A CRIPTOGRAFIA E SEUS REFLEXOS JURÍDICOS. ESTUDO DE CASO SOBRE A ADPF 403 E ADI 5527 NO SUPREMO TRIBUNAL FEDERAL

CRYPTOGRAPHY AND ITS LEGAL REFLECTIONS. CASE STUDY ON ADPF 403 AND ADI 5.527 AT THE SUPREME FEDERAL COURT

Giovani Agostini Saavedra[1]
Professor de Direito Econômico e Político (Mackenzie, São Paulo/SP, Brasil)

Stela Chaves Rocha Sales[2]
Mestranda em Direito Político e Econômico (Mackenzie, São Paulo/SP, Brasil)

Roberta Battisti Pereira[3]
Mestranda em Direito Político e Econômico (Mackenzie, São Paulo/SP, Brasil)

ÁREA(S): direito constitucional; direito digital.

RESUMO: O propósito desse artigo é o de compreender os desafios jurídicos postos diante do uso de criptografia de ponta a ponta, a partir da compreensão da ferramenta e da análise das decisões judiciais que determinaram o bloqueio do aplicativo *WhatsApp* pelo uso da criptografia ponta a ponta. O trabalho abordou a relação de criptografia com

[1] Doutor em Direito e Filosofia pela *Johann Wolfgang Goethe – Universidade de Frankfurt am Main*. Mestre em Direito pela PUCRS. *E-mail*: giovani.saavedra@saavedra.adv.br. Currículo: http://lattes.cnpq.br/5594109824546097. Orcid: https://orcid.org/0000-0002-5269-3844.

[2] Pesquisadora do Laboratório de Direito Digital e Democracia, Advogada na área de Direito Digital. Membro do Instituto Liberdade Digital. *E-mail*: stela.rocha.sales@gmail.com. Currículo: http://lattes.cnpq.br/3586789274100055. Orcid: https://orcid.org/0000-0003-1397-9222.

[3] Pesquisadora do Laboratório de Direito Digital e Democracia e do Instituto Liberdade Digital. *E-mail*: rbattistip@gmail.com. Currículo: http://lattes.cnpq.br/8745084475722485. Orcid: https://orcid.org/0000-0002-9446-5997.

direitos fundamentais, como: privacidade, segurança pública, soberania estatal e liberdade econômica. Por fim, o artigo analisou a experiência de alguns países sobre o uso de criptografia de ponta a ponta e a compreensão brasileira sobre o assunto, fazendo um estudo de caso sobre as duas ações que tramitam no STF, a ADI 5.527 e ADPF 403, ambas envolvendo os bloqueios dos serviços prestados pelo *WhatsApp*, motivadas pela impossibilidade de quebra de criptografia de ponta a ponta.

***ABSTRACT**: The purpose of this article is to understand the legal challenges posed by the use of end-to-end encryption, by comprehending the tool and analyzing the judicial decisions that determined the blocking of the WhatsApp Application by using end-to-end encryption. The work addressed the relationship of cryptography with fundamental rights, such as privacy, public security, state sovereignty, and economic freedom. Finally, the article analyzed the experience of some countries on the use of end-to-end cryptography and the Brazilian understanding on the subject, making a case study on the two actions that are being processed in the STF, ADI 5.527, and ADPF 403, both involving the blocking of services provided by WhatsApp, motivated by the impossibility of breaking end-to-end encryption.*

PALAVRAS-CHAVE: criptografia; privacidade; segurança.

***KEYWORDS**: cryptography; privacy; safety.*

INTRODUÇÃO

A sociedade atual é marcada pelo crescimento exponencial do uso da Internet e das tecnologias de informação e comunicação. E entre as tecnologias destacam-se os provedores de aplicação, que passaram a ser grandes aliados nas relações pessoais e profissionais. O *WhatsApp*, aplicativo de troca de mensagens instantâneas e um dos aplicativos mais utilizados no mundo, conta, hoje, com mais de 2 bilhões de usuários[4] e

[4] *Whatsapp* atinge 2 bilhões de usuários. *Forbes*, Brasil, Negócios, 12 fev. 2020. Disponível em: <https://forbes.com.br/last/2020/02/whatsapp-atinge-2-bilhoes-de-usuarios/>. Acesso em: 10 mai. 2020.

tem sido ferramenta importante para diversas esferas da sociedade: utilizam o aplicativo não apenas pessoas físicas, mas também pequenas, médias e grandes empresas que usam o provedor para impulsionar seus negócios, centros médicos para marcar consultas, sistema judiciário para notificar sobre processos e até mesmo organizações do terceiro setor para facilitar doações.

O *WhatsApp* é um dos grandes exemplos de serviço *on-line* que faz uso da criptografia de ponta a ponta, mas não é o único, diversos provedores de aplicação usam a tecnologia como forma de proteção aos seus usuários contra invasão de terceiros. Em tempos de pandemia de Covid-19, os ataques cibernéticos se intensificaram na mesma proporção que o tempo em que as pessoas permanecem conectadas, e tornou-se fundamental a manutenção de sistemas com alto nível de segurança dos usuários que proporcionem não apenas segurança contra informações de seus usuários, mas especialmente segurança com relação à proteção da privacidade, à liberdade de expressão e à liberdade econômica.

Para que seja possível a compreensão em torno dos desafios jurídicos que essa tecnologia impõe, faz-se necessário compreender a criptografia enquanto ferramenta e a função para a qual foi criada, além de investigar se, de fato, a "decriptação" é possível e por qual meio. Na sequência, pretende-se analisar os conflitos jurídicos em torno da criptografia, o caso instaurado no Supremo Tribunal Federal envolvendo os bloqueios dos serviços prestados pelo *WhatsApp*, motivados pela impossibilidade de quebra da criptografia de ponta a ponta, bem como a experiência internacional sobre a legitimidade do uso de criptografia.

