DOI: 10.12818/P.0304-2340.2017v71p607

WHATSAPP E A CRIPTOGRAFIA PONTO-A-PONTO: TENDÊNCIA JURÍDICA E O CONFLITO PRIVACIDADE VS. INTERESSE PÚBLICO

WHATSAPP AND END-TO-END ENCRYPTION: LEGAL TREND AND THE CONFLICT PRIVACY VS. PUBLIC INTEREST

Tarcisio Teixeira[*]
Paulo Henrique Sabo[**]
Isabela Cristina Sabo[***]

RESUMO: Diante da atual polêmica gerada pelo aplicativo WhatsApp ao lançar a criptografia "ponto-a-ponto" (*end-to-end* – E2E), a pesquisa aborda, por meio de um estudo interdisciplinar, quais os impactos jurídicos provocados pela postura da empresa e sua consonância com as legislações brasileiras. Utilizando-se o método matemático experimental e expondo-se brevemente as técnicas criptográficas comuns, o estudo perquire o tempo aproximado para decifrar uma única mensagem gerada pelo aplicativo, considerando aspectos como o nível do sistema de segurança utilizado pela empresa e hardwares necessários. A par do método dedutivo, analisa-se os efeitos que essa complexidade em torno do acesso às mensagens suscita quanto às disposições da Lei n. 12.965/2014

ABSTRACT: *In front of the current controversy generated by WhatsApp in launching the end-to-end encryption (E2E), the research addresses, through an interdisciplinary study, which legal impacts are caused by the attitude of the company and its accordance with Brazilian legislations. Using the experimental mathematical method and briefly exposing the common cryptographic techniques, the study calculates the approximate time to decipher a single message generated by the application, considering aspects such as the level of the security system used by the company and the required hardware. Along with the deductive method, it analyzes the effects that this complexity surrounding the access to messages raises to the provisions of Law 12.965/2014 (Brazilian Civil Rights*

* Professor Adjunto de Graduação e Pós-graduação *lato sensu* e *stricto sensu* da Universidade Estadual de Londrina. Doutor e Mestre em Direito Comercial pela Universidade de São Paulo.
E-mail: contato@tarcisioteixeira.com.br.

** Aluno do Curso de Doutorado do Programa de Pós-Graduação em Engenharia Elétrica da Universidade Estadual de Campinas. Mestre e Graduado em Ciência da Computação pela Universidade Estadual de Maringá. Professor Adjunto de Graduação da Universidade Tecnológica Federal do Paraná, Campus Campo Mourão.
E-mail: phsabo@gmail.com.

*** Mestre em Direito pela Universidade Estadual de Londrina. Graduada em Direito pela Universidade Estadual de Maringá.
E-mail: isabelasabo@gmail.com.

(Marco Civil da Internet), sobretudo quanto à configuração de responsabilidade civil. Por fim, afere-se a respeito do conflito entre a necessidade de investigação policial e a proteção da privacidade, para ao final concluir se as recentes determinações e bloqueios judiciais estão sendo o melhor caminho para solucionar a questão e harmonizar os interesses envolvidos.

PALAVRAS-CHAVE: Criptografia E2E. Responsabilidade civil. Conflito de interesses.

Framework for the Internet), particularly to the configuration of civil liability. Finally, it evaluates about the conflict between the need for police investigation and the privacy protection, to conclude whether the recent judicial determinations and deadlocks are being the best way to resolve the issue and harmonize the involved interests.

KEYWORDS: *E2E encryption. Civil liability. Conflicting interests.*

INTRODUÇÃO

A sociedade da informação é uma realidade irreversível, pois a inserção da tecnologia no cotidiano das pessoas cada vez mais gera um intervalo mínimo entre a sensação de uma novidade e o que, em seguida, vem a se tornar uma necessidade. É neste cenário que aplicativos de troca de mensagens obtidos gratuitamente e de utilização por simples conexão à Internet podem alcançar, para alguns, a categoria de essencial à atividade humana e/ou corporativa, em vista da comunicação viabilizada pela alta velocidade e sem custos financeiros diretos.

Como consequência natural, a circulação de dados e informações entre pessoas demanda certa segurança para garantir um mínimo de privacidade. Empresas do ramo de tecnologia de informação têm buscado técnicas protetivas para tanto, tal como o uso da criptografia em sistemas operacionais e aplicativos.[1] O WhatsApp é um aplicativo de Internet que melhor representa esse contexto, sobretudo ao lançar o sistema de criptografia "ponto-a-ponto" (*end-to-end* – E2E) no intuito de garantir maior proteção aos seus usuários. No entanto, a nova técnica gerou confrontos polêmicos com o Poder Judiciário em razão da empresa responsável

1 Dentre as mais variadas funções da criptografia para usuários comuns, cabe destacar: a) proteção de dados sigilosos armazenados em computador, como arquivo de senhas e Declaração de Imposto de Renda; b) criação de uma área (partição) específica em computador, na qual todas as informações que forem lá gravadas serão automaticamente criptografadas; c) proteção de backups contra acesso indevido, principalmente aqueles enviados para áreas de armazenamento externo de mídias; d) proteção das comunicações realizadas pela Internet, como e-mails enviados/recebidos e operações bancárias e comerciais realizadas (CERT.BR, online).

não atender às ordens judiciais para fornecimento de mensagens em determinados casos investigatórios.

Na primeira seção será narrado o histórico de bloqueios decorrentes de decisões judiciais e a atual situação perante o Supremo Tribunal Federal, a fim de contextualizar o problema que se pretende enfrentar. Na segunda seção, será utilizado o método matemático experimental a fim de expor, brevemente, as técnicas criptográficas comuns, calculando o tempo aproximado para decifrar uma única mensagem gerada pelo aplicativo, considerando aspectos como o nível do sistema de segurança utilizado pela empresa e hardwares necessários.

Abordada a nova sistemática computacional do WhatsApp, a partir do método dedutivo (compreensão da premissa maior à compreensão do caso específico), na terceira e quarta seções será enfrentado o problema principal deste estudo, qual seja, se a criptografia E2E efetivamente conflita com os ditames da atual legislação brasileira, sobretudo com o Marco Civil da Internet (Lei n. 12.965/2014), recentemente regulamentado pelo Decreto n. 8.771/2016, como também com os princípios constitucionais adotados no país.

Sob o enfoque legal mencionado, será examinado nestes tópicos a respeito da responsabilidade civil pela circulação de conteúdo indevido, agora criptografado, e futuras posições a serem tomadas pelas empresas de Tecnologia da Informação. Ainda, permanecendo com método dedutivo, será analisado, em meio às decisões tomadas pelo Poder Judiciário sobre o assunto, a garantia da privacidade dos indivíduos e o segredo empresarial em contraposição com a garantia publicidade das informações com vistas à segurança e interesse públicos.

Após esse estudo, será traçada uma hipótese ao problema indicado, apresentando respostas aos questionamentos: a criptografia E2E é incompatível com o ordenamento jurídico brasileiro? A sanção judicial ao WhatsApp, na ótica do Marco Civil da Internet e da Constituição Federal, é viável ou não à sociedade brasileira?

Justifica-se que a investigação não será exaurida neste estudo, dada a complexidade das questões mencionadas, notadamente por atingir níveis transnacionais e cuja discussão possui repercus-

são mundial. O que se propõe é uma análise acurada do método criptográfico E2E e seu diálogo com a legislação brasileira, a fim de refletir sobre sua aceitação e convívio no atual cenário social.

2 CONTEXTUALIZAÇÃO DO PROBLEMA: HISTÓRICO DOS BLOQUEIOS DO WHATSAPP

No início de abril de 2016, o WhatsApp anunciou a utilização da criptografia "ponto-a-ponto" (*end-to-end* – E2E) nas mensagens enviadas entre usuários do aplicativo, a ser executada em qualquer plataforma.[2] Ou seja, com a nova técnica, somente usuários em comunicação passam a ter acesso às mensagens compartilhadas. Nem mesmo a própria empresa, segundo ela, terá acesso ao conteúdo da comunicação.[3] Entretanto, a novidade gerou embates polêmicos com o Poder Judiciário, estando atualmente em discussão no Supremo Tribunal Federal. A fim de contextualizar o leitor da problemática enfrentada nessa pesquisa, expõe-se a seguir um breve histórico dos conflitos ocorridos.

Antes mesmo de apresentar a criptografia ponto-a-ponto, o aplicativo, hoje de propriedade da empresa Facebook,[4] sofreu algumas sanções judiciais por não colaborar com determinadas investigações. Em dezembro de 2015, o WhatsApp foi bloqueado por 48 horas por uma determinação da 1ª Vara Criminal de São Bernardo do Campo (SP). A decisão foi proferida pela juíza Sandra Regina Nostre Marques em um procedimento criminal, que corre em segredo de justiça.[5] Porém, no dia seguinte, o desembargador Xavier de Souza, da 11ª Câmara Criminal do Tribunal de Justiça

2 "WhatsApp's Signal Protocol integration is now complete" (OPEN WHISPER SYSTEMS, 2016, online).

