NOTA TÉCNICA SOBRE CRIPTOGRAFIA NO WHATSAPP

Na última terça-feira (05/04), a empresa WhatsApp anunciou que passou a implementar a "criptografia de ponta-a-ponta" nas últimas versões do aplicativo, hoje utilizado por 1 bilhão de pessoas em todo o mundo.[1] Somente no Brasil, o WhatsApp tem 90 milhões de usuários, tornando-o o mais popular "aplicativo de mensagens multiplataforma". A empresa foi fundada em 2009 nos EUA e comprada pelo Facebook em 2014.[2]

A adoção da criptografia[3] – um processo de "cifragem" de informação por meios de chaves numéricas sem as quais não é possível analisar o conteúdo da informação cifrada – pelo WhatsApp foi operacionalizado em parceria com a Open Whisper System, responsável por desenvolver o *Signal Protocol*.[4] Como anunciado pelo grupo, "todos os testes foram realizados" e agora o sistema de criptografia está pronto para ser adotado automaticamente para todos os usuários do aplicativo.

Segundo anunciado pela empresa, "a criptografia de ponta-a-ponta do WhatsApp assegura que somente você e a pessoa com a qual você está se comunicando podem ler o que é enviado **e ninguém mais, nem mesmo o WhatsApp**". Isso pois as "mensagens são criptografadas com um **cadeado único**, onde somente você e o destinatário possuem uma chave especial para abrir e ler a mensagem", afirma a empresa. Segundo o fundador da empresa Jan Koum, o propósito da criptografia é simples: "quando você manda uma mensagem, a única pessoa que pode ler é a pessoa ou grupo que você mandou a mensagem. Ninguém pode ver o conteúdo daquela mensagem. Nem *cibercriminosos*. Nem *hackers*. Nem regimes opressivos. Nem mesmo nós"[5].

O anúncio da adoção do complexo sistema de criptografia ocorreu em um contexto extremamente delicado de fortalecimento das capacidades de investigação e obtenção de dados por autoridades policiais, em nível global. Nos Estados Unidos da América, a Apple iniciou uma batalha contra o FBI após negar a instalação de um sistema de duplicação de informação e mensagens dos usuários do iPhone. Tanto a Apple quanto o

[1] https://www.whatsapp.com/security/
[2] https://www.crunchbase.com/organization/whatsapp#/entity (contendo dados sobre fundadores, financiamentos e capital investido na empresa).
[3] Para uma explicação do que é criptografia, ver o estudo de Fernando Trinta e Rodrigo Macedo pela UFPE (Trinta & Macedo, 1998): http://www.di.ufpe.br/~flash/ais98/cripto/criptografia.htm
[4] https://whispersystems.org/blog/whatsapp-complete/ (contendo uma análise técnica da implementação do *Signal Protocol*).
[5] Citado em matéria do Financial Times: http://www.ft.com/intl/cms/s/0/6edb3b6c-fb49-11e5-8f41-df5bda8beb40.html#axzz454kL56XX

WhatsApp apostam na criptografia como solução técnica para aumentar a privacidade dos seus usuários e evitar que terceiros visualizem o conteúdo de mensagens trocadas por tais aparelhos e aplicativos.

Para o Brasil, a questão é extremamente relevante por, pelo menos, dois motivos. Primeiro, pois a criptografia de ponta a ponta tem a capacidade de evitar "grampos" em chamadas realizadas pelo aplicativo, tal como ocorreu no recente episódio das gravações das ligações do ex-Presidente Luiz Inácio Lula da Silva.[6] Segundo, pois membros da Câmara dos Deputados finalizaram o relatório da "Comissão Parlamentar de Inquérito de Cibercrimes" (CPI Cibercrimes) e anunciaram que é preciso reforçar as capacidades das autoridades policiais para obtenção de dados de empresas de tecnologia.[7]

Some-se a esse cenário o turbulento episódio sobre a suspensão do WhatsApp em dezembro de 2015 em razão da recusa da empresa em encaminhar às autoridades policiais as mensagens de um narcotraficante,[8] bem como a prisão do Vice Presidente do Facebook em março de 2016 por descumprir ordens judiciais.[9] Há, sem dúvidas, um conflito entre o sistema de justiça brasileiro e a empresa estadunidense.

A adoção da criptografia de ponta a ponta para todas as comunicações feitas no WhatsApp é uma resposta às pretensões punitivas das autoridades policiais e legisladores do Brasil, dos Estados Unidos e do resto do mundo. Ao adotar um sistema de "chaves públicas" e "chaves privadas",[10] o WhatsApp cria um engenhoso processo onde não é possível decifrar as mensagens dos seus usuários a partir de seu servidor ou base de dados. Caso uma autoridade policial demande o repasse de informações de um dos usuários, a mensagem estará "embaralhada" e "indecifrável", pois a decodificação só pode ocorrer com a **chave única** (a chave privada) gerada automaticamente para o usuário.