1 BREVES COMENTÁRIOS SOBRE CRIPTOGRAFIA

A necessidade de se manter a comunicação privada e segura subsiste ao longo dos anos. Com o surgimento da Internet, o fluxo constante de informações e a predominância da comunicação *on-line*, verificou-se a imprescindibilidade de meios sofisticados para proteger dados do governo, empresas e particulares. Isso porque depositamos grande parte das informações de nossas vidas em nossos dispositivos móveis. Como precisamente exposto no voto da Relatora da ADI 5.527[5], Ministra Rosa Weber: "Parte significativa da vida privada de milhões de

[5] BRASIL. STF, ADI 5.527, Relª Min. Rosa Webber. Disponível em: <http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADC43votoRW.pdf>. Acesso em: 2 mai. 2020.

pessoas descortinam-se por meio dos aparelhos celulares, que quando ativados em nossas mãos convertem-se em janelas luminosas de nossa intimidade".

Assim, a vigilância, a reunião de dados específicos dos usuários, os ataques digitais contra a sociedade civil e a censura das atividades em linha despertaram a sociedade para a necessidade das pessoas de um nível maior de segurança para buscar, receber e difundir informações de qualquer espécie, sem que isso resultasse em riscos de repercussões, divulgações e vigilância de suas opiniões ou expressões.

Conforme o manual da segurança dos computadores NIST [NIST95][6], o termo segurança de computadores baseia-se em três objetivos principais, sendo eles confidencialidade, integridade e disponibilidade. Esses três conceitos abrangem os objetivos fundamentais de segurança tanto para dados quanto para serviços de informação e computação, formando, assim, a chamada tríade CIA (*confidentiality, integrity and availability*). Assim, no âmbito da segurança da informação, a criptografia – a arte da escrita secreta – desempenha um papel vital, provando ser uma ferramenta primária em segurança de informação, garantindo os objetivos fundamentais da tríade[7].

Até a década de 1970, a criptografia era utilizada unicamente por setores governamentais, "até o momento em que criptografadores independentes surpreenderam o mundo, demonstrando que a privacidade pode ser fabricada 'de ponta a ponta'[8] sem a ajuda de quaisquer recursos centralizados". Mas somente no final de 1980 surgiu a primeira aplicação criptográfica de massa, por meio do sistema de telefonia móvel digital. No entanto, foi o crescimento exponencial da Internet e, consequentemente, dos provedores de aplicação financeiro, como os bancos eletrônicos, que a criptografia passou a ser amplamente utilizada pela população, ainda que inconscientemente:

> Com a popularização da criptografia para uso de particulares, contudo, classificá-la como apenas produto de uso militar ou civil se tornou uma tarefa

[6] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. *An Introduction to Computer Security*: The NIST Handbook. Special Publication 800-12, out. 1995.

[7] KOOPS, E. J. *The Crypto Controversy*: A Key Conflict in the Information Society. Kluwer Law International. London/Boston: The Hague, 1998. p. 19.

[8] DIFFIE, Whitfield; LANDAU, Susan. *Privacy on the Line The Politics of Wiretapping and Encryption*, London: Massachusetts Institute of Technology, v. 7, n. 3, p. 313, 2007 (ISSN 2236-1677).

> 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).[9]

A criptografia envolve três conceitos básicos: o texto claro, o texto cifrado, a encriptação e a decriptação. A mensagem original é chamada de texto claro (*plaintext*) e a mensagem codificada é nominada como texto cifrado (*ciphertext*). Quando falamos de cifração ou encriptação, trata-se do processo de conversão do texto claro ao texto cifrado. Por sua vez, a decifração ou decriptação diz respeito à restauração do texto cifrado para o texto claro[10].

A criptologia é um termo geral que abarca o estudo de dois ramos, a criptoanálise e a criptografia. A primeira consiste no estudo das técnicas empregadas para decifrar a mensagem, ou seja, "a arte de quebrar sistemas criptográficos", sendo de essencial importância para os sistemas criptográficos modernos, pois, como bem ressalta Christof Paar[11], sem pessoas que tentam quebrar métodos criptográficos nunca iremos saber se eles são seguros ou não. Por sua vez, a criptografia em si pode ser definida como a "ciência da escrita secreta com o objetivo de ocultar o significado de uma mensagem". A realidade é que, sem perceber, todos utilizam a criptografia diariamente, principalmente porque a intensificação de troca de dados surgiu da necessidade de meios de

---

9 LIGUORI FILHO, Carlos Augusto; SALVADOR, João Pedro Favaretto. *Crypto Wars* e bloqueios de aplicativos: o debate sobre regulação jurídica da criptografia nos Estados Unidos e no Brasil. *Revista da Faculdade de Direito*, Curitiba: UFPR, v. 63, n. 3, p. 135-161, set./dez. 2018.

10 STALLINGS, William. *Criptografia e segurança de redes*. 6. ed. Trad. Daniel Vieira. São Paulo: Pearson Education do Brasil, 2014.

11 PAAR, Christof; PELZL, Jan. *Understanding Cryptography*: a textook for students and practitioners. New York: Springer Heidelberg Dordrecht London, 2009. p. 3.

comunicação privados e seguros, conforme destaca o *Travel guide to the digital world: Encryption policy for himan rights defenders*[12]:

> Manter dados e comunicações privados e seguros. Esse talvez seja o motivo mais comum pelo qual as pessoas usam criptografia. A criptografia nos permite comprar, depositar, enviar e receber comunicações sem medo de interferência ou vigilância. [...]
>
> Receber os dados como pretendidos. A criptografia garante a integridade dos dados; em outras palavras, que os dados recebidos são exatamente iguais ao que foram enviados, sem adição, exclusão ou exclusão modificação. (tradução livre)

Na maioria dos casos, o uso da criptografia não é percebida em razão da utilização de serviços que já incorporam essa tecnologia. Assim, a criptografia é utilizada para abrir a porta do carro por um dispositivo de controle remoto, conectar-se à Internet sem fio, comprar mercadorias com cartão de crédito, comunicar-se por meio de serviços de mensageria privada, utilizar navegadores de Web, programas de *e-mail* e até mesmo para cometer crimes.