3 "A criptografia ponto-a-ponto do WhatsApp assegura que somente você e a pessoa com que você está se comunicando podem ler o que é enviado e ninguém mais, nem mesmo o WhatsApp" (WHATSAPP, online-a).

4 "Facebook says it has wrapped up its landmark $19 billion acquisition of WhatsApp" (OLSON, 2014, online).

5 "Justiça determina bloqueio do aplicativo WhatsApp" (TRIBUNAL DE JUSTIÇA DO ESTADO DE SÃO PAULO, 2015a, online).

do Estado de São Paulo determinou o restabelecimento do aplicativo, destacando que "[...] em face dos princípios constitucionais, não se mostra razoável que milhões de usuários sejam afetados em decorrência da inércia da empresa".[6]

Em março de 2016 o juiz da Vara Criminal de Lagarto (SE), Marcel Maia Montalvão, decretou a prisão de Diego Jorge Dzodan, vice-presidente do Facebook na América Latina, motivada pelo descumprimento da ordem judicial em um processo envolvendo tráfico de drogas interestadual, no qual a Polícia Federal solicitou ao Juízo a quebra do sigilo de mensagens trocadas pelo WhatsApp. No entanto, a empresa Facebook, mesmo diante de várias oportunidades, não liberou as conversas solicitadas à Policia Federal, o que motivou a prisão do responsável pela empresa no Brasil. Na madrugada do dia seguinte, o desembargador plantonista Ruy Pinheiro da Silva, do Tribunal de Justiça do Estado de Sergipe, concedeu *habeas corpus*.[7]

Novamente, em maio de 2016, o juiz Marcel Maia Montalvão, da Vara Criminal de Lagarto (SE), determinou a suspensão dos serviços do aplicativo WhatsApp em todo território nacional. O magistrado atendeu a uma medida cautelar ingressada pela Polícia Federal, com parecer favorável do Ministério Público, em virtude do não atendimento, mesmo após o pedido de prisão do representante do Facebook no Brasil, da determinação judicial de quebra do sigilo das mensagens do aplicativo para fins de investigação criminal sobre crime organizado de tráfico de drogas na comarca.[8] Isso em razão da empresa justificar que a ordem judicial não poderia ser cumprida por razões técnicas. O aplicativo já contava com o método de criptografia ponto-a-ponto, ao passo que o descumprimento se atribuiu ao fato de os dados provenientes do uso do programa não ficarem armazenados no servidor ou em um banco de informações do provedor, mas nos próprios aparelhos telefônicos dos usuários.

6 "TJSP concede liminar para restabelecer WhatsApp" (TRIBUNAL DE JUSTIÇA DO ESTADO DE SÃO PAULO, 2015b, online).

7 "Nota sobre a prisão do vice-presidente do Facebook" (TRIBUNAL DE JUSTIÇA DO ESTADO DE SERGIPE, 2016c, online).

8 "Juiz criminal de Lagarto determina suspensão do WhatsApp por 72 horas" (TRIBUNAL DE JUSTIÇA DO ESTADO DE SERGIPE, 2016b, online).

No dia seguinte, a decisão foi revogada, em segunda instância, pelo desembargador Ricardo Múcio Santana de Abreu Lima.[9]

Esse fato aproximou-se ao ocorrido no caso FBI vs. Apple, envolvendo suspeitas de ataques terroristas em San Bernardino, Califórnia (CA), em 16 de fevereiro de 2016,[10] e tráfico de drogas e armas no Brooklyn, Nova Iorque (NY), em 29 de fevereiro de 2016,[11] nos quais a justiça norte-americana determinou que a empresa entregasse à polícia o conteúdo das mensagens trocadas via iMessage.[12] A companhia respondeu que isso não seria possível em razão de só ter acesso ao texto criptografado das conversas. Inclusive, o caso serviu de incentivo ao WhatsApp e outros aplicativos desenvolverem seu sistema criptográfico para o método ponto-a-ponto, situação denominada atualmente de "*crypto war*".[13]

Em julho de 2016, o bloqueio ocorreu novamente, porém por poucas horas. A decisão partiu da juíza Daniela Barbosa Assumpção de Souza, da 2ª Vara Criminal de Duque de Caxias (RJ). De acordo com o processo, o Facebook descumpriu a determinação

9 "Desembargador Ricardo Múcio decide pelo cancelamento da suspensão do WhatsApp" (TRIBUNAL DE JUSTIÇA DO ESTADO DE SERGIPE, 2016a, online).

10 "Order compelling Apple, Inc. to assist agents in search" (UNITED STATES DISTRICT COURT FOR THE CENTRAL DISTRICT OF CALIFORNIA, 2016, online).

11 "Order requiring Apple, Inc. to assist in the execution of a search warrant issued by the court" (U.S. DISTRICT COURT FOR THE EASTERN DISTRICT OF NEW YORK, 2016, online).

12 "iMessages são textos, fotos ou vídeos que você envia para dispositivos iOS e Macs por meio de redes Wi-Fi ou de dados celulares. Essas mensagens aparecem em balões azuis" (APPLE, online-b).

13 "Within weeks, Facebook's messaging service WhatsApp plans to expand its secure messaging service so that voice calls are also encrypted, in addition to its existing privacy features. The service has some one billion monthly users. Facebook is also considering beefing up security of its own Messenger tool. Snapchat, the popular ephemeral messaging service, is also working on a secure messaging system and Google is exploring extra uses for the technology behind a long-in-the-works encrypted email project. Engineers at major technology firms, including Twitter, have explored encrypted messaging products before only to see them never be released because the products can be hard to use – or the companies prioritized more consumer-friendly projects. But they now hope the increased emphasis on encryption means that technology executives view strong privacy tools as a business advantage – not just a marketing pitch" (YADRON, 2016, online).

judicial de fornecer informações sobre uma investigação policial. A ordem judicial determinou a quebra do sigilo e a interceptação de mensagens para viabilizar o andamento de um inquérito instaurado pela 62ª Delegacia de Polícia. A magistrada também ordenou a instauração de um procedimento contra o representante legal da empresa Facebook pela suposta prática de obstrução de investigação criminal, com base no art. 2º, § 1º, da Lei n. 12.850/2013.[14]

No mesmo dia, o desembargador José Roberto Lagranha Távora, da 4ª Câmara Criminal do Tribunal de Justiça do Estado do Rio de Janeiro concedeu liminar em mandado de segurança impetrado pelo Facebook Serviços Online do Brasil LTDA e liberou o uso do aplicativo de mensagens WhatsApp em todo o país[15]. Horas depois, o ministro Ricardo Lewandowski, do Supremo Tribunal Federal, suspendeu decisão. A liminar foi deferida na Medida Cautelar em Arguição de Descumprimento de Preceito Fundamental (ADPF) n. 403, ajuizada em maio deste ano pelo Partido Popular Socialista (PPS), originalmente contra decisão do juiz da Vara Criminal de Lagarto (SE). Segundo o ministro, a suspensão do serviço aparentemente viola o preceito fundamental da liberdade de expressão e comunicação (art. 5º, inciso IX, da Constituição Federal) e a legislação de regência sobre a matéria.[16]

Diante deste cenário, em novembro de 2016, o ministro Edson Fachin, do Supremo Tribunal Federal (STF), convocou audiência pública para discutir o bloqueio do aplicativo WhatsApp por decisões judiciais no Brasil, bem como para instruir o julgamento da ADPF n. 403 e da ADI n. 5527. Esta última, por sua vez, tem por objeto dispositivos do Marco Civil da Internet (Lei n. 12.965/2014), os quais têm servido de fundamentação para decisões judiciais que determinam a suspensão dos serviços de troca de mensagens entre usuários da Internet. Ao convocar a audiência, o ministro elaborou

14 "Juíza ordena bloqueio do WhatsApp em todo o país" (TRIBUNAL DE JUSTIÇA DO ESTADO DO RIO DE JANEIRO, 2016a, online).

15 "TJRJ suspende decisão e libera uso do WhatsApp" (TRIBUNAL DE JUSTIÇA DO ESTADO DO RIO DE JANEIRO, 2016b, online).

