n. 5.527, Voto Ministra Relatora Rosa Weber. Disponível em < https://bit.ly/33HzBho >. Acesso em: 17 set. 2020.

> contemporaneidade é o que torna as comunicações e as transações online mais seguras e, em consequência, a sociedade também fica mais segura.
>
> [...] De modo similar, o emprego da criptografia de chave pública confere segurança e privacidade às comunicações efetuadas por meio de redes abertas ao acesso de todos.
>
> Seria um inadmissível contrassenso, e mesmo retrocesso, tornar ilegal ou limitar dessa maneira o uso de criptografia [...].
>
> Além disso, a difusão da criptografia também tem garantido a segurança da comunicação de grupos de direitos humanos e indivíduos que se mobilizam contra regimes opressivos ao redor do mundo.
>
> Em certa medida, a liberdade fundamental que assegura ao indivíduo o direito de fechar o portão de casa com um cadeado, elevar a altura do muro ou pendurar uma cortina na janela, autoriza cogitar uma espécie de direito fundamental à encriptação, ou pelo menos que o uso da criptografia consiste em uma ferramenta indispensável, nos dias de hoje, para assegurar o direito à privacidade.

O entendimento concerta-se com o decreto regulamentador do Marco Civil da Internet, que assume a criptografia como ferramenta de segurança, com a finalidade de proteger a inviolabilidade de dados do usuário e a privacidade de sua comunicação[39].

Na esteira desse raciocínio, percebe-se que, ao dar concreção ao postulado da inviolabilidade das comunicações privadas, a criptografia de ponta a ponta diz respeito tanto à proteção da privacidade quanto da segurança.

Assim também, ao proteger a privacidade, a criptografia facilita, ou permite, o exercício de outros direitos a ela relacionados, como a liberdade de expressão, garantia essencial para uma sociedade que se pretenda democrática. A esse respeito, destaca-se, novamente, relevante passagem do voto da Ministra Rosa Weber (2020, p. 10)[40]:

> Integra o pleno exercício das liberdades de expressão e de comunicação a capacidade das pessoas de escolherem livremente as informações que pretendem compartilhar, as ideias que pretendem discutir, o estilo de linguagem empregado e o meio de comunicação.

[39] "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" (Decreto nº 8.771/2016).

[40] Supremo Tribunal Federal, ADI n. 5.527, Voto Ministra Relatora Rosa Weber. Disponível em: < https://bit.ly/33HzBho >. Acesso em: 17 set. 2020.

> O conhecimento de que a comunicação é monitorada por terceiros interfere em todos esses elementos componentes da liberdade de informação: os cidadãos podem mudar o modo de se expressar ou até mesmo absterem-se de falar sobre certos assuntos, no que a doutrina designa por efeito inibitório (*chilling effect*) sobre a liberdade de expressão.

A violação da privacidade das comunicações, é evidente, torna as pessoas cautelosas em relação àquilo que dizem, reduzindo, assim, o ambiente plural da *Internet*[41], acabando por instalar o temor e a inibição como parte da cultura política[42].

O respeito à liberdade de expressão exige que os indivíduos possam se comunicar sem interferências indevidas, o que requer que suas comunicações sejam privadas e seguras, e, no papel de garantir tais predicados, a criptografia é essencial[43].

A difusão da criptografia também tem garantido a segurança da comunicação de grupos de direitos humanos e indivíduos que se mobilizam contra regimes opressivos ao redor do mundo. Banir a criptografia poderia ter implicações extremamente perigosas sobre ativistas de direitos humanos, jornalistas, denunciantes e dissidentes políticos, acabando por favorecer regimes autoritários[44].

---

[41] "Maximizar o número e a diversidade de vozes que podem participar da deliberação pública é, ao mesmo tempo, uma condição e uma finalidade essencial do processo democrático. Nesse sentido, as garantias robustas para o exercício da liberdade de expressão pela internet são, na atualidade, uma condição para a possibilidade dessa abertura da esfera pública." (ORGANIZAÇÃO DOS ESTADOS AMERICANOS. Comissão Interamericana de Direitos Humanos. Liberdade de expressão e internet. Relatoria Especial para a Liberdade de Expressão. § 18. 31 de dezembro de 2013. Disponível em: < https://bit.ly/33aS476 >. Acesso em: 17 set. 2020).