E é especificamente nesse último ponto que a controvérsia da criptografia fica mais clara. Isso porque a mesma tecnologia que garante a privacidade e os avanços também é utilizada para o planejamento e cometimento de ilícitos. De um lado, há a crescente necessidade da sociedade de consumir produtos e serviços *on-line* de forma privada e segura, e, de outro, a crescente preocupação de que a proteção oferecida por serviços criptografados possa ser utilizada para uso ilícito, de forma a encobrir crimes.

Na obra *The Crypto Controversy: A Key Conflict in the Information Society*, publicada em 1999, Koops[13] já afirmava que a criptografia emergia com um grande problema para os governos, e questionava: "Como equilibrar os interesses conflitantes da privacidade e da segurança da informação, por um lado, com os interesses da aplicação da lei e da segurança nacional, por outro?" Sabe-

[12] GLOBAL PARTNERS DIGITAL. Travel Guide to The Digital World: Encryption Policy for Human Rights Defenders. London, 2017. Disponível em: <https://www.gp-digital.org/wp-content/uploads/2017/09/TRAVELGUIDETOENCRYPTIONPOLICY.pdf>. Acesso em: jun. 2020.

[13] KOOPS, E. J. *The Crypto Controversy*: A Key Conflict in the Information Society. Kluwer Law International. London/Boston: The Hague, 1998. p. 19.

se que a proteção da segurança nacional e o cumprimento de leis são valores básicos da sociedade; entretanto, por vezes competem com outro valor básico, a privacidade. A competição entre esses valores é quase injusta, já que a segurança nacional e a aplicação da lei são constituições políticas que são representadas pela maioria das organizações da sociedade.

Assim, "a privacidade não tem muito 'músculo' por trás dela. Como resultado, embora um apego à privacidade perdure e às vezes cresça, a privacidade é frequentemente violada"[14]. Com todos os avanços tecnológicos, frequentes monitoramentos e coletas de dados, o direito de ser deixado só, proposto em 1890 por Louis Brandeis e Samuel Warren, talvez não seja tão realista na atual sociedade informacional, especialmente porque:

> [...] em um mundo que diariamente invade nosso espaço pessoa, privacidade e confidencialidade no discurso permanecem importantes para a psique humana. Pensamentos e valores ainda se desenvolvem nas tradições milenares de fala, reflexões, argumentos, verdade e privacidade são essenciais. Nossas conversas podem ser com pessoas que estão longe, e a mídia eletrônica talvez possa transmitir discussões que podem ter ocorridos sobre uma mesa de cozinha ou em uma caminhada para o trabalho. Mas a confidencialidade – e a percepção de confidencialidade – são tão necessárias para a alma da humanidade como fazer pão é para o corpo.[15]

A partir das reflexões suscitadas, analisaremos no próximo capítulo os desafios jurídicos da criptografia, em especial no território brasileiro, e como os entraves com o sistema criptográfico não se limitam ao campo da segurança pública.

---

[14] DIFFIE, Whitfield; LANDAU, Susan. *Privacy on the Line The Politics of Wiretapping and Encryption*, London: Massachusetts Institute of Technology, v. 7, n. 3, p. 313, 2007 (tradução nossa). No original: "*Privacy has no such muscle behind it. As a result, although an attachment to privacy endures and at times grows, privacy is often violated*".

[15] Ibidem, p. 185 (tradução nossa). No original: "*But in a world that daily intrudes upon our personal space, privacy and confidentiality in discourse remain important to the human psyche. Thoughts and values still develop in the age-old traditions of talk, reflection, and argument, and trust and privacy are essential. Our conversations may be with people who are at a distance, and electronic media may transmit discussions that once might have occurred over a kitchen table or on a walk to work. But confidentiality – and the perception of confidentiality – are as necessary for the soul of mankind as bread is for the body*".

2 DESAFIOS JURÍDICOS EM TORNO DA CRIPTOGRAFIA

Nos anos de 2015 e 2016, o *WhatsApp* sofreu sucessivas suspensões de seus serviços no Brasil, pelo fato de ter se recusado a entregar em juízo o conteúdo de mensagens veiculadas no aplicativo. As ordens judiciais foram descumpridas pela empresa sob a alegação de impossibilidade técnica de cumprimento, considerando que seu sistema conta com criptografia de ponta a ponta, o que impede a interceptação de mensagens em tempo real. Apesar de o método de codificar mensagens ser usado há bastante tempo, inclusive pelo Estado, a discussão jurídica em torno da tecnologia tomou corpo recentemente quando a criptografia apresentou óbice ao poder do Estado.

O argumento do Juiz Marcel Maia Montalvão, prolator de uma das decisões mais emblemáticas de bloqueio do *WhatsApp*, deixa claro alguns dos desafios jurídicos impostos em torno da criptografia. Sob as lentes do Estado, nota-se a preocupação com a impossibilidade de interceptação das mensagens em tempo real, liberdade econômica e soberania nacional.