16 "Presidente do STF determina restabelecimento imediato dos serviços do WhatsApp" (SUPREMO TRIBUNAL FEDERAL, 2016, online).

algumas questões a serem respondidas pelos habilitados a participar, tais como o funcionamento do sistema de criptografia E2E utilizado pelo WhatsApp, as formas de interceptar, desabilitar ou utilizar essa criptografia em outras plataformas.[17] [18]

A audiência pública foi realizada nos dias 02/06/2017 e 05/06/2017, e contou com expositores do Departamento de Polícia Federal, do Ministério Público, da Ordem dos Advogados do Brasil (OAB), da Associação dos Magistrados Brasileiros (AMB), da WhatsApp Inc., do Facebook Serviços Online do Brasil Ltda., do Comitê Gestor da Internet no Brasil (CGI.br), do Núcleo de Informação e Coordenação do Ponto BR (NIC.br), do Instituto de Computação da Universidade Estadual de Campinas (UNICAMP), do Departamento de Engenharia de Computação e Sistemas Digitais da Escola Politécnica da Universidade de São Paulo (USP), do Laboratório de Pesquisa Direito Privado e Internet da Universidade de Brasília (UnB), entre outros órgãos públicos e instituições de pesquisa[19]. Aguarda-se, atualmente, o julgamento das ações mencionadas.

A seguir será abordado os sistemas criptográficos aplicados à segurança de redes, bem como a técnica E2E, a fim de verificar, a partir do conhecimento interdisciplinar, os efeitos da nova técnica com relação à legislação brasileira pertinente, bem como a responsabilidade civil do WhatsApp e a viabilidade das sanções judiciais (bloqueios).

17 "Ministro Fachin convoca audiência pública para debater bloqueios judiciais do WhatsApp" (SUPREMO TRIBUNAL FEDERAL, 2016, online).

18 "Inscrições para audiência pública sobre WhatsApp e Marco Civil da Internet se encerram dia 1º/2" (SUPREMO TRIBUNAL FEDERAL, 2017, online).

19 "STF inicia audiência pública que discute bloqueio judicial do WhatsApp e Marco Civil da Internet" (SUPREMO TRIBUNAL FEDERAL, 2017, online).

3 CRIPTOGRAFIA E SEGURANÇA DE REDES: CONSIDERAÇÕES GERAIS E SUA INSERÇÃO NO WHATSAPP

3.1 TÉCNICAS DE CRIPTOGRAFIA APLICADAS À SEGURANÇA DE REDES

Criptografia, segundo William Stallings, consiste no desenvolvimento de técnicas para garantir o sigilo e/ou a autenticidade de informações.[20] A seguir será abordado acerca da criptografia aplicada à segurança de rede, ou seja, o uso de técnicas aplicadas nos protocolos e aplicativos de rede.

A palavra criptografia é formada pelos termos gregos *kryptos*, que significa secreto, oculto, ininteligível, e *grapho*, que significa escrita, escrever. Trata-se da ciência/arte de se comunicar secretamente. O objetivo básico da criptografia é tornar uma mensagem ininteligível para um adversário, que possa vir a interceptar a mensagem. Hoje a criptografia é um campo de estudos abrangente, incluindo diversos aspectos da segurança de dados em geral, razão pela qual se tornou alvo de extensas pesquisas científicas. Não só quem manda a mensagem, mas também quem a intercepta, deve possuir um considerável poder computacional.[21]

Desse modo, pode-se afirmar que a criptografia é um ramo da matemática combinado com a ciência da computação. Para Bruce Schneier, é uma tecnologia básica do ciberespaço, dado que a criptografia é que permite gerir a sua segurança.[22] O uso da criptografia na Internet é relativamente novo, cuja necessidade adveio do e-commerce. Protocolos criptográficos visualizados em várias áreas da Internet é algo recente e os primeiros exemplos referem-se ao ano 2000, tais como a encriptação do e-mail e dos cartões de crédito.

O modelo mais simples de criptografia é denominado de cifra simétrica. Trata-se de uma chave secreta compartilhada entre o emissor e o receptor. O emissor cifra a mensagem com a chave

20 STALLINGS, 2008, p. 18.

21 CARVALHO, 2000, p. 7.

22 SCHNEIER, 2001, p. 93 e 118-119.

secreta e gera uma nova mensagem cifrada, ao passo que o receptor, ao receber a mensagem cifrada e, tendo em mãos a chave secreta para decodificá-la, recupera a mensagem original. Essa técnica é eficiente, porém apenas até o momento em que um terceiro descubra a chave secreta. Uma vez descoberta, ele pode interceptar as mensagens e decodificá-las em tempo real, além de poder se passar pelo emissor ao enviar mensagens cifradas. Essa técnica é amplamente utilizada por ser simples de ser aplicada. Para deixá-la mais eficiente, a chave secreta é substituída por uma nova após um curto período de tempo. Há exemplos do uso que vão desde a máquina alemã utilizada para criptografar e descriptografar mensagens durante a segunda grande guerra (denominada Enigma) até os mais recentes *tokens* para operações bancárias.

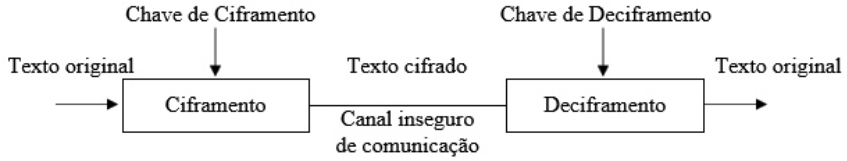

Figura 1 – Sistema criptográfico simétrico[23]

O modelo mais seguro de troca de mensagens na rede atualmente utilizado é denominado criptografia de chave pública, ou de cifra assimétrica. De acordo com William Stallings, este modelo evoluiu para resolver dois problemas do modelo de cifra simétrica.[24] O primeiro é o de como distribuir as chaves secretas com proteção; o segundo é o das assinaturas digitais, de modo a assegurar que não trata-se de um terceiro passando-se pelo emissor durante a comunicação.

Nesse modelo assimétrico todos os membros do sistema de comunicação possuem a sua chave pública, que é compartilhada com todos, e uma chave privada, mantida secretamente. Estas duas são complementares neste modelo. O texto cifrado com a chave pública só pode ser decifrado com a chave privada. Assim, ao enviar uma

23 LUCCHESI, 1986, p. 5.

24 STALLINGS, 2008, p. 181.

mensagem ao receptor, o emissor cifra a mensagem com a chave pública do receptor, e o receptor de posse da mensagem possui a sua chave privada para decifrar a mensagem. O inverso também é possível. O texto cifrado com a chave privada só pode ser decifrado com a chave pública, de forma que para o emissor ser autenticado, ele cifra a mensagem com sua chave privada, e o receptor de posse da mensagem faz uso da chave pública do emissor para decifrar a mensagem em um texto claro.

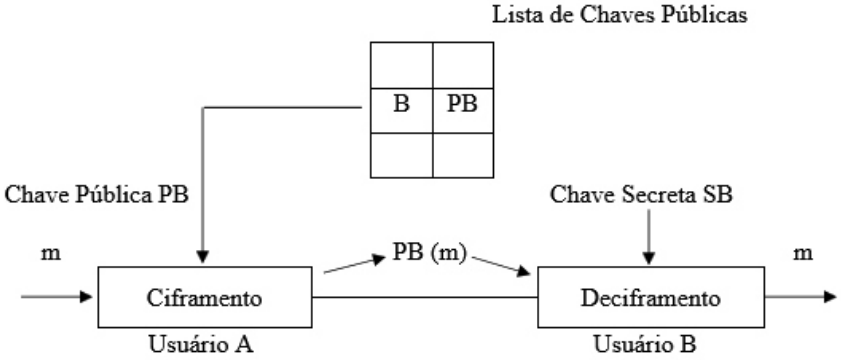

Figura 2 – Sistema criptográfico assimétrico[25]

Cabe observar que nenhum modelo de criptografia é 100% seguro, pois se a chave secreta for descoberta por um terceiro, ele terá posse da mensagem.

3.1 O CASO WHATSAPP

O WhatsApp é um aplicativo de troca de mensagens desenvolvido pela WhatsApp Inc., visando substituir de forma gratuita o serviço de SMS (*Short Message Service*) cobrado pelas operadoras de telefonia.

Segundo a WhatsApp Inc., o conteúdo das mensagens entregues pelo aplicativo WhatsApp não é copiado, mantido ou arquivado pela empresa. Os usuários digitam as mensagens, que são enviadas por algum serviço de acesso à Internet aos servidores

25 LUCCHESI, 1986, p. 14.

WhatsApp, e encaminhadas para o destinatário (que também deve ser um usuário do WhatsApp) se este estiver online. Se o destinatário estiver off-line, a mensagem é armazenada no servidor até que possa ser entregue. Se o destinatário não acessar o aplicativo por 30 (trinta) dias, a mensagem não é entregue e também é excluída do servidor.[26] Logo, sendo entregue uma mensagem, é imediatamente excluída do servidor.

Desde abril de 2016, a WhatsApp Inc. disponibilizou uma nova versão do aplicativo, agora com criptografia ponto-a-ponto.[27] Criptografia ponto-a-ponto é um termo dado para descrever que mesmo que a mensagem passe por um terceiro ou gerenciador, ela só é decifrada no receptor, ao passo que os gerenciadores da troca de mensagens não possuem acesso às chaves para decifrá-las.