[42] A violação da privacidade das comunicações pode gerar uma restrição direta quando, por exemplo, o direito não puder ser exercido de forma anônima como consequência da atividade de vigilância. Por outro lado, a mera existência do programa de vigilância produz uma restrição indireta que gera um efeito inibidor sobre o exercício da liberdade de expressão. A respeito do efeito inibidor que a potencial violação à privacidade provoca à liberdade de expressão ver: NAÇÕES UNIDAS. Assembleia Geral. Relatório do Relator Especial sobre a Promoção e Proteção do Direito à Liberdade de Opinião e Expressão, Frank La Rue. A/HRC/17/27. 16 de maio de 2011. § 26, 53 e 55. Disponível em: < https://undocs.org/en/A/HRC/17/27 >. Acesso em: 17set. 2020.

[43] Como salienta o Relator Especial da ONU para a liberdade de expressão, David Kaye, a criptografia e o anonimato criam uma zona de privacidade que permitem o exercício dos direitos à liberdade de opinião e de expressão, motivo pelo qual conclui que eventuais restrições ao uso de encriptação devem ser estritamente limitadas: "*Encryption and anonymity, and the security concepts behind them, provide the privacy and security necessary for the exercise of the right to freedom of opinion and expression in the digital age. Such security may be essential for the exercise of other rights, including economic rights, privacy, due process, freedom of peaceful assembly and association, and the right to life and bodily integrity. Because of their importance to the rights to freedom of opinion and expression, restrictions on encryption and anonymity must be strictly limited according to principles of legality, necessity, proportionality and legitimacy in objective. The Special Rapporteur therefore recommends the following.*" (NAÇÕES UNIDAS. Assembleia Geral. Relatório do Relator Especial para a promoção e proteção da liberdade de opinião e de expressão, David Kaye, A/HRC/29/32. 22 de maio de 2015. § 56. Disponível em: < https://undocs.org/en/A/HRC/29/32 >. Acesso em: 17 set. 2020).

[44] A esse respeito, ver mais uma vez as recomendações do Relator Especial para a promoção e proteção da liberdade de expressão, notadamente: "*States should promote strong encryption and anonymity. National laws should recognize that individuals are free to protect the privacy of their digital communications by using encryption technology and tools that allow anonymity online. Legislation and regulations protecting human rights defenders and journalists should also include provisions enabling access and providing support to use*

*Em resumo, a criptografia confere eficácia e materializa a proteção dos direitos de liberdade expressão, liberdade de comunicação e privacidade, na medida em que "*permite a comunicação livre, aberta e honesta, sem receio de que terceiros não autorizados tenham acesso ao seu conteúdo*" (MAGRANI, 2017, p. 62)*[45].

Além disso, não se pode olvidar a sua importância para que pessoas, governos e negócios continuem se comunicando de maneira segura, o que, em última análise, representa um vetor de promoção do crescimento econômico.

*E, finalmente, deve-se ter em mente que a criptografia também visa coibir crimes, justamente os delitos que podem advir de sistemas inseguros, como fraudes, furto de identidade (*account takeover*), extorsão, e outros ilícitos associados à obtenção desautorizada de informações pessoais*[46].

Portanto, a criptografia exerce papel instrumental de garantia do exercício de outros direitos que, em uma sociedade democrática, são essenciais para a vida pública. Por essa razão, propostas que impliquem limitações aos mecanismos de encriptação devem ser avaliadas com extrema cautela.

6. Considerações finais

Cada vez mais os serviços de mensagem instantânea têm oferecido criptografia forte por padrão, implementando protocolos criptográficos de ponta a ponta que não proporcionam ao provedor acesso ao conteúdo de conversas de seus usuários, e a principal razão para essa guinada é o fato de que os próprios consumidores estão buscando segurança para os seus dados pessoais quando optam por um entre os diversos aplicativos disponíveis no mercado.