> Ora, é de clareza solar o perfeito enquadramento do comportamento arredio da Facebook no caso presente, e em tantos outros, neste País de vasta extensão territorial, considerando o 5º, maior no mundo neste particular. Vale dizer, obrigada está aquela recalcitrante em se submeter às leis brasileiras, pouco importando que sua controladora deite berço nos Estados Unidos. O fato é que oferece serviços no Brasil e aqui está instalada, auferindo lucros bilionários, conforme seu objetivo precípuo. Em casos de ordens judiciais, deve, sim, atender ao cumprimento destas, sob pena de "governar este país". Não fazendo, determinadas sanções serão aplicadas para dizimar seu comportamento violador das normas vigentes no Brasil. Os reflexos e as consequências de sua rebeldia somente àquela podem ser atribuídos, a par de invocar, sabiamente, mas sob subterfúgios, prejuízos a milhões de seus usuários, como se preocupada estivesse desde sempre.[16]

[16] Nesse período, uma série de decisões judiciais foram exaradas, solicitando o bloqueio do *WhatsApp*. Uma das sentenças de maior repercussão foi a exarada pelo Juiz Marcel Maia Montalvão da Vara

Nessa perspectiva, a criptografia acaba implicando um desafio ao Estado à medida que, pelo menos à primeira vista, enfraquece seu poder de vigilância como um todo. Um exemplo é a decisão referida, segundo a qual o Estado interpreta a impossibilidade de interceptação de mensagens e de quebra de sigilo, como abuso da liberdade econômica por parte do *WhatsApp*, além de enfraquecimento da soberania e ameaça à segurança pública.

Com o avanço dos debates jurisprudenciais sobre o *Whatsapp*, percebeu-se que a tecnologia empregada pelo *WhatsApp* impede não apenas ele, enquanto empresa, mas qualquer terceiro de interferir nas mensagens trocadas no aplicativo. Essa peculiaridade não é da plataforma, mas da tecnologia empregada, e não pode ser considerada um *bug* do sistema ou uma falha da empresa pela criação de uma tecnologia que impossibilita seu criador de ter acesso ao conteúdo que nele trafega. A criptografia de ponta a ponta também não indica estratégia da empresa para impedir a entrega de dados. A tecnologia empregada faz parte do modelo de negócio da empresa, que foi desenhado para oferecer privacidade, intimidade e liberdade de comunicação ao usuário. Neste contexto, o Desembargador Alvides Leopoldo e Silva Junior, nos autos do Agravo de Instrumento nº 2184235-15.2016.8.26.0000, manifestou-se sobre a tecnologia:

> [...] tal mensagem já estava protegida por criptografia ponta-a-ponta, o que passou a ser adotado pela *WhatsApp* desde o mês de abril/2016, o que significa que, sendo cifradas as mensagens, a provedora não tem como ler ou rastrear mensagens compartilhadas ou a origem da transmissão inicial, *sem precedente infiltração em grupos de conversas ou em canais ou hackeamento do aparelho*, mas apenas os usuários de cada extremo da mensagem protegida. [...].[17] (grifo nosso)

As decisões de bloqueio fundamentaram-se no art. 12, III, do Marco Civil da Internet[18]. Todavia, discute-se, se as ordens judiciais de suspensão de serviços

Criminal da Comarca de Lagarto no Sergipe, nos autos do Processo nº 201655090143, em 2016. A recusa da empresa motivou a suspensão dos serviços em todo o Brasil.

17 TJSP, Agravo de Instrumento nº 2184235-15.2016.8.26.0000, 2ª Câmara de Direito Privado, Rel. Alcides Leopoldo e Silva Junior, J. 21.02.2017.

18 "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

encontram amparo no Marco Civil da Internet ("Marco Civil"), afinal, da leitura atenta do art. 12 do MCI percebe-se que o preceito legal é voltado à proteção da privacidade, e não ao contrário. O art. 12, no entanto, dispõe sobre a penalidade de suspensão dos serviços, para os aplicativos que violem os direitos previstos nos arts. 10 e 11[19], que tratam da preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas e dos direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros. Percebe-se que o que é apenada é a violação da privacidade e de outros direitos dos usuários e, portanto, não há nada no Marco Civil da Internet que autorize a suspensão de serviços por ausência de cumprimento de ordem judicial que determine a entrega de conteúdo de mensagens. De acordo com o Marco Civil, as penalidades de suspensão temporária das atividades de provedores de conexão e de aplicações de Internet somente podem ser aplicadas nas hipóteses de descumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como aos direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros. Nesse sentido, é oportuno ressaltar o entendimento doutrinário sobre o tema:

> O Marco Civil da Internet, em especial no seu art. 12, não autoriza qualquer intervenção na infraestrutura da rede, muito menos o bloqueio de sites e aplicações de Internet, mas, ao contrário, preza pelo exercício da liberdade de expressão também no ambiente virtual. A razão disso é clara: o legislador não tinha como objetivo criar uma sanção que retirasse os serviços

isolada ou cumulativa: [...] suspensão temporária das atividades que envolvam os atos previstos no art. 11;
[...]"

19 "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.
[...]
Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.
[...]"

> do ar pela desobediência de uma ordem judicial, mas sim uma sanção que impossibilitasse as empresas de continuarem tratando os registros, dados pessoais e comunicações de forma irresponsável.[20]

Por óbvio, nem o provedor de aplicação nem qualquer pessoa física ou jurídica está desobrigada de cumprir uma ordem judicial legítima. O que se observa, no entanto, é que a ordem judicial de suspensão de serviço de comunicação, por ausência de entrega de mensagens, não encontra amparo no Marco Civil da Internet. Algumas inquietações surgem: A criptografia de ponta a ponta de fato impede órgãos de segurança pública de investigação de ilícitos? A quebra da criptografia resolverá os problemas da persecução penal dos infratores? As plataformas digitais que fazem uso da criptografia de ponta a ponta estão afrontando a soberania nacional? A quebra da criptografia significa aumento ou redução da segurança pública?

O fato é que essa tecnologia tem sido colocada em xeque pelo Estado, sob o argumento de impedir a segurança pública em determinados casos. No entanto, como exposto no questionamento anterior, é necessário refletir se, de fato, essa tecnologia tem impedido os órgãos de segurança pública de realizarem o trabalho de investigação e persecução penal frente às novas tecnologias e se a quebra da criptografia poderia significar êxito no deslinde de crimes e no fim do tráfico de drogas. Reportagem do Jornal *O Globo*, de 2016, relata que a Polícia Federal teria infiltrado agentes para driblar a criptografia. Essa operação ficou conhecida como "Hashtag", e a abordagem policial em grupos de conversa dos aplicativos *WhatsApp* e do *Telegram*, usados supostamente por adeptos do Estado islâmico, resultou na obtenção de informações sobre eventuais atentados que poderiam vir a acontecer nos Jogos Olímpicos do Rio 2016[21].