Para o desenvolvimento dessa nova versão do aplicativo, a WhatsApp Inc. em parceria com a referida Open Whisper Systems, uma empresa de poucos programadores financiados por doações que mantém seus projetos abertos para que qualquer programador possa ingressar na comunidade e contribuir com o desenvolvimento, fez o uso da Biblioteca Signal Protocol,[28] uma biblioteca livre e de código aberto licenciada pela GPLv3,[29] específica para troca de mensagens de dados e áudio.

Esta biblioteca utiliza o modelo de chave pública para cifrar as mensagens. Um par de chaves pública e privada é definida para cada mensagem. Isso significa que durante uma conversa no aplicativo WhatsApp cada mensagem enviada ou recebida possui uma chave exclusiva, de modo que se um terceiro descobrir uma chave privada ele conseguirá ter acesso a uma única mensagem.

Quanto ao nível de segurança, o modelo utiliza chaves de 256 bits. Ou seja, é possível ter $\mathbf{2^{256}}$ [dois elevado a duzentos e cinquenta e seis] chaves diferentes, aproximadamente $\mathbf{1x10^{77}}$ [um multiplicado por dez elevado a setenta e sete]. Supondo que o invasor, ou

26 WHATSAPP, online-b.

27 OPEN WHISPER SYSTEMS, online.

28 GITHUB, online.

29 FREE SOFTWARE FOUNDATION, online.

um órgão investigador, possua um computador muito rápido para testar essas chaves, como, por exemplo, o supercomputador mais rápido do mundo, hoje o Sunway TaihuLight localizado no Centro Nacional de Supercomputação em Wuxi, China;[30] este computador possui mais de 10 milhões de núcleos e pode realizar **93014x10^{12}** [noventa e três mil e quatorze multiplicado por dez elevado a doze] operações por segundo, o que demoraria em média **1,9737 x10^{53}** [três multiplicado por dez elevado a cinquenta e três] anos para testar todas as chaves possíveis para cada mensagem, tornando improvável que a chave seja descoberta.[31]

A intercepção de mensagens acompanha o mesmo raciocínio. A mensagem adquirida por esse meio estará igualmente criptografada, sendo necessário o mesmo mecanismo de tentativas de descoberta das chaves para que o acesso ao seu conteúdo seja possível. O que será encontrado, de início, será apenas um "punhado de bits" sem sentido para quem não detém as chaves corretas. Portanto, o acesso às mensagens será viável apenas com a posse do aparelho móvel do usuário, de forma que a segurança da técnica criptográfica dependerá unicamente dele, sendo de sua responsabilidade mantê-lo em local seguro.

30 TOP500 SUPERCOMPUTER SITES, online.

31 Para o cálculo do tempo de solução do problema foram considerados:
1) O número 1 na lista dos computadores mais rápidos do mundo, Sunway TaihuLight, localizado no Centro Nacional de Supercomputação em Wuxi, que possui 10649600 processadores de 1,45Ghz, 1310720 GB de memória RAM e é capaz de executar em média 93014.6 x 10^{12} instruções de cálculos de números reais por segundo;
2) Um ano tem 31536000 segundos;
3) A chave possui 256 bits, por combinação isto gera 2^{256} chaves possíveis, que corresponde a aproximadamente 1,1579x10^{77} chaves diferentes.
Supondo que para testar cada chave diferente é necessário um algoritmo equivalente em tempo de 10 instruções de cálculo de números reais. Logo, anualmente este computador pode testar 31536000 x 93014.6 x 10^{12} / 10 chaves que resulta em 293330842560000000000000, que corresponde a aproximadamente 2,9333 x10^{23}.
A quantidade de anos para se testar todas as chaves é o total de chaves dividido por quantas chaves o computador pode testar por ano, que resulta em 3,9474 x10^{53} anos.
O tempo médio para encontrar a chave correta é calculado na metade do tempo em que se testaria todas as chaves, que corresponde a 1,9737 x10^{53} anos.

4 RESPONSABILIDADE CIVIL DO WHATSAPP PELO CONTEÚDO CRIPTOGRAFADO: POSSÍVEL EXCLUDENTE E TENDÊNCIA JURÍDICA

Na era da Internet e da digitalização da informação, marcada pela velocidade e pela grande quantidade de operações eletrônicas, a capacidade de coleta, o armazenamento e a divulgação de dados e informações atingem altos níveis de eficácia. É possível, em segundos, coletar e transferir para países ao redor do mundo milhões de informações pessoais, estabelecer perfis digitais das pessoas, que servem para realizar escolhas, decidir quem pode ter acesso ao crédito, quem é merecedor de confiança, ou até mesmo reconhecer um potencial terrorista.[32]

Marcel Leonardi reflete que grandes quantidades de informação sempre estiveram disponíveis de modo esparso, mas a possibilidade de análise e agregação de todos esses dados por qualquer pessoa, e não apenas por governos e empresas, é algo inédito.[33] Na era da informação e das redes, marcada pelo anonimato dos agentes e pela complexidade e velocidade das relações comerciais, a troca de informações é instantânea e ocorre em uma escala sem precedentes. Isso porque os baixos custos de armazenamento de informações e a facilidade de sua manipulação provocaram o surgimento de bancos de dados e cadastros de toda espécie.

Conforme observa Liliana Minardi Paesani, no Brasil, é possível notar que não é o governo que ameaça a privacidade, mas sim o comércio, por meio da Internet.[34] A web transformou-se em um mercado, e, nesse processo, a privacidade passa de um direito a uma *commodity*. A informática possibilita não só acumular informações em quantidade ilimitada sobre a vida de cada indivíduo (suas condições físicas, mentais, econômicas ou suas opiniões religiosas e políticas), como também confrontar, agregar, rejeitar e comunicar as informações obtidas.

32 BESSA, 2011, p. 57.

33 LEONARDI, 2011, p. 71-72.

34 PAESANI, 2003, p. 52.

Como aponta Demócrito Ramos Reinaldo Filho, o direito à privacidade da pessoa, previsto pela Constituição Federal em seu art. 5º, inc. X, também pode ser desrespeitado no ambiente eletrônico.[35] A publicação de dados ou informações de caráter íntimo ou que diga respeito à vida particular de uma pessoa pode acarretar-lhe prejuízo de ordem extrapatrimonial e patrimonial. Logo, aquele que ofender esse direito constitucional, revelando dados pertencentes à esfera da privacidade alheia, poderá ser condenado a ressarcir o dano causado.

A responsabilidade civil por danos ocasionados na Internet abrange quaisquer agentes que, mesmo indiretamente, percebam alguma vantagem econômica com o manuseio dos aplicativos eletrônicos. Dentre eles, destacam-se os provedores, cuja responsabilidade civil por seus próprios atos deve ser interpretada pelo sistema de responsabilidade previsto no Código de Defesa do Consumidor ou no Código Civil, conforme afetem diretamente os consumidores que os utilizam, ou terceiros. Já a responsabilidade civil por atos de usuários e terceiros, deve ser interpretada a par de um sistema que atribua responsabilidade solidária aos provedores em caso de dolo ou negligência, quando deixam de cumprir seus deveres (e tornam assim impossível a identificação do efetivo responsável pelo ato ilícito), quando colaboram para sua prática, ou quando deixam de bloquear o acesso à informação ilegal, após terem sido cientificados de sua existência.[36]

Esta última hipótese trata-se da responsabilidade civil fundada na culpa, na modalidade negligência, posição adotada pela Lei n. 12.965/2014 (Marco Civil da Internet), nos arts. 19[37] e 21[38]

35 FILHO, 2005, p. 84.

36 LEONARDI, 2005, p. 79-80.

37 Art. 19. Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de Internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário. [...].

38 Art. 21. O provedor de aplicações de Internet que disponibilize conteúdo gerado por

quanto aos provedores de aplicações. De acordo com a legislação, os provedores de aplicações de Internet somente poderão ser responsabilizados por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial, não tomarem as providências para indisponibilizar o conteúdo indevido, no âmbito e nos limites técnicos do seu serviço, dentro do prazo legal (art. 19). E, se os provedores de aplicações de Internet disponibilizarem conteúdo indevido gerado por terceiros, serão responsabilizados subsidiariamente pela violação da intimidade daí decorrente, caso não indisponibilizarem o conteúdo indevido, após o recebimento de notificação do lesado ou de seu representante legal, também no âmbito e nos limites técnicos do seu serviço (art. 21).