A postura dos provedores de aplicação, não colaborativa com as agências de investigação criminal, tem gerado disputas ao redor do mundo a respeito da imposição de limites à encriptação. Nos Estados Unidos, o embate já se estabeleceu há muito, passando por diversas tentativas de impedir ou limitar o avanço da criptografia – tentativas que ficaram conhecidas por "*crypto wars*"[47] –, com iniciativas como a

the technologies to secure their communications." (NAÇÕES UNIDAS. Assembleia Geral. Relatório do Relator Especial para a promoção e proteção da liberdade de opinião e de expressão, David Kaye, A/HRC/29/32. 22 de maio de 2015. § 59. Disponível em: < https://undocs.org/en/A/HRC/29/32 >. Acesso em: 17 set. 2020).

[45] Audiência Pública Conjunta, Marco Civil Da Internet, ADI 5.527 e Bloqueio Judicial do *WhatsApp*, ADPF 403. Ata. Disponível em: <https://bit.ly/3c3jDli>. Acesso em: 17 set. 2020.

[46] Merecem destaque, também nesse ponto, as relevantes ponderações da Ministra Rosa Weber: "O *trade-off* aqui, portanto, não se dá entre segurança pública e privacidade, pois a pretensão que ameaça a privacidade, ainda que fundada no combate a uma ameaça imediata à segurança, vulnera no longo prazo, também a segurança das redes e seus usuários como um todo, expondo-os a maiores riscos de ciberataques, fraudes, roubos de identidade, invasão da intimidade extorsão etc. A mesma tecnologia que tornaria mais fácil às autoridades de segurança pública acessarem conteúdo armazenado pode – e, existindo, será – utilizada por criminosos para terem acesso a informações privadas de futuras vítimas." (Supremo Tribunal Federal, ADI n. 5.527, Voto Ministra Relatora Rosa Weber. Disponível em < https://bit.ly/33HzBho >. Acesso em: 17set. 2020).

[47] Sobre o tema das "*cripto wars*" estadunidenses ver: LIGUORI FILHO, Carlos Augusto; SALVADOR, João Pedro Favaretto. *Crypto wars* e bloqueio de aplicativos: o debate sobre regulação jurídica da criptografia

restrição da sua exportação e também ao uso doméstico, destacando-se neste ponto o programa de guarda de chaves conhecido como *Clipper Chip*[48].

As medidas de controle de exportação de criptografia forte implementadas nos Estados Unidos desestimularam o desenvolvimento de pesquisa pelas fabricantes americanas, diminuindo, por consequência, a disponibilidade de mecanismos de segurança de ponta no mercado interno; ademais, fizeram essa indústria americana menos competitiva frente a empresas estrangeiras não sujeitas às mesmas regras de controle, gerando, dessa maneira, elevados custos para a economia[49] e, evidenciando, mais uma vez, o peso da regulação[50].

---

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://bit.ly/2RlCZmA >. Acesso em: 17 set. 2020.

[48] *Clipper Chip* foi um chip desenvolvido pela Agência de Segurança Nacional dos EUA (NSA) para ser utilizado em equipamentos de voz seguros, como telefones criptografados, mas que, ao mesmo tempo, viabilizava que as chaves para decodificar as transmissões ficassem em depósito juntamente a um "terceiro confiado" para que pudessem ser acessadas no contexto de investigações criminais. O plano foi permeado por diversas polêmicas, e acabou abandonado, conforme bem sintetizou o resultado da mencionada pesquisa da FGV: "O governo desenvolveu um chip que poderia ser adquirido por empresas fabricantes de dispositivos de comunicação. Esse chip, alegava o governo, era mais seguro, conveniente e barato que outras soluções de criptografia disponíveis na época. A contrapartida era que as chaves criptográficas associadas a cada chip seriam enviadas para instituições associadas ao governo no momento da fabricação, permitindo a interceptação das comunicações quando embasada em uma ordem judicial. A proposta não vingou por uma série de razões. Em primeiro lugar, o chip possuía falhas técnicas que permitiam burlar o poder de interceptação do governo. Em segundo lugar, o algoritmo implementado no chip, o *Skipjack*, foi mantido em sigilo, impedindo a realização de testes públicos que poderiam confirmar ou desconfirmar sua solidez. Em terceiro lugar, a comunidade científica se mobilizou no sentido de rejeitar a proposta por seu alto custo, sua insegurança e sua excessiva complexidade técnica. Todos esses fatores contribuíram para a desconfiança em relação à iniciativa do governo, o que levou as empresas fabricantes de dispositivos de comunicação a não adotarem o *Clipper Chip*. Posteriormente, em 1999, o governo americano declarou que não mais buscaria formas de restringir o uso ou a implementação de ferramentas criptográficas no país, abandonando propostas de guarda de chaves e de controle de exportação". (CENTRO DE ENSINO E PESQUISA EM INOVAÇÃO. Criptografia e Direito: uma perspectiva comparada. Relatório de Pesquisa. Estados Unidos da América. *In: Criptomap*. FGV Direito SP, 2018. Disponível em: < https://bit.ly/33zN0rS >. Acesso em: 17 set. 2020).