Na verdade, porém, a quebra da criptografia ponta a ponta não facilitará a persecução penal de infratores, o que possivelmente ocorrerá é a migração do infrator para outro tipo de plataforma e a vulnerabilidade dos cidadãos,

---

[20] VIOLA, Mario; ITAGIBA, Gabriel. Bloqueio de aplicações. In: SOUZA, Carlos Affonso; LEMOS, Ronaldo; BOTTINO, Celina (Coord.). *Marco Civil da Internet*: jurisprudência comentada. São Paulo: Revista dos Tribunais, 2018.

[21] MATSUURA, Sérgio; SCHIMITT, Luiz Gustavo. PF pode ter infiltrado agentes para driblar criptografia em *apps*. *O Globo*. Disponível em: <https://oglobo.globo.com/economia/pf-pode-ter-infiltrado-agentes-para-driblar-criptografia-em-apps-19758949. Publicado em 21/07/2016>. Acesso em: 14 jun. 2020.

que nenhuma relação possuem com ilícitos criminais[22]. Percebe-se, assim, que a ausência de criptografia não exporá o infrator, mas o cidadão cumpridor de seus deveres. Não foi o surgimento da criptografia de ponta a ponta que inviabilizou a investigação criminal. Há muitos outros meios de investigação e muitas outras deficiências estatais que não são estão ligadas à tecnologia. São problemas estruturais muito mais sérios, como corrupção, falta de investimento público, de auditoria, de programas de integridade, deficiência de mão de obra, entre outros. Como se observa, os desafios jurídicos em torno da criptografia de ponta a ponta não se resumem em um debate binário entre segurança pública e privacidade.

3 COMO OS PAÍSES TEM ENFRENTADO A CRIPTOGRAFIA

Uma das formas mais antigas de representação do exercício da soberania é o controle da comunicação. O crescimento da Internet e das Tecnologias de Informação e Comunicação (TIC) foi e ainda continua sendo constante e ascendente. A informação migrou para o mundo *on-line*, sendo cada vez mais difícil nos desvincularmos da revolução informacional. Assim, "à medida que a sociedade evolui, particularmente à medida que a tecnologia evolui, o poder do governo de controlar as comunicações muda"[23].

Com a evolução criptológica não foi diferente, conforme pontuado no primeiro capítulo. Foi a partir do custo decrescente da computação e do aumento das necessidades civis da década de 70 que acadêmicos passaram a explorar a arte de criptografar. O poder de criptografar antes centralizado nas mãos governamentais passou a ser desenvolvido por entes privados. Essa "abertura" da criptografia gerou preocupação e diversos governos buscaram controlar a sua difusão. Em razão do caráter global da Internet, o debate político a respeito da encriptação de conteúdos precisa ser abordado de forma conjunta. Diversas organizações internacionais construíram normas conjuntas de política

[22] Ver a esse respeito o voto da Ministra Rosa Weber: BRASIL. Supremo Tribunal Federal, ADI 5.527, p. 7. Disponível em: <http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADC43votoRW.pdf>. Acesso em: 2 mai. 2020.

[23] DIFFIE, Whitfield; LANDAU, Susan. *Privacy on the Line The Politics of Wiretapping and Encryption*, London: Massachusetts Institute of Technology, v. 7, n. 3, 2007 (tradução nossa). No original: "*As society evolves, particularly as technology evolves, the government's power to control communications changes*".

de encriptação. Uma delas é a recomendação da OCDE de 27 de março de 1997, que estabelece orientações para a política de criptografia[24].

A Organização das Nações Unidas elaborou um relatório, no âmbito do Conselho de Direitos Humanos, ressaltando que a criptografia e o anonimato são conceitos que proporcionam a privacidade e a segurança necessárias para o exercício da liberdade de expressão na era digital, sendo essenciais para o exercício de diversos outros direitos. Em uma de suas recomendações, David Keyne afirmou que os Estados não devem restringir a encriptação, e, caso houver, deve ser estritamente limitada de acordo com alguns princípios, como proporcionalidade, legitimidade e necessidade[25].

Em um recente relatório, a Unesco expôs cinco estudos de casos sobre países e suas estruturas legais e políticas em relação à encriptação, analisando a tipologia geral de possíveis limitações e também de medidas positivas sobre a tecnologia. Entre as constatações, verificou-se uma variedade grande de limitações impostas à encriptação, podendo equivaler à proibição geral do uso, a condições sobre o uso, a neutralização, os mandados de desincriptação para que provedores de comunicação sejam capazes de ajudar no acesso legal do conteúdo, o que representa proibição no desenvolvimento de criptografia de ponta a ponta.

Verificou-se, também, a presença de algumas legislações positivas que estabelecem medidas de estímulo à adoção de encriptação por diversos atores da sociedade. Além disso, constataram que as leis de privacidade de dados também incentivam e determinam a implantação e o cuidado da criptografia[26].

Uma das mais recentes manifestações do embate entre o Poder Público e Privado relacionada à tentativa dos governos em ter acesso legal de conteúdo foi a carta enviada por autoridades dos Estados Unidos, do Reino Unido e da Austrália ao CEO do Facebook, Mark Zuckemberg. No documento, as autoridades

---

[24] Disponível em: <http://www.oecd.org/internet/ieconomy/guidelinesforcryptographypolicy.htm>. Ver, a esse respeito também: <https://www.oecd.org/sti/consumer/34023696.pdf> [Criptografia no C(97)62/FINAL], documentos acessados em 28 jun. 2020.