Cabe observar que o provedor de aplicações é um gênero que abarca o provedor de correio eletrônico, de hospedagem, de conteúdo. O provedor de correio eletrônico é aquele que fornece serviço de envio, recebimento e armazenamento de mensagens eletrônicas. Já o provedor de hospedagem é aquele que permite o armazenamento de sites, blogs, redes sociais, etc., com textos, imagens, sons e informações em geral. E o provedor de conteúdo, por sua vez, coloca à disposição do usuário a possibilidade de adquirir diversos serviços (acesso e armazenamento de informações, como redes sociais, blogs, etc.) e produtos (eletrodomésticos, programas de computador, etc.) ao conectar-se à Internet.[39]

Por aplicações de Internet, compreende-se ser o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à Internet. Essas funcionalidades correspondem, por exemplo, a sites institucionais, governamentais, empresariais de e-commerce, blogs, redes sociais, etc. Vale frisar que registros de

terceiros será responsabilizado subsidiariamente pela violação da intimidade decorrente da divulgação, sem autorização de seus participantes, de imagens, de vídeos ou de outros materiais contendo cenas de nudez ou de atos sexuais de caráter privado quando, após o recebimento de notificação pelo participante ou seu representante legal, deixar de promover, de forma diligente, no âmbito e nos limites técnicos do seu serviço, a indisponibilização desse conteúdo. Parágrafo único. A notificação prevista no caput deverá conter, sob pena de nulidade, elementos que permitam a identificação específica do material apontado como violador da intimidade do participante e a verificação da legitimidade para apresentação do pedido.

39 TEIXEIRA, 2015, p. 30, 32 e 34.

acesso a aplicações de Internet tratam-se do conteúdo de informações referentes a data e hora de uso de uma determinada aplicação de Internet a partir de um determinado endereço IP.[40]

A par desse conceito, o Facebook, enquanto fornecedor de diversas funcionalidades sob o formato de rede social, inclusive abrangendo o serviço de troca de mensagens por meio do WhatsApp, pode ser compreendido como provedor de aplicações para efeitos do Marco Civil da Internet. Ao passo que o WhatsApp, por si só, pode ser entendido como uma aplicação de Internet.

Antes do Marco Civil da Internet, Demócrito Ramos Reinaldo Filho já observava que as áreas do sistema informático de um provedor postas à disposição dos usuários podem ser vistas como regiões privadas em relação aos controladores do sistema, no sentido de que não podem intervir de modo desarrazoado no conteúdo produzido pelo usuário.[41] Todavia, a liberdade editorial que o provedor desfruta não o previne contra indenizações ou ações criminais em virtude da publicação de informações obscenas, difamatórias ou pornográficas, visto que esses "espaços privados" representam, na realidade, uma grande rede pública de comunicação. Para não ser responsabilizado solidariamente ou como co-autor pela circulação desses conteúdos ilícitos, o operador do sistema deve tomar alguma iniciativa que exclua sua responsabilidade e que demonstre efetivamente que não agiu com negligência, assumindo ou transferindo passivamente o conteúdo das publicações realizadas pelo usuário nos "espaços privados". A comum atividade intermediária dos controladores de sistema, embora nem sempre exerça um controle real sobre o conjunto de informações que neles circulam, pode ser interpretada como um conhecimento presumido do caráter ilícito da informação que se encontra em seu sistema.

Após o Marco Civil da Internet, Marcel Leonardi bem coloca que o conteúdo gerado por usuários e disponibilizado por meio de serviços oferecidos pelos provedores representa, hoje, uma das principais formas de expressão, fomentando o pensamento crítico

40 TEIXEIRA, 2016, p. 93.

41 FILHO, 2005, p. 214-215.

e o estabelecimento de novas comunidades.[42] Um ambiente de insegurança jurídica a respeito do tratamento legal desse conteúdo circulado poderia forçar as plataformas digitais e as redes sociais a fechar os espaços ou a desativar as ferramentas que viabilizem essas formas de atividade, fazendo com que todo o potencial desses espaços e dessas ferramentas fosse desperdiçado. Logo, não se pode presumir que a Internet, uma das maiores conquistas tecnológicas da humanidade, sirva apenas para a prática de atos ilícitos. A propósito, nas palavras de Newton De Lucca: "[...] o Marco Civil da Internet, sejam quais forem suas limitações e seus pontos polêmicos – e eles existem, realmente –, poderá servir de adminículo para que, pelo menos, decisões teratológicas sejam evitadas".[43]

O uso da criptografia ponto-a-ponto é uma excelente iniciativa nesse sentido, pois assegura, ao menos em tese, que a empresa não terá acesso ao conteúdo compartilhado entre os usuários, únicos detentores do conjunto das chaves para decifrar a mensagem. A ideia é aplaudida sob o ponto de vista da criatividade empresarial, visto que se interpretando os arts. 19 e 20 do Marco Civil da Internet, ao lado da não retenção de mensagens pelo servidor do WhatsApp, depreende-se que a empresa sequer disponibiliza o conteúdo gerado por terceiros. Além disso, a criptografia ponto-a-ponto gerada instantaneamente quando da criação e envio do texto pelo usuário faz com que a mensagem seja impossível de ser acessada desde o seu início. Logo, o conteúdo já nasce indisponível para o WhatsApp.

A partir do instante em que a empresa não disponibiliza o conteúdo (as mensagens não são arquivadas no servidor), o qual está em mãos apenas dos usuários, e ainda protegido por um sistema criptográfico eficiente, infere-se que a responsabilidade civil, da forma como é colocada na legislação, é excluída com o método de criptografia E2E, por tornar inviável e improvável o acesso do WhatsApp às mensagens compartilhadas entre os usuários. Isso porque não é possível tornar indisponível aquilo que se origina indisponível.

42 LEONARDI, 2015, p. 536-537.

43 LUCCA, 2015, p. 29.

Por oportuno, cabe observar que a posição tomada pela empresa, em uma interpretação literal da lei, não fere o previsto no art. 15 do Marco Civil da Internet,[44] tendo em vista que o dispositivo menciona o dever de manutenção de "registros de acesso a aplicações de Internet", e não de mensagens/comunicações particulares compartilhadas entre os usuários das aplicações de Internet[45].

A novidade será alvo de muitas críticas, em especial pela atual desconfiança de que o WhatsApp realmente não detém a guarda das chaves específicas geradas pelos usuários necessárias para decifrar a mensagem em uma única tentativa. No entanto, essa posição deverá ser enfrentada cautelosamente pelos operadores do Direito, pois consiste em uma tendência a ser praticada pelas demais empresas de Tecnologia da Informação, as quais, inclusive, já têm manifestado apoio às Apple e ao WhatsApp[46] frente às ordens judiciais "descumpridas" e aos bloqueios ocorridos.

5 NECESSIDADE DE INVESTIGAÇÃO E ACESSO JUDICIAL: O CONFLITO PRIVACIDADE VS. INTERESSE PÚBLICO

A questão da privacidade vem sendo erguida sob o patamar dos direitos da personalidade, porquanto fundamentais, tendo como base a dignidade da pessoa humana, regra principiológica constante no texto da Constituição Federal brasileira. A doutrina jurídica cada

44 Art. 15. O provedor de aplicações de Internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de Internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento.

45 Cabe expor também a distinção entre "dados" e "informações". Dados, por si só, é algo cru, bruto. Simplesmente existem e não possuem significado além de sua existência. Podem existir em qualquer forma, utilizáveis ou não. Em linguagem de computador, uma planilha geralmente começa pela exploração dos dados. Já informações são dados que possuem significado por meio de uma conexão relacional. Este "sentido" pode ser útil ou não. Em linguagem de computador, um banco de dados relacional torna as informações a partir dos dados armazenados no seu interior (ACKOFF, 1989, p. 3).

46 No caso Apple vs. FBI, empresas anunciaram oficialmente apoio à Apple por meio de Departamento de Justiça dos Estados Unidos, tais como, Amazon, Box, Cisco, Dropbox, Evernote, Facebook, Google, Microsoft, Mozilla, Nest, Pinterest, Slack, Snapchat, WhatsApp, and Yahoo (APPLE, 2016a, online).

vez mais debate o tema, incorrendo em certa dificuldade em defini-la, tendo em vista o grande número de interesses que são tutelados em nome da privacidade. Muito embora as intermináveis discussões sobre o seu conceito, um dos seus principais focos é a proteção e segurança dos dados pessoais, por manter um nexo de causalidade direto com o tema da privacidade, da qual é uma espécie de herdeira, atualizando-a e impondo características próprias.[47]

Para a Ciência da Computação, o conceito de privacidade ultrapassa o conceito de segurança, pois a privacidade examina como o uso da informação pessoal, que um sistema adquire sobre um usuário, está de acordo com suposições explícitas ou implícitas relativas a esse uso. Para o usuário final, a privacidade pode ser considerada sob duas perspectivas diferentes: impedindo o armazenamento de informações pessoais; ou garantindo o uso apropriado dessas informações. Logo, a privacidade é a capacidade de os indivíduos controlarem os termos sob os quais sua informação pessoal é adquirida e usada. Enquanto a segurança envolve a tecnologia para garantir que a informação está devidamente protegida, a privacidade, por sua vez, envolve mecanismos para dar suporte à conformidade com alguns princípios básicos, como o dever de cientificar as pessoas sobre a coleta de informações, avisá-las com antecedência sobre o que será feito com elas, oportunizando-as de aprovar o uso das informações.[48]