[49] "O crescimento econômico vem em grande parte da inovação em ciência, tecnologia e processos de negócios. Atualmente, o progresso tecnológico se dá em grande parte sobre a incorporação de inteligência – software e comunicações – em todos os lugares. Produtos e serviços que eram autônomos agora vêm com um aplicativo de celular, um serviço da *Web on-line* e modelos de negócios que envolvem anúncios ou assinatura. Sendo esses cada vez mais "sociais" e permitindo aos usuários conversar com seus amigos e atraí-los para o *Web marketing* do fornecedor. Países que exigem que esses novos aplicativos e serviços da Web tenham suas funções de comunicação de usuário-para-usuário (*user-to-user*) autorizadas pelo governo estarão em significativa desvantagem. Atualmente, o mundo usa amplamente aplicativos e serviços dos EUA, em vez de aplicativos aprovados pelo governo da Rússia e da China, proporcionando, assim, enorme alavancagem para as empresas dos Estados Unidos." (ABELSON, Harold et al. *Chaves Embaixo do Tapete*: exigências de acesso a todos os dados e comunicações pelo governo geram insegurança. Tradução: SALES, R. et al. Instituto de Tecnologia e Sociedade do Rio (ITS Rio). Rio de Janeiro, 2018, p. 17. Disponível em: < https://bit.ly/35Nxuvc >. Acesso em: 17set. 2020).

[50] "É impossível operar a Internet comercial ou outra rede global de comunicações, mesmo em níveis modestos de segurança, sem o uso de encriptação. […] No início dos anos de 1990, a comercialização da Internet era frustrada pelos controles do governo dos EUA sobre encriptação – controles que, em muitos aspectos, eram contraproducentes para os interesses comerciais e de segurança nacional em longo prazo. Um estudo de 1996 da Academia Nacional de Ciências dos Estados Unidos concluiu que, 'em última análise, as vantagens do uso mais difundido da criptografia superam as desvantagens' [4, p. 6]. Quatro anos depois, diversos motivos fizeram com que os EUA afrouxassem os controles de exportação sobre encriptação, em resposta: a) às pressões da indústria; b) ao afrouxamento dos controles criptográficos de exportação pela União Europeia; c) aos controles criptográficos de exportação declarados inconstitucionais pelos tribunais

A experiência pioneira norte-americana, com diversos esforços para impor restrições à encriptação fracassados, deve servir de lição aos demais países. No momento, no Brasil, aguarda-se a decisão do STF acerca da legalidade dos bloqueios, algo que deve influenciar diretamente a condução do debate sobre regulação de criptografia no país, questão que se afigura chave para enfrentar o mérito das ações de controle concentrado, *ADI 5.527 e ADPF 403*.

O julgamento conjunto das ações iniciou em maio de 2020, com o voto de ambos os relatores revelando a tendência de que o STF entenderá inconstitucional a proibição da criptografia ponta a ponta ou a estipulação de restrições ao seu uso.