[25] 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/23/40. 17 de abril de 2013. § 47, p. 21. Disponível em: <http://ap.ohchr.org/documents/dpage_s.aspx?m=85>.

[26] UNESCO. Direitos humanos e criptografia. Série da Unesco sobre liberdade na Internet. Trad. Instituto de Tecnologia e Sociedade do Rio (ITS). França, 2016. p. 36 (ISBN 978-92-3-100185-7). Disponível em: <https://itsrio.org/wp-content/uploads/2018/10/direitos-humanos-e-criptografia-1.pdf>.

alertam que o aprimoramento da criptografia de ponta a ponta nos serviços de mensagens dificultaria a prevenção de crimes, como exploração infantil, e, por esse motivo, solicitaram que a empresa viabilizasse uma "forma de acesso legal ao conteúdo em um formato legível e usável", por meio das chamadas *backdors*[27]. Esse pedido, do Estados Unidos, do Reino Unido e da Austrália, no entanto, vai de encontro à posição de diversos países, que se posicionaram contra a implementação de um acesso excepcional pelo Estado:

> [...] certos países, como a Alemanha ou os Países Baixos, assumiram uma posição rigorosa contra as restrições de encriptação na Internet. Em uma declaração conjunta, a Agência Europeia para a Segurança das Redes e da Informação (*European Agency for Network and Information Security* – "ENISA") e a Europol também tomaram uma posição contra a introdução de *backdoors* em produtos de encriptação. Recentemente, os Ministros do Interior da França e da Alemanha afirmaram conjuntamente a necessidade de trabalhar em soluções para os desafios que a aplicação da lei pode enfrentar como resultado da encriptação de ponta-a-ponta, em particular, quando oferecida por uma jurisdição estrangeira.[28]

Embora existam diversas iniciativas legislativas e julgados favoráveis ao uso da tecnologia, como é o caso brasileiro apresentado no próximo capítulo, diversos países se posicionam favoráveis à interferência na encriptação de ponta a ponta. No entanto, tal interferência não encontra aplicabilidade prática e científica, porque a maioria das propostas é impossível de aplicação ou ineficazes.

Conforme pronunciado pela Unesco, essas iniciativas "reduziriam a segurança para todos ao criar vulnerabilidades e não conseguiriam alcançar seus objetivos finais. As restrições teriam também efeitos prejudiciais graves na segurança cibernética e comércio eletrônico"[29]. Além do mais, é necessário não só considerar os interesses governamentais, mas também daqueles que

---

[27] MCALEENAN, Kevin K.; DUTTON, Hon Peter; PATEL, Priti Hon. Open Letter: Facebook's "privacy first" Proposals. Disponível em: <https://www.justice.gov/opa/press-release/file/1207081/download>. Acesso em: 2 fev. 2020.

[28] Ibidem, p. 36.

[29] Ibidem, p. 38.

usufruem diariamente da criptografia. Após escândalos de vazamento de dados de usuários, as empresas tecnológicas buscaram aumentar o uso da encriptação para garantir a proteção de informações e comunicações. Assim, o incentivo contrário por parte do governo pode resultar em um retrocesso quanto à proteção de dados pessoais, liberdade de expressão, comunicação e liberdade econômica.

4 A ADPF 403 E A ADI 5527 INTERPOSTAS NO STF E O CONFLITO JURÍDICO INSTAURADO EM TORNO DA CRIPTOGRAFIA

Como explanado no primeiro capítulo, a criptografia impede que terceiros possam monitorar, armazenar ou modificar o conteúdo trocado pelos usuários, incluindo o próprio *WhatsApp*. A Polícia Federal, parte autora de uma das ações propostas contra o *WhatsApp*, pleiteava o conteúdo das mensagens trocadas no aplicativo para a investigação de crimes, sob o argumento de que a recusa da empresa na entrega de informações prejudicava a segurança pública. Considerando a repercussão nacional que a suspensão dos serviços ocasionou, especialmente pelo fato de ter atingido boa parte da população brasileira que usa o aplicativo para seus relacionamentos pessoais e profissionais, o Partido Popular Socialista e o Partido da República ingressaram com duas ações no STF sobre o tema.

Uma das ações é a arguição de descumprimento de preceito fundamental (ADPF 4030), que foi motivada pela suspensão dos serviços do aplicativo *WhatsApp*, em todo território nacional, pelo prazo de 72 horas, em cumprimento à decisão de 02.05.2016, exarada nos autos da Medida Cautelar nº 201655000183, da Vara Criminal de Lagarto/SE. Apesar de o *WhatsApp* ter informado que não possuía capacidade técnica de acessar as mensagens de seus usuários por conta da criptografia de ponta a ponta, o Juiz de Lagarto/SE entendeu a recusa da empresa como desobediência e proferiu a seguinte decisão:

> [...] não se mostra razoável a rebeldia da empresa em querer impor uma desobediência confessa à legislação nacional. Mantendo-se nesse comportamento arredio aloca-se a ilegalidade. Ou seja, encontra-se em território brasileiro atuando ilegalmente, sob os olhares inertes de quem dever/poder de vigilância deveria ser exercido a fim de obstar o desrespeito provocador de uma Empresa que se arvora em descumprir as ordens de diversos Juízos no território brasileiro, levando este Magistrado

> a determinar a prisão do seu Vice-Presidente para a América Latina, em data muito recente. Aqui, não se atribui ao *Facebook* a responsabilidade direta por uma organização criminosa, pelo que se apresenta. Mas, diante de sua recalcitrância inconcebível, contribui para tanto, por razoes unicamente comerciais e seu desejo, legal, de lucros bilionários. A conhecida "febre do ouro".[30]

O PPS buscou a Suprema Corte por meio da ADPF, para ser declarada a impossibilidade de os provedores de aplicação serem obrigados a entregar o conteúdo das mensagens veiculadas em seus aplicativos, por entender que tal medida representa uma violação ao direito à liberdade de comunicação, prevista no art. 5º, IX, da Constituição Federal. Em liminar, nos autos da ADPF, o Ministro Ricardo Lewandowsk se posicionou contra a suspensão do serviço, entendendo que a medida era desproporcional e ofendia a liberdade de expressão:

> A suspensão do serviço do aplicativo *WhatsApp*, que permite a troca de mensagens instantâneas pela rede mundial de computadores, da forma abrangente como foi determinada, parece-me violar o preceito fundamental da liberdade de expressão aqui indicado, bem como a legislação de regência sobre o tema. Ademais, a extensão do bloqueio a todo o território nacional, afigura-se, quando menos, medida desproporcional ao motivo que lhe deu causa.[31]

A segunda ação, ADI 5527, proposta pelo Partido da República, foi motivada por três sucessivas decisões proferidas por juízos criminais determinando o bloqueio do *WhatsApp* em todo o território nacional, em razão da sua impossibilidade de cumprir ordens de interceptação de mensagens dos usuários do aplicativo. O objeto da ADI 5527 é a inconstitucionalidade da penalidade de suspensão de aplicativos de troca de mensagens, em caso de descumprimento de ordem judicial, imposta nos incisos III e IV do art. 12 do

---

30 TJSE, Juízo da Vara Criminal da Comarca de Lagarto, Processo nº 201655090143, Juiz Marcel Maia Montalvão, J. 26.04.2016.

31 BRASIL. STF, ADPF 5527, Rel. Min. Edson Fachin. Disponível em: <http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADPF403voto.pdf>. Acesso em: 2 mai. 2020.

Marco Civil da Internet, considerando especialmente a função social desse tipo de serviço.

O Ministro Edson Fachin, Relator da ADPF, e a Ministra Rosa Weber, Relatora da ADI 5527, realizaram audiência pública em 2 e 5 de junho 2017. Foram ouvidas as partes, terceiros interessados e diversos *amicus curiae*, que trouxeram importantes contribuições aos autos, não apenas sob o viés técnico, da ferramenta em si, mas também do ponto de vista social, econômico e até político. Destaca-se posicionamento do Comitê Gestor da Internet e da Associação Brasileira de Magistrados, enquanto *amicus curiae*. O primeiro favorável ao uso de criptografia em tecnologias atuais e o segundo contrário:

> A criptografia e outras tecnologias de segurança da informação são convergentes à ordem pública, na medida em que a sua adoção e difusão são barreiras de contenção à escalada de crimes cibernéticos e de atividades de vigilância em massa. Pode-se dizer que para cada uso ilícito de tais tecnologias, há uma pletora de usos legítimos que não se restringem à proteção da privacidade de indivíduos, mas sobretudo – e em um número significativo – de transações comerciais, de informações governamentais confidenciais, entre outras coisas.
>
> Não viola o princípio da livre comunicação e da continuidade do serviço, porque a eventual decisão de suspensão ou de proibição do serviço decorrerá da conduta do *WhatsApp* ou congênere de não se submeter à legislação penal brasileira.

O julgamento das ações iniciou em 27.05.2020 com a leitura dos votos dos Relatores. A Ministra Rosa Weber, Relatora da ADI, foi a primeira a pronunciar seu voto e fez ponderações importantes para a sociedade, entre elas que o Estado não pode compelir a empresa a oferecer um serviço menos seguro e vulnerável para cumprir ordem judicial a respeito, o que significaria tornar ilegal a criptografia. Pontuou que a criptografia consiste em uma ferramenta indispensável para garantir o direito à privacidade e que o argumento de que ela é usada para ilícito criminal não a deslegitima, afinal, a "descriptografia" não seria um óbice para a atividade ilícita, usuários criminosos migrariam para

outro meio de comunicação. Assim, em sede de ADI, concluiu que as *mens legis* das sanções do art. 12 do Marco Civil da Internet é voltada à proteção da privacidade, e não ao contrário. O que é apenada é a violação da privacidade e de outros direitos dos usuários. Não há nenhum dispositivo, no Marco Civil da Internet, que autorize a suspensão de serviços por ausência de cumprimento de ordem judicial que determine a entrega de conteúdo de mensagens.

O voto da Ministra foi pela improcedência quanto à declaração de inconstitucionalidade, sem redução de texto, do art. 12, III e IV, da Lei nº 12.965/2014 e procedente quanto ao pedido de interpretação conforme a constituição do art. 10, § 2º, da Lei nº 12.965/2014. A decisão da Relatora declarou, ainda, que 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 e para fins de investigação criminal ou instrução processual penal. Além disso, determinou em seu voto que as penalidades de suspensão temporária das atividades de provedores de conexão e de aplicações de Internet somente podem ser aplicadas nas hipóteses de descumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como aos direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros, o que impede novos bloqueios do *WhatsApp* por negativa de entrega de mensagens criptografadas de seus usuários.

O Ministro Edson Fachin, Relator da ADPF 403, em seu voto, entendeu procedente a arguição de descumprimento de preceito fundamental e declarou a inconstitucionalidade parcial sem redução de texto tanto do inciso II do art. 7º quanto do inciso III do art. 12 da Lei nº 12.965/2014, e deslegitimou qualquer ordem judicial que exija acesso a conteúdo de mensagem criptografada ponta a ponta ou que, por qualquer outro meio, enfraqueça a proteção criptográfica de aplicações da Internet. O voto do Ministro Edson Fachin asseverou que ordens judiciais, ainda que para fins de investigação criminal ou instrução processual penal, não podem obrigar provedores de aplicação a mudarem seu sistema de criptografia. E mais, que

> o risco causado pelo uso da criptografia ainda não justifica a imposição de soluções que envolvam acesso excepcional ou ainda outras soluções que diminuam a proteção garantida por uma criptografia forte, penso

> que não há como obrigar que as aplicações de internet que ofereçam criptografia ponta-a-ponta quebrem o sigilo do conteúdo de comunicações, ao menos à luz das informações que traduzem o consenso científico atual sobre a matéria. [...] Em síntese, senhor Presidente e eminentes pares, no atual estágio de desenvolvimento da Internet, a criptografia forte é, de acordo com as principais evidências científicas, o mecanismo por excelência de garantia do relevantíssimo direito à privacidade.[32]

Apesar de o Ministro Alexandre de Moraes ter pedido vista e suspendido o julgamento das duas ações, restou cristalina a importância do avanço de novas tecnologias para a tutela da integridade do cidadão em ambiente *on-line*.