A criptografia E2E, ao possibilitar a geração do conjunto de chaves pública e privada apenas entre os usuários do WhatsApp, atende esse objetivo quanto à privacidade do ponto de vista informático. A propósito, a criptografia é elevada como um padrão de segurança a ser observado pelos provedores de aplicações, sendo expressamente prevista no art. 13, inc. IV e § 2º, do Decreto n. 8.771/2016, que regulamenta o Marco Civil da Internet. De acordo com o dispositivo, os provedores de aplicações devem adotar, na guarda, armazenamento e tratamento de dados pessoais, "[...] soluções de gestão dos registros por meio de técnicas que garantam a

47 DONEDA, 2006, p. 204.

48 ELMASRI; NAVATHE, 2011, p. 566-567.

inviolabilidade dos dados, como encriptação ou medidas de proteção equivalentes". Além disso, os provedores de aplicações devem "[...] reter a menor quantidade possível de dados pessoais, comunicações privadas e registros de conexão e acesso a aplicações [...]".[49]

Entretanto, a tutela da privacidade da pessoa física, bem como os segredos empresariais encontram algumas limitações, como a publicidade de informações para a busca judicial da verdade em uma determinada investigação. Em outras palavras, é possível que o direito à privacidade seja relativizado face ao interesse público.

De acordo com José Adércio Leite Sampaio,[50] esse conflito de interesses é um dos tópicos mais complicados no trâmite processual por conjugar múltiplos aspectos de direito material e subjetivo, além de uma gama de diferentes situações e posições jurídicas que impossibilitam uma solução judicial imediata. No caso de necessidade de acesso judicial por meio da violação de comunicações em formato eletrônico, o fundamento é o mesmo da interceptação telefônica, conforme interpreta-se pelo art. 2º, da Lei n. 9.296/1996. Por ser medida de extrema gravidade, deve-se preencher alguns requisitos: a) indícios razoáveis de autoria ou participação em infração penal; b) imprescindibilidade da medida; c) o fato investigado deve constituir crime punido com reclusão. O referido autor defende que a relativização do sigilo das comunicações telefônicas prevista no art. 5º, inc. XII, da Constituição Federal se estende às comunicações em sistema informático e telemático. E não há nenhuma arbitrariedade contra direito fundamental ou diminuição do índice democrático do Estado de Direito, mas sim uma exigência da vida em comunidade que supera o sentido individual da existência humana e de seus interesses, além de reduzir os riscos de ruptura e desequilíbrio sistêmico que um apego exagerado à forma pode patrocinar.

Assim, em alguns casos é necessário contrapor o interesse coletivo ao interesse individual. Vale salientar que o direito à segurança tem sido invocado pela sociedade em detrimento da privacidade, sobretudo após os atentados terroristas de 11 setembro

49 BRASIL, 2014.

50 SAMPAIO, 1998, p. 396 E 410-411.

de 2011 nos Estados Unidos. Ilustra-se essa ideia com a vistoria de bagagens em aeroportos, situação regulamentada pelo Decreto n. 7.168/2010 com vistas a prevenir acidentes e interferências ilícitas.[51]

Entretanto, indaga-se: a interceptação das mensagens compartilhadas via WhatsApp é imprescindível? Existem outras ferramentas que igualmente propiciam a comunicação para colaborar com a investigação policial e com o Poder Judiciário? Em que pese o WhatsApp ser um dos meios de comunicação mais utilizados nos dias atuais, não se descarta a utilização de outros instrumentos com a mesma finalidade, como o próprio telefone, cuja forma de interceptação encontra-se regulamentada. Logo, entende-se que a interceptação, a princípio, não seria imprescindível.

A princípio, cabe observar que na interceptação o conteúdo da informação trocada pode ser coletado e, em razão de sua instantaneidade, não há limites específicos impostos, como há para os registros, tratados no Marco Civil da Internet. Não há que se falar de interceptação dentro de limites razoáveis, nem se tutela a privacidade nela. Assim, autorizada a interceptação, a coleta da informação é integral.[52]

André Ramos Tavares destaca essa necessidade de ater-se à perpetração de variadas afrontas a direitos fundamentais e, em especial, aos individuais, sob a justificativa do interesse público.[53] Segundo o autor, não se pode desconhecer que a aproximação do público ao particular legitima governos totalitários e condutas impróprias. Afinal, a sociedade é composta por indivíduos. Ela não existe por si só, mas através da congregação daqueles, que deverão ter garantida a esfera de seus direitos para que o convívio social não seja impossibilitado pelo esfacelamento da necessária harmonia, segurança e confiança.

Outro ponto conflituoso no que diz respeito à legislação atual sobre o tema é que ao mesmo tempo em que a encriptação é padrão de segurança exigido para garantir a inviolabilidade de

51 TEIXEIRA, 2015, p. 84.

52 NORI, 2015, p. 176.

53 TAVARES, 2005, p. 236-237.

dados e das comunicações privadas (art. 13, inc. IV, do Decreto n. 8.771/2016, grifo anterior), o art. 15 do mesmo regulamento determina que os dados cadastrais deverão ser guardados pelos provedores de forma que o eventual acesso judicial seja facilitado:

> Art. 15. Os dados de que trata o art. 11 da Lei nº 12.965, de 2014, deverão ser mantidos em **formato interoperável e estruturado, para facilitar o acesso decorrente de decisão judicial ou determinação legal, respeitadas as diretrizes elencadas no art. 13 deste Decreto** (BRASIL, 2016, grifou-se).

Como exposto, a criptografia, seja qual for a técnica utilizada, ensejará certa dificuldade de acesso a quem não detém o conjunto de chaves. Cabe observar, também, que o dispositivo mencionado refere-se a "dados cadastrais", e não conteúdo relativo à comunicação privada, ou seja, mensagens compartilhadas entre os usuários, o que torna duvidosa a sua aplicabilidade ao WhatsApp. Ademais, ainda que a empresa detenha todo o conjunto de chaves criptográficas geradas por cada mensagem lançada por bilhões de usuários, a sua disponibilização acarretaria um certo enfraquecimento do sistema, gerando custos anormais e comprometendo a privacidade de diversos indivíduos, como também o segredo empresarial. Este último é preocupação do Decreto n. 8.771/2016, conforme redação do art. 16:

> Art. 16. As informações sobre os padrões de segurança adotados pelos provedores de aplicação e provedores de conexão devem ser divulgadas de forma clara e acessível a qualquer interessado, preferencialmente por meio de seus sítios na Internet, **respeitado o direito de confidencialidade quanto aos segredos empresariais**.[54]

A tutela da privacidade também recebe um reforço considerável com a proteção do sigilo profissional, assegurando-se de que as confidências feitas em razão da função, ministério, ofício ou profissão recebam uma proteção relevante. Da mesma forma que a interceptação telefônica, a ordem judicial em caso de eventual violação de segredo empresarial deverá ser fundamentada com

54 BRASIL, 2016, grifou-se.

a indispensabilidade da medida, diante da inexistência de outro meio menos gravoso a substituí-la, reservado à empresa o direito de corrigir possível excesso judicial.[55]

Sobre o assunto, vale expor a análise econômica de Richard Posner, ao defender que a informação empresarial deveria receber mais proteção legal que a própria informação na esfera pessoal.[56] Para o autor, o sigilo é importante para os empresários, por ser um método pelo qual se apropriam dos benefícios sociais que criam. Na vida privada, porém a função mais provável do sigilo é ocultar informações demeritórias. Ademais, as comunicações dentro das empresas e demais organizações privadas parecem merecer proteção, tanto quanto as comunicações entre indivíduos; pois, em ambos os casos, o efeito da divulgação seria o de obstruir e retardar a comunicação. Ainda assim, a tendência é que empresas e outras organizações privadas tenham sua confidencialidade cada vez menos protegida, no que depender da legislação. Enquanto os fatos sobre os indivíduos – ficha criminal, saúde, credibilidade, estado civil, inclinação sexual – são cada vez mais protegidos contra a divulgação desautorizada, as informações sobre grandes empresas são colocadas em domínio público pelas infindáveis exigências de divulgação impostas pelas leis federais que regulam os mercados de valores mobiliários (a ponto de algumas empresas estarem "fechando seu capital", para garantir a confidencialidade de seus projetos e de suas operações), pelas leis de direitos civis, pela obrigatoriedade de emissão de relatórios segmentados, entre outras regulamentações.