O cenário que se apresenta deve despertar os órgãos de persecução penal para a necessidade de adaptar o aparato investigativo de maneira a funcionar na presença de criptografia forte[51], fazendo o bom uso de dados acessíveis nas plataformas de comunicação, como os metadados[52] por exemplo, empregando técnicas especiais de coleta de evidências como a infiltração virtual[53], e também buscando soluções para contornar a criptografia, mediante acesso a dados disponíveis em serviços de computação em nuvem[54] ou ainda por meio da exploração de vulnerabilidades de sistemas e aparelhos (*government hacking*[55]).

---

dos EUA; d) à crescente dependência das comunicações eletrônicas e do comércio." (ABELSON, Harold et al. *Chaves Embaixo do Tapete*: exigências de acesso a todos os dados e comunicações pelo governo geram insegurança. Tradução: SALES, R. et al. Instituto de Tecnologia e Sociedade do Rio (ITS Rio). Rio de Janeiro, 2018, p. 17. Disponível em: < https://bit.ly/35Nxuvc >. Acesso em: 17 set. 2020).

[51] "A inviabilidade técnica de introdução de falhas intencionais para interceptação legal não significa que plataformas de comunicação segura estejam completamente imunes a esforços de investigação ou qualquer outra intervenção do aparato investigativo. Na verdade, o esforço de investigação deve se adaptar às características de plataformas para comunicação segura para exercer o seu papel. Equipar agentes e especialistas com informação técnica acurada sobre essas tecnologias é garantir o poder investigativo do Estado em longo prazo, à medida que tecnologias de preservação de privacidade se disseminam cada vez mais." (ARANHA, Diego de Freitas. O que é criptografia fim a fim e o que devemos fazer a respeito? *In*: DONEDA, Danilo; MACHADO, Diego (org.). *A criptografia no direito brasileiro*. São Paulo: Thomson Reuters Brasil, 2020, RR-2.5. E-book). A respeito de maneiras de "contornar" a criptografia, ver: KERR, Orin S.; SCHNEIER, Bruce. Encryption Workarounds. *Georgetown Law Journal*, 20 de mar. 2017. Disponível em: < https://ssrn.com/abstract=2938033 >. Acesso em: 17 set. 2020.

[52] "[...] consideram-se metadados todos os dados e registros gerados a partir de uma comunicação e que não constituam o seu conteúdo em si, como, por exemplo, data, hora e duração da comunicação, remetente, destinatários, eventuais dados de localização geográfica do dispositivo (como Estação Rádio Base), códigos de identificação de dispositivos (como IMEI) etc." (ABREU, Jacqueline de Souza; ANTONIALLI, Dennys. *Vigilância sobre as comunicações no Brasil*: interceptações, quebras de sigilo, infiltrações e seus limites constitucionais. São Paulo: InternetLab, 2017, p. 17. Disponível em: < https://bit.ly/3hLu5z7 >. Acesso em: 17set. 2020).

[53] A propósito do tema infiltração virtual, foi editada a Lei nº 13.441/2017, que autoriza expressamente a infiltração de agentes de polícia na Internet com o fim de investigar crimes contra a dignidade sexual de criança e de adolescente. Para mais sobre o tema, ver: WOLFF, Rafael. Infiltração de agentes por meio virtual. *In*: SILVA, Ângelo Roberto Ilha (org.). *Crimes Cibernéticos*. Porto Alegre: Livraria do Advogado, 2017.

[54] É comum que usuários façam cópia de segurança autorizada de suas conversas em serviços de armazenamento em nuvem, como *Google Drive*, *Apple iCloud* e *Microsoft One Drive*, para preservar acesso ao conteúdo em caso de perda de acesso ao dispositivo (e chaves criptográficas lá armazenadas). Ao contrário das mensagens enviadas e recebidas em aplicativos de mensagens como o *WhatsApp*, os *backups* dessas mesmas conversas, quando armazenados em nuvem, não costumam contar com a proteção da criptografia. (MENN, Joseph. Exclusive: *Apple dropped plan for encrypting backups after FBI complained – sources*. Thomson Reuters, 21 de jan. 2020. Disponível em: < https://reut.rs/35TU3yj >. Acesso em: 17set. 2020).