---

[6] http://www.bbc.com/portuguese/noticias/2016/03/160317_juristas_grampos_jp (mapeando a divergência entre juristas sobre a violação da privacidade e legalidade do procedimento do juiz Sergio Moro pela Justiça Federal).
[7] http://www.brasilpost.com.br/2016/04/04/censura-cpi-crimes-ciberneticos_n_9610006.html (reforçando a crítica da sociedade civil às pretensões punitivas do relatório e a criminalização da Internet).
[8] http://www.idec.org.br/em-acao/em-foco/para-idec-bloqueio-do-whatsapp-foi-desproporcional-e-prejudicial-ao-consumidor (notando a violação do Código de Defesa do Consumidor e a desproporcionalidade da medida de suspensão, tendo em vista multas e cooperação internacional).
[9] http://tecnologia.uol.com.br/noticias/redacao/2016/03/01/pf-prende-vice-presidente-do-facebook-por-descumprir-ordens-judiciais.htm
[10] Ver o relatório técnico do WhatsApp em: https://www.whatsapp.com/security/WhatsApp-Security-Whitepaper.pdf

Como o consumidor é afetado?

Para o consumidor dos serviços do WhatsApp, a adoção da criptografia ponta a ponta significa mais *proteção à privacidade*, um direito basilar do Marco Civil da Internet (Lei 12.945/2014).

De acordo com o artigo 7º desta lei, os usuários de internet no Brasil possuem o direito à "inviolabilidade da intimidade e da vida privada" (inciso I), bem como a "inviolabilidade e sigilo do fluxo das suas comunicações pela internet" (inciso II). Na prática, a medida adotada pelo WhatsApp reforça tais direitos por meio da criptografia e de procedimentos computacionais. Da *perspectiva da proteção da privacidade aos consumidores*, a medida é benéfica e fortalece direitos civis.

Cidadãos e consumidores podem celebrar a adoção da criptografia de forma automática no aplicativo, considerando a dificuldade técnica de adotar mecanismos individuais de criptografia (ainda pouco utilizados em razão da dificuldade técnica de instalar e operar mecanismos de criptografia). Não é preciso esforço, pois a proteção ocorre para todos aqueles que usarem versões atualizadas do aplicativo.

Além disso, como notado por Camilla Costa (BBC Brasil), a criptografia do WhatsApp "torna a vida de hackers e autoridades mais difícil"[11]. Consumidores que costumam passar números de contas bancárias, dados pessoais e informações de cartões de crédito pelo aplicativo podem ficar tranquilos. A partir de agora, se um hacker invadir o servidor do WhatsApp, é pouco provável que ele será capaz de ler o conteúdo das mensagens enviadas pelo aplicativo. Isso significa mais segurança e menos vulnerabilidade dos consumidores para fraudes bancárias e financeiras – ainda gritantes no Brasil.

Por fim, é importante lembrar que a criptografia é uma técnica fundada na matemática que não garante segurança eterna. A criptografia pode ser "quebrada", como aconteceu na batalha do FBI contra a Apple.[12] No entanto, como lembra Edward Snowden – o ex-técnico contratado pela *National Security Agency* (NSA) para realizar operações de vigilância e monitoramento de dados na Internet que colocou o debate de privacidade no centro da agenda pública em 2013 –, a criptografia é uma importante ferramenta de proteção de direitos dos indivíduos.

Nada garante que a criptografia ponta a ponta do WhatsApp seja inquebrável e que governos e *hackers* não consigam acessar o conteúdo de mensagens dos usuários no

11 http://www.bbc.com/portuguese/noticias/2016/04/160406_whatsapp_criptografia_cc.shtml?ocid=socialflow_twitter

12 http://brasil.elpais.com/brasil/2016/03/29/internacional/1459204906_761502.html (informando como o governo estadunidense conseguiu "hackear" o iPhone 5 de um terrorista sem ajuda da Apple).

futuro. Mas, por enquanto, ela é uma extraordinária técnica de proteção de direitos de uso da Internet.

A dificuldade, obviamente, é a "responsabilização dos agentes de acordo com suas atividades", como diz o próprio artigo 3º do Marco Civil da Internet. Fica clara a tensão entre sistemas de segurança nacional e justiça criminal *versus* privacidade e proteção das comunicações pessoais. Com a criptografia ponta a ponta, os pedidos da Justiça brasileira de obtenção de comunicações de pessoas investigadas por crimes serão negados por "motivos técnicos". Essa tensão ainda renderá inúmeros debates públicos e está longe de ser resolvida.

Rafael A. F. Zanatta
Pesquisador em Telecomunicações – Idec