CONCLUSÃO

Observamos, nos últimos meses, impulsionado pela pandemia de Covid-19, um verdadeiro êxodo do ambiente *off-line*. Houve um acelerado movimento migratório do mundo "real" para o *on-line*, o que modificou drasticamente a forma das pessoas se relacionarem. No momento atual de pandemia, os aplicativos de videochamada passaram a ser considerados serviços imprescindíveis para se manter o ensino a distância, os negócios funcionando, as famílias se reunindo, os julgamentos acontecendo. No entanto, um desses aplicativos foi objeto de escândalos e queda do preço de suas ações por não manter um alto nível de criptografia em seus serviços. Como se vê, ainda que diversos outros avanços no âmbito da segurança na informação tenham surgido, atualmente, a criptografia é uma das mais efetivas formas de garantia de privacidade no mundo eletrônico.

Os embates sobre as formas de controle de comunicação estão longe de ser resolvidos. Para tanto, questões sensíveis como esta necessitam de amplos debates e contribuições multisetoriais. As regulamentações propostas devem considerar o caráter global da Internet e a multinacionalidade das empresas de tecnologia. A Internet de hoje não será a Internet de amanhã e limitar a inovação e os avanços em segurança pode representar um grande retrocesso, considerando

[32] BRASIL. STF, ADPF 5527, Rel. Min. Edson Fachin. Disponível em: <http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADPF403voto.pdf>. Acesso em: 2 mai. 2020.

especialmente que a criptografia de ponta a ponta não é um óbice à segurança pública, e sim uma ferramenta que estimula a segurança pública.

REFERÊNCIAS

BRASIL. Supremo Tribunal Federal, ADI 5.527, Relatora Ministra Rosa Webber. Disponível em: <http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADC43votoRW.pdf>. Acesso em: 2 maio 2020.

_____. ADPF 5527, Relator Ministro Edson Fachin. Disponível em: <http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADPF403voto.pdf>. Acesso em: 2 mai. 2020.

DIFFIE, Whitfield; LANDAU, Susan. *Privacy on the Line The Politics of Wiretapping and Encryption*, London: Massachusetts Institute of Technology, v. 7, n. 3, 2007 (ISSN 2236-1677).

GLOBAL PARTNERS DIGITAL. Travel Guide to The Digital World: Encryption Policy for Human Rights Defenders. London, 2017. Disponível em: <https://www.gp-digital.org/wp-content/uploads/2017/09/TRAVELGUIDETOENCRYPTIONPOLICY.pdf>. Acesso em: jun. 2020.

KOOPS, E. J. *The Crypto Controversy*: A Key Conflict in the Information Society. Kluwer Law International. London/Boston: The Hague, 1998.

LIGUORI FILHO, Carlos Augusto; SALVADOR, João Pedro Favaretto. *Crypto Wars* e bloqueios de aplicativos: o debate sobre regulação jurídica da criptografia nos Estados Unidos e no Brasil. *Revista da Faculdade de Direito*, Curitiba: UFPR, v. 63, n. 3, p. 135-161, set./dez. 2018.

MCALEENAN, Kevin K.; DUTTON, Hon Peter; PATEL, Priti Hon. Open Letter: Facebook's "privacy first" Proposals. Disponível em: <https://www.justice.gov/opa/press-release/file/1207081/download>. Acesso em: 2 fev. 2020.

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/23/40. 17 de abril de 2013. § 47. Disponível em: <http://ap.ohchr.org/documents/dpage_s.aspx?m=85>.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. *An Introduction to Computer Security*: The NIST Handbook. Special Publication 800-12, out. 1995.

O GLOBO. PF pode ter infiltrado agentes para driblar criptografia em *apps*, 21 jul. 2016. Disponível em: <https://oglobo.globo.com/economia/pf-pode-ter-infiltrado-agentes-para-driblar-criptografia-em-apps-19758949>. Acesso em: 14 jun. 2020.

PAAR, Christof; PELZL, Jan. *Understanding Cryptography*: a textook for students and practitioners. New York: Springer Springer Heidelberg Dordrecht London, 2009.

STALLINGS, William. *Criptografia e segurança de redes*. 6. ed. Trad. Daniel Vieira. São Paulo: Pearson Education do Brasil, 2014.

TJSP. Agravo de Instrumento nº 2184235-15.2016.8.26.0000, 2ª Câmara de Direito Privado, Rel. Alcides Leopoldo e Silva Junior, J. 21.02.2017.

UNESCO. Direitos humanos e criptografia. Série da Unesco sobre liberdade na Internet. Trad. Instituto de Tecnologia e Sociedade do Rio (ITS). França, 2016. ISBN 978-92-3-100185-7. Disponível em: <https://itsrio.org/wp-content/uploads/2018/10/direitos-humanos-e-criptografia-1.pdf>.

VIOLA, Mario; ITAGIBA, Gabriel. Bloqueio de aplicações. In: SOUZA, Carlos Affonso; LEMOS, Ronaldo; BOTTINO, Celina (Coord.). *Marco Civil da Internet*: jurisprudência comentada. São Paulo: Revista dos Tribunais, 2018.

Submissão em: 20.10.2020
Avaliado em: 21.10.2020 (Avaliador A)
Avaliado em: 11.11.2020 (Avaliador B)
Aceito em: 11.11.2020