[55] Se o fluxo da comunicação não pode ser interceptado, então se atacam as pontas da comunicação. Nos EUA, por exemplo, o que a NSA tem feito há muito é explorar vulnerabilidades dos aparelhos utilizados na

Nesta conjuntura, a única estratégia viável para o Estado preservar poderes de investigação é modernizar-se, reformulando suas equipes e provendo-as com especialistas que detenham qualificação técnica voltada às novas tecnologias, empreendendo esforços na formação contínua de seus agentes de maneira a acompanhar a tendência crescente e, certamente, benéfica à coletividade do emprego de criptografia.

Referências

ABELSON, Harold et al. *Chaves Embaixo do Tapete*: exigências de acesso a todos os dados e comunicações pelo governo geram insegurança. Tradução: SALES, R. et al. Instituto de Tecnologia e Sociedade do Rio (ITS Rio). Rio de Janeiro, 2018. Disponível em: < https://bit.ly/35Nxuvc >. Acesso em: 17set. 2020. Título Original: *Keys Under Doormats: mandating insecurity by requiring government access to all data and communications*.

ABREU, Jacqueline de Souza; ANTONIALLI, Dennys. *Vigilância sobre as comunicações no Brasil*: interceptações, quebras de sigilo, infiltrações e seus limites constitucionais. São Paulo: InternetLab, 2017. Disponível em: < https://bit.ly/3hLu5z7 >. Acesso em: 17set. 2020.

_____. *Passado, presente e futuro da criptografia forte*: desenvolvimento tecnológico e regulação. Rev. Bras. Polít. Públicas, Brasília, v. 7, nº 3, 2017, p. 24-42.

ALEIXO, Gabriel. A criptografia aplicada para além da privacidade. *In*: DONEDA, Danilo (org.). *A regulação da criptografia no direito brasileiro*. São Paulo: Thomson Reuters Brasil, 2019. E-book. Não paginado.

ALIMONTI, Veridiana. Criptografia, direitos e a problemática polarização entre "privacidade individual" e "segurança coletiva". *In*: DONEDA, Danilo; MACHADO, Diego (org.). *A criptografia no direito brasileiro*. São Paulo: Thomson Reuters Brasil, 2020. E-book. Não paginado.

ARANHA, Diego de Freitas. O que é criptografia fim a fim e o que devemos fazer a respeito? *In*: DONEDA, Danilo; MACHADO, Diego (org.). *A criptografia no direito brasileiro*. São Paulo: Thomson Reuters Brasil, 2020. E-book. Não paginado.

BRASIL. Câmara dos Deputados. *Projeto de lei nº 9.808, 20 de março de 2018*. Autor: João Campos. Câmara dos Deputados, Brasília, DF, 20 de mar. 2018. Disponível em: < https://bit.ly/3hlz5Vk >. Acesso em: 17 set. 2020.

comunicação (*endpoints*), onde a informação não está criptografada. Sobre o tema *Hacking Governamental*, ver LIGUORI, Carlos. *Exploring Lawful Hacking as a Possible Answer to the "Going Dark" Debate.* 26 MICH. TELECOMM. & TECH. L. REV. 317, 2020. Disponível em: < https://bit.ly/33LtOYd >. Acesso em: 17set. 2020. Ver também: SCHNEIER, Bruce. *O mercado de vulnerabilidades e o futuro da segurança*. Tradução: GOULART, Guilherme Damasio; SERAFIM, Vinícius Silveira. 2012. Disponível em: < https://bit.ly/3hZyiPQ >. Acesso em: 17 set. 2020. Título Original: *The Vulnerabilities Market and the Future of Security.*

_____. Câmara dos Deputados. *Projeto de lei nº 10.372, 06 de junho de 2018*. Autor: José Rocha. Câmara dos Deputados, Brasília, DF, 06 de jun. 2018. Disponível em: < https://bit.ly/3myty7y >. Acesso em: 17set. 2020.

_____. *Decreto nº 8.771, de 11 de maio de 2016*. Regulamenta a Lei nº 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações. Brasília, DF, 11 de mai. 2016. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8771.htm >. Acesso em: 17 set. 2020.

