I Encontro Internacional de Gestão, Desenvolvimento e Inovação
12 a 14 de setembro de 2017- Naviraí-MS
I EIGEDIN 2017

WHATSAPP: da segurança as implicações judiciais no seu uso para troca de mensagens

Mariana Akemi Lombardi
Instituto Federal de Mato Grosso do Sul (IFMS)
akemims@gmail.com

Hávila Correia Bezerra
Instituto Federal de Mato Grosso do Sul (IFMS)
havilainfo@gmail.com

Danilo Adriano Mikucki
Instituto Federal de Mato Grosso do Sul (IFMS)
danilo.mikucki@ifms.edu.br

Eixo Temático: Tecnologias e sistemas de informação

RESUMO
O mundo moderno hoje exige agilidade e segurança nas ações que são realizadas no dia a dia das pessoas, incluindo as comunicações, onde as melhorias na tecnologia para aparelhos de celular e *smartphones* e os aplicativos desenvolvidos tornaram instantâneas a troca de informações. Com a evolução da tecnologia e o aperfeiçoamento dos sistemas operacionais, surgiram novos aplicativos como WhatsApp e Telegram. A criptografia utilizada nesses diversos aplicativos permitia que as informações trocadas entre os usuários, fossem armazenadas nos servidores das empresas. Com o aumento do uso deste tipo de aplicativo e os bilhões de informações trocadas entre os usuários, as empresas começaram a melhorar a segurança através da criptografia utilizada. No ano de 2014 o Facebook em parceria com a *Open Whisper Systems* começou a incorporar o protocolo T*extSecure* em sua mais nova aquisição, o aplicativo WhatsApp e em abril de 2016, todos os usuários do aplicativo começaram a ter suas mensagens criptografadas de ponta-a-ponta. Esta criptografia levantou um questionamento de ordem judicial, pois com este novo sistema de segurança, o WhatsApp passou a não fornecer mais informações importantes a justiça brasileira, levando ao Facebook severas punições como multas e bloqueios temporários do aplicativo.

Palavras-chave: Criptografia; segurança; informações; WhatsApp.

1 INTRODUÇÃO

Em virtude da necessidade de uma rede segura que não corresse o risco de ser interrompida, a internet surgiu em meados de 1969 em pleno conflito da Guerra fria para estreitar o elo de comunicação nos laboratórios dos Estados Unidos. Esta rede originalmente pertencia ao Departamento de Defesa norte americano e o seu intuito era manter a comunicação à longa distância, mesmo em casos de ataques aos seus meios de comunicação convencionais. (BRASIL, 2015)

A partir da liberação da *ARPAnet* (como era chamada a internet na sua origem) de conectar a comunicação somente entre laboratórios e universidades primeiramente nos Estados Unidos e depois nas universidades de outros países, a internet passou a ser uma rede sem um gerenciamento centralizado, o que a tornou um alvo difícil de ser destruído já que se espalhou pelo mundo de maneira veloz e sem controle. Literalmente a internet hoje é uma rede sem dono, onde cada componente é uma parte desse sistema distribuído pelo mundo (BRASIL, 2015).

A Intensidade com que a internet tomou conta do mundo é exatamente na mesma proporção que ela causou dependência no mesmo. Hoje, basicamente tudo e em todas as áreas existe a conexão com a internet, e isso de certa maneira agiliza e facilita as tarefas mais básicas na vida de uma pessoa comum, no ambiente corporativo, em todos os meios de comunicação, como por exemplo a televisão. Nada do que se fazia há alguns anos atrás se faz hoje sem a internet. As pessoas compram, vendem, fazem negócios, planejam viagens e até se relacionam pela internet, através das redes sociais, (ambientes completamente virtuais e exclusivamente dependente da internet) (BRASIL, 2015).

Um estudo realizado no Brasil pela TIC Domicílios apontou que em 2014, cerca de 50% dos domicílios possuíam computadores com acesso à internet. No período de 2011 a 2014 a utilização dos aparelhos