Além disso, quanto à possibilidade do WhatsApp quebrar ou não a criptografia aplicada às mensagens dos usuários, permitindo acesso judicial ao seu conteúdo, Ricardo Lewandowski (ministro do STF), ressaltou que se trata de tema da mais alta complexidade, não existindo dados e estudos concretos quanto à possibilidade de execução da medida determinada pelo Juízo da 2ª Vara Criminal da Comarca de Duque de Caxias (RJ) e supostamente descumprida pela empresa. Assim, em análise preliminar, o ministro concluiu que

55 SAMPAIO, 1998, p. 413-415.

56 POSNER, 2010, p. 293-294.

o poder geral de cautela do magistrado assegura a suspensão de ato aparentemente pouco razoável e proporcional, além de gerar insegurança jurídica, deixando milhões de brasileiros sem esse meio comunicação.[57]

Nesse ponto, cabe destacar as palavras de Bruce Schneier a respeito da possibilidade de violar um sistema criptográfico, para posterior reflexão:

> A criptografia também é difícil. Ela combina vários ramos da matemática com ciência de computação. Ela requer anos de prática. Até mesmo pessoas inteligentes, conhecedoras e experientes inventam uma criptografia ruim. Na comunidade criptográfica, as pessoas nem sequer ficam tão embaraçadas quando seus algoritmos e protocolos são violados. É realmente difícil. O problema é esse: qualquer um, não importa suas habilidades, pode projetar um primitivo criptográfico que ele mesmo não possa violar. Esse é um ponto importante. **O que isso significa é que alguém pode se sentar e criar um primitivo criptográfico, tentar violá-lo e falhar, para depois anunciar: "Inventei um algoritmo/protocolo/etc. seguro". O que ele está realmente dizendo é: "Não consigo violar isso; portanto, é seguro".**[58]

Portanto, diante do estudo realizado, depreende-se que os bloqueios ocorridos por determinação judicial carecem do devido fundamento técnico e jurídico. Inexiste comprovação de que o WhatsApp detém a guarda de todas chaves geradas a cada mensagem compartilhada por milhões de usuários. E, ainda assim, a divulgação seria uma possível afronta à confidencialidade empresarial, além dos custos incomuns que a tarefa geraria, colocando-se em risco a privacidade de diversos indivíduos que comunicam-se via WhatsApp.

6 CONCLUSÃO

Conforme visto, a criptografia ponto-a-ponto (E2E) consiste em um sistema de segurança no qual apenas os pontos da conexão possuem acesso às chaves que irão decifrar o conteúdo do texto criptografado. No caso do WhatsApp, considerando que as mensa-

57 BRASIL, 2016, online.

58 SCHNEIER, 2001, p. 122, grifou-se.

gens compartilhadas não são armazenadas em um servidor, significa que mesmo interceptando-se uma mensagem em seu trâmite, ela será encontrada em forma encriptada, sendo ilegível para quem não detém o conjunto de chaves. Isso vale também para o próprio aplicativo, segundo sua política de privacidade.

A novidade gera diversos efeitos no mundo jurídico, sendo necessário o estudo interdisciplinar para averiguar se determinada ordem judicial é passível de cumprimento sem gerar desproporcionalidade entre as partes envolvidas e demais interessados. De acordo com os cálculos apresentados, demonstrou-se que decifrar uma única mensagem criptografada com a tecnologia ponto-a-ponto pelo aplicativo WhatsApp não é impossível, mas é inviável em razão da empreitada requerer tempo excessivo e largos investimentos em hardwares. Isso porque essa é a característica da matemática avançada, em que a solução para certas operações numéricas é difícil de ser alcançada, ou mesmo inexiste. Assim deve ser a criptografia aplicada à segurança de redes, visto que em tempos de Internet e seus exponenciais efeitos, é necessário que e-mails, mensagens instantâneas, páginas de web, arquivos, processos, aplicativos, etc., sejam criptografados em sua melhor técnica, pois tudo o que ali trafega pode ser violado.

Ainda que seja incerta a alegação da empresa de que não mantém as chaves próprias geradas por cada mensagem, ou de que não possui mecanismos para decifrar o texto objeto de investigação, além da desconfiança sobre o não armazenamento de mensagens no servidor, analisou-se que, do contrário, os custos dessas providências seriam altíssimos, e possivelmente seriam repassados aos usuários do WhatsApp, gerando uma onerosidade indesejada a eles, bem como a perda da credibilidade do aplicativo.

Quanto à responsabilidade civil do WhatsApp (ou melhor do seu proprietário, a empresa Facebook) em razão de danos ocasionados pela circulação de conteúdo gerado por terceiros, verificou-se que a criptografia ponto-a-ponto é capaz de fazer com que este mesmo conteúdo se origine indisponível a partir do instante em que a mensagem é criptografada logo em sua criação e envio pelo usuário a outro. Diante disso, não há configuração de ato ilícito, tampouco de responsabilidade civil, tendo em vista que

o provedor, neste caso, adotou as medidas cabíveis para a proteção da mensagem enviada (seja por escrito, por áudio ou por imagem), e retirou sua possibilidade de acesso àquela mensagem. Também apontou-se que essa postura será adotada pelas demais empresas de TI, configurando uma possível tendência jurídica no sentido de exclusão de responsabilidade civil.

Finalmente, com relação à eventual necessidade de investigação policial e/ou acesso judicial, vindo a caracterizar, porquanto, um conflito entre o interesse público (segurança) e interesse privado (privacidade), demonstrou-se que a interceptação da comunicação via WhatsApp ou a determinação à empresa para fornecer as mensagens em texto claro, e consequente bloqueio justificado na "recusa" de seu cumprimento, podem constituir medidas desequilibradas e ineficazes.

Tais ações não violam somente o segredo empresarial, mas também prejudicam a privacidade dos demais usuários a partir da abertura e concessão para determinado caso, dando margem à admissão de ordens judiciais infundadas e à exorbitância estatal. Assim, um interesse privado que seja comum a bilhões de usuários ganha dimensão coletiva, e também pública, quando o assunto é um direito que após anos de luta social foi elevado como fundamental ao viver digno, e, por sua vez, ao convívio digno entre as pessoas: o direito à privacidade e o dever de tê-la respeitada, o mínimo que se pode assegurar à existência humana, física e psíquica.

Logo, a criptografia ponto-a-ponto não é incompatível com o Marco Civil da Internet (Lei n. 12.965/2014), como também não afronta o ordenamento jurídico brasileiro, por ser um método que ratifica a segurança das comunicações. Ao contrário, as ordens judiciais é que não estão observando qual é a correta preocupação legal em se tratando de agentes que operam na Internet (se o dever é de fornecer registros de acesso ou dados e informações privadas); ou ainda, se preenchem os requisitos legais para a interceptação, sendo totalmente inviáveis. Por fim, constatou-se que o desconhecimento da complexidade técnica da matéria por parte do Poder Judiciário poderá acarretar consequências muito maiores à sociedade a favor da busca pela punição em situações apartadas.

REFERÊNCIAS

ACKOFF, Russell L. From data to wisdom. **Journal of Applies Systems Analysis**, v. 16, jul. 1989, p. 3-9.

APPLE. "Brief of amici curiae Amazon.com et. al.", 3 mar. 2016a. Disponível em: <https://www.apple.com/pr/pdf/Amazon_Cisco_Dropbox_Evernote_Facebook_Google_Microsoft_Mozilla_Nest_Pinterest_Slack_Snapchat_WhatsApp_and_Yahoo.pdf>. Acesso em: 03 ago. 2016.

_____. "Usar o Mensagens com o iPhone, iPad ou iPod touch". Disponível em: <https://support.apple.com/pt-br/HT201287>. Acesso em: 17 jul. 2016b.

BESSA, Leonardo Roscoe. **Cadastro positivo**: comentários à Lei 12.414, de 09 de junho de 2011. São Paulo: Revista dos Tribunais, 2011.

BRASIL. Decreto n. 8.771, de 11 de maio de 2016. Regulamenta a Lei n. 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 maio. 2016. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Decreto/D8771.htm>. Acesso em: 26 jun. 2016.

BRASIL. Lei n. 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **Marco Civil da Internet**. Brasília, DF, 23 abr. 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 26 jun. 2016.

_____. Supremo Tribunal Federal. **Medida Cautelar na Arguição de Descumprimento de Preceito Fundamental n. 403 SE**, Pres. Min. Ricardo Lewandowski, Data de Julgamento e Publicação: 19 jul. 2016. Disponível em: <http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADPF403MC.pdf>. Acesso em: 19 jul. 2016.

CARVALHO, Daniel Balparda de. **Criptografia**: métodos e algoritmos. Rio de Janeiro: Book Express, 2000.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL (CERT.BR). **Cartilha de segurança para a Internet**: criptografia. Disponível em: <http://cartilha.cert.br/criptografia>. Acesso em: 17 jul. 2016.