_____. *Decreto nº 10.222, de 05 de fevereiro de 2020*. Aprova a Estratégia Nacional de Segurança Cibernética. Brasília, DF, 05 de fev. 2020. Disponível em: < http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Decreto/D10222.htm >. Acesso em: 17 set. 2020.

_____. *Lei nº 12.965, de 23 de abril de 2014*. Marco Civil da Internet. Brasília, DF:

Presidência da República. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm >. Acesso em: 17 set. 2020.

_____. *Lei nº 13.441, de 8 de maio de 2017.* Altera a Lei nº 8.069, de 13 de julho de 1990 (Estatuto da Criança e do Adolescente), para prever a infiltração de agentes de polícia na internet com o fim de investigar crimes contra a dignidade sexual de criança e de adolescente. Disponível em < http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2017/Lei/L13441.htm >. Acesso em: 17 set. 2020.

_____. Superior Tribunal de Justiça (Sexta Turma). *Recurso em Habeas Corpus nº 99.735/SC*. RECURSO ORDINÁRIO EM *HABEAS CORPUS*. PENAL E PROCESSO PENAL. TRÁFICO DE DROGAS E ASSOCIAÇÃO AO TRÁFICO. AUTORIZAÇÃO JUDICIAL DE ESPELHAMENTO, VIA *WHATSAPP WEB*, DAS CONVERSAS REALIZADAS PELO INVESTIGADO COM TERCEIROS. ANALOGIA COM O INSTITUTO DA INTERCEPTAÇÃO TELEFÔNICA. IMPOSSIBILIDADE. PRESENÇA DE DISPARIDADES RELEVANTES. ILEGALIDADE DA MEDIDA. RECONHECIMENTO DA NULIDADE DA DECISÃO JUDICIAL E DOS ATOS E PROVAS DEPENDENTES. PRESENÇA DE OUTRAS ILEGALIDADES. LIMITAÇÃO AO DIREITO DE PRIVACIDADE DETERMINADA SEM INDÍCIOS RAZOÁVEIS DE AUTORIA E MATERIALIDADE. DETERMINAÇÃO ANTERIOR DE ARQUIVAMENTO DO INQUÉRITO POLICIAL. FIXAÇÃO DIRETA DE PRAZO DE 60 (SESSENTA) DIAS, COM PRORROGAÇÃO POR IGUAL PERÍODO. CONSTRANGIMENTO ILEGAL EVIDENCIADO. RECURSO PROVIDO. Relatora: Min. Laurita Vaz. Brasília, DF, 27 de nov. 2018. Disponível em: < https://bit.ly/3ccVYiy >. Acesso em: 17 set. 2020.

_____. Supremo Tribunal Federal. *Ação Direta de Inconstitucionalidade nº 5.527*. Voto Min. Relatora Rosa Weber. Brasília, DF, 27 de mai. 2020. Disponível em < https://bit.ly/33HzBho >. Acesso em: 17 set. 2020.

_____. Supremo Tribunal Federal. *Arguição de Descumprimento de Preceito Fundamental nº 403*. Voto Min. Relator Luiz Edson Fachin. Brasília, DF, 28 de mai. 2020. Disponível em < https://bit.ly/3iN3UcT >. Acesso em: 17 set. 2020.

_____. Supremo Tribunal Federal. *Audiência Pública Conjunta, Marco Civil da Internet*, ADI 5.527, e Bloqueio Judicial do WhatsApp, ADPF 403. Ata. Brasília, DF, 02, 05 de jun. 2017. Disponível em: <https://bit.ly/3c3jDli>. Acesso em: 17 set. 2020.

CENTRO DE ENSINO E PESQUISA EM INOVAÇÃO. *Criptografia e Direito*: uma perspectiva comparada. Relatório de Pesquisa. FGV Direito SP, 2018. Disponível em: < https://bit.ly/33zN0rS >. Acesso em: 17 set. 2020.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL (CERT.br). *Estatísticas dos Incidentes Reportados ao CERT.br*. Atual 09 de set. 2020. Disponível em: < https://www.cert.br/stats/incidentes/ >. Acesso em: 17 set. 2020.

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://bit.ly/32DztQN>. Acesso em: 17 set. 2020.

FAGUNDES, I.; SENRA, R. *Executivo do Facebook é libertado em SP*. BBC Brasil. São Paulo, 02 de mar. 2016. Disponível em: < https://bbc.in/2FEcRqn >. Acesso em: 17 set. 2020.

INTERNETLAB. *BLOQUEIOS.INFO*. Disponível em < https://bloqueios.info/pt/linha-do-tempo/ >. Acesso em: 17 de set. 2020.

KERR, Orin S.; SCHNEIER, Bruce. Encryption Workarounds. *Georgetown Law Journal*, 20 de mar. 2017. Disponível em: < https://ssrn.com/abstract=2938033 >. Acesso em: 17 set. 2020.

LEE, Timothy B. *Here's everything we know about PRISM to date*. The Washington Post. Washington D. C., 12 de jun. 2013. Disponível em: < https://wapo.st/3mEg4qX >. Acesso em: 17 set. 2020.

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://bit.ly/2RICZmA >. Acesso em: 17 set. 2020.

LIGUORI, Carlos. *Exploring Lawful Hacking as a Possible Answer to the "Going Dark" Debate*. 26 MICH. TELECOMM. & TECH. L. REV. 317, 2020. Disponível em: < https://bit.ly/33LtOYd >. Acesso em: 17set. 2020.

MACASKILL, E. et al. NSA files: decoded. *The Guardian*, 01 de nov. 2013. Disponível em: <https://bit.ly/2ZHLvXt >. Acesso em: 17 set. 2020.

MENN, Joseph. Exclusive: *Apple dropped plan for encrypting backups after FBI complained – sources*. Thomson Reuters, 21 de jan. 2020. Disponível em: < https://reut.rs/35TU3yj >. Acesso em: 17set. 2020.

MINISTÉRIO PÚBLICO FEDERAL. Câmara de Revisão Criminal, 2. Roteiro de Atuação: Crimes Cibernéticos. 3ª edição. Brasília – DF, 2016. E-book.

NAÇÕES UNIDAS (ONU). Assembleia Geral. Relatório do Relator Especial para a promoção e proteção da liberdade de opinião e de expressão, Frank La Rue. A/HRC/17/27. 16 de maio de 2011. Disponível em: < https://undocs.org/en/A/HRC/17/27 >. Acesso em: 17set. 2020.

_____. Assembleia Geral. Relatório do Relator Especial para a promoção e proteção da liberdade de opinião e de expressão, David Kaye, A/HRC/29/32. 22 de maio de 2015. Disponível em: < https://undocs.org/en/A/HRC/29/32 >. Acesso em: 17set. 2020

NSA slides explain the PRISM data-collection program. *The Washington Post*. Washington D. C., 10 de jul. 2013. Disponível em: < https://wapo.st/2ZM9k0g >. Acesso em: 17 set. 2020.

ORGANIZAÇÃO DOS ESTADOS AMERICANOS (OEA). Comissão Interamericana de Direitos Humanos. Relatoria Especial para a Liberdade de Expressão, Liberdade de expressão e internet. Disponível em: < https://bit.ly/33aS476 >. Acesso em: 17set. 2020

SCHNEIER, Bruce. *O mercado de vulnerabilidades e o futuro da segurança*. Tradução: GOULART, Guilherme Damasio; SERAFIM, Vinícius Silveira. 2012. Disponível em: < https://bit.ly/3hZyiPQ >. Acesso em: 17set. 2020. Título Original: *The Vulnerabilities Market and the Future of Security*.

WHATSAPP'S Signal Protocol integration is now complete. 05 de abr. 2016. Disponível em < https://signal.org/blog/whatsapp-complete/ >. Acesso em: 17set. 2020.

WOLFF, Rafael. Infiltração de agentes por meio virtual. *In*: SILVA, Ângelo Roberto Ilha (org.). *Crimes Cibernéticos*. Porto Alegre: Livraria do Advogado, 2017.