DE LUCCA, Newton. Marco Civil da Internet: uma visão panorâmica dos principais aspectos relativos às suas disposições preliminares. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (coords.). **Direito & Internet III**: Marco Civil da Internet (Lei n. 12.965/2014). São Paulo: Quartier Latin, 2015. t. I.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.

ELMASRI, Ramez; NAVATHE, Shamkant B. **Sistemas de banco de dados**. 6. ed. São Paulo: Pearson Addison Wesley, 2011.

FREE SOFTWARE FOUNDATION. "Welcome to GPLv3". Disponível em: <http://gplv3.fsf.org>. Acesso em: 26 jun. 2016.

GITHUB. "Open Whisper Systems". Disponível em: <https://github.com/whispersystems>. Acesso em: 26 jun. 2016.

LEONARDI, Marcel. Marco Civil da Internet e proteção de dados pessoais. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (coords.). **Direito & Internet III**: Marco Civil da Internet (Lei n. 12.965/2014). São Paulo: Quartier Latin, 2015. t. I.

_____. **Responsabilidade civil dos provedores de serviços de Internet**. São Paulo: Juarez de Oliveira, 2005.

_____. **Tutela e privacidade na Internet**. São Paulo: Saraiva, 2011.

LUCCHESI, Cláudio Leonardo. **Introdução à criptografia computacional**. Campinas: Papirus (UNICAMP), 1986.

NORI, Fabio. A guarda dos registros de conexão e dos registros de acesso às aplicações no Marco Civil. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (coords.). **Direito & Internet III**: Marco Civil da Internet (Lei n. 12.965/2014). São Paulo: Quartier Latin, 2015. t. II.

OLSON, Parmy. "Facebook says it has wrapped up its landmark $19 billion acquisition of WhatsApp". **Forbes**, 06 oct. 2014. Disponível em:

<http://www.forbes.com/sites/parmyolson/2014/10/06/facebook-closes-19-billion-whatsapp-deal/#6b508e8179ee>. Acesso em: 17 jul. 2016.

OPEN WHISPER SYSTEMS. "WhatsApp's Signal Protocol integration is now complete", 05 apr. 2016. Disponível em: <https://whispersystems.org/blog/whatsapp-complete>. Acesso em: 26 jun. 2016.

PAESANI, Liliana Minardi. **Direito e Internet**: liberdade de informação, privacidade e responsabilidade civil. 2. ed. São Paulo: Atlas, 2003.

POSNER, Richard A. **A economia da justiça**. Trad. de Evandro Ferreira e Silva e Aníbal Mari. São Paulo: WMF Martins Fontes, 2010.

REINALDO FILHO, Demócrito Ramos. **Responsabilidade por publicações na Internet**. Rio de Janeiro: Forense, 2005.

SAMPAIO, José Adércio Leite. **Direito à intimidade e à vida privada**: uma visão jurídica da sexualidade, da família, da comunicação e informações pessoais, da vida e da morte. Belo Horizonte: Del Rey, 1998.

SCHNEIER, Bruce. **Segurança.com**: segredos e mentiras sobre a proteção na vida digital. Trad. de Daniel Vieira. Rio de Janeiro: Campus, 2001.

STALLINGS, William. **Criptografia e segurança de redes**. 4. ed. São Paulo: Pearson Prentice Hall, 2008.

SUPREMO TRIBUNAL FEDERAL. "Inscrições para audiência pública sobre WhatsApp e Marco Civil da Internet se encerram dia 1º/2", 25 jan. 2017. Disponível em: <http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=334536>. Acesso em: 31 mar. 2017.

_____."Ministro Fachin convoca audiência pública para debater bloqueios judiciais do WhatsApp", 3 nov. 2016. Disponível em: <http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=328600>. Acesso em: 31 mar. 2017.

_____. "Presidente do STF determina restabelecimento imediato dos serviços do WhatsApp", 19 jul. 2016. Disponível em: <http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=321191>. Acesso em: 19 jul. 2016.

_____. "STF inicia audiência pública que discute bloqueio judicial do WhatsApp e Marco Civil da Internet", 2 jun. 2017. Disponível em: <http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=345369>. Acesso em: 06 jul. 2017.

TAVARES, André Ramos. Liberdade de expressão-comunicação em face do direito à privacidade. In: MARTINS FILHO, Ives Gandra; MONTEIRO JUNIOR, Antônio Jorge (coord.). **Direito à privacidade.** Aparecida, SP: Idéias e Letras; São Paulo: Centro de Extensão Universitária, 2005.

TEIXEIRA, Tarcisio. **Curso de direito e processo eletrônico**: doutrina, jurisprudência e prática. 3. ed. atual. e ampl. São Paulo: Saraiva, 2015.

_____. **Marco civil da Internet comentado**. São Paulo: Almedina, 2016.

TOP500 SUPERCOMPUTER SITES. "Sunway TaihuLight - Sunway MPP, Sunway SW26010 260C 1.45GHz, Sunway". Disponível em: <https://www.top500.org/system/178764>. Acesso em: 26 jun. 2016.

TRIBUNAL DE JUSTIÇA DO ESTADO DO RIO DE JANEIRO. "Juíza ordena bloqueio do WhatsApp em todo o país", 19 jul. 2016a. Disponível em: <http://www.tjrj.jus.br/ca/web/guest/home/-/noticias/visualizar/36201?p_p_state=maximized>. Acesso em: 19 jul. 2016.

_____. "TJRJ suspende decisão e libera uso do WhatsApp", 19 jul. 2016b. Disponível em: <http://www.tjrj.jus.br/web/guest/home/-/noticias/visualizar/36204>. Acesso em: 19 jul. 2016.

TRIBUNAL DE JUSTIÇA DO ESTADO DE SÃO PAULO. "Justiça determina bloqueio do aplicativo WhatsApp", 16 dez. 2015a. Disponível em: <http://www.tjsp.jus.br/Institucional/CanaisComunicacao/Noticias/Noticia.aspx?Id=29056>. Acesso em: 17 jul. 2016.

_____. "TJSP concede liminar para restabelecer WhatsApp", 17 dez. 2015b. Disponível em: <http://www.tjsp.jus.br/Institucional/Corregedoria/Noticias/Noticia.aspx?Id=29057>. Acesso em: 17 jul. 2016.

TRIBUNAL DE JUSTIÇA DO ESTADO DE SERGIPE. "Desembargador Ricardo Múcio decide pelo cancelamento da suspensão do WhatsApp", 3 mai. 2016a. Disponível em: <http://www.tjse.jus.br/agencia/decisoes/item/9192-desembargador-ricardo-mucio-decide-pelo-cancelamento-da-suspensao-do-WhatsApp>. Acesso em: 17 jul. 2016.

_____. "Juiz criminal de Lagarto determina suspensão do WhatsApp por 72 horas", 2 mai. 2016b. Disponível em: <http://www.tjse.jus.br/agencia/decisoes/item/9187-juiz-criminal-de-lagarto-determina-suspensao-do-WhatsApp-por-72-horas>. Acesso em: 17 jul. 2016.

_____. "Nota sobre a prisão do vice-presidente do Facebook", 1 mar. 2016c. Disponível em: <http://www.tjse.jus.br/agencia/noticias/item/9073-nota-sobre-a-prisao-do-vice-presidente-do-facebook>. Acesso em: 17 jul. 2016.

UNITED STATES DISTRICT COURT FOR THE CENTRAL DISTRICT OF CALIFORNIA. "Order compelling Apple, Inc. to assist agents in search", Sheri Pym, Magistrate Judge, 16 feb. 2016. Disponível em: <https://assets.documentcloud.org/documents/2714005/SB-Shooter-Order-Compelling-Apple-Asst-iPhone.pdf>. Acesso em: 03 ago. 2016.

U.S. DISTRICT COURT FOR THE EASTERN DISTRICT OF NEW YORK, "Order requiring Apple, Inc. to assist in the execution of a search warrant issued by the court", James Orenstein, Magistrate Judge, 29 feb. 2016. Disponível em: <https://www.documentcloud.org/documents/2728314-Orenstein-Order.html>. Acesso em: 03 ago. 2016.

WHATSAPP. "Criptografia de ponta-a-ponta", FAQ (Geral). Disponível em: <https://www.whatsapp.com/faq/pt_br/general/28030015>. Acesso em: 26 jun. 2016a.

_____. "Terms of service". Disponível em: <https://www.whatsapp.com/legal>. Acesso em: 26 jun. 2016b.

YADRON, Danny. "Facebook, Google and WhatsApp plan to increase encryption of user data". **The Guardian**, 14 mar. 2016. Disponível em: <https://www.theguardian.com/technology/2016/mar/14/facebook-google-whatsapp-plan-increase-encryption-fbi-apple>. Acesso em: 17 jul. 2016.

Recebido em 13/10/2016.

Aprovado em 30/05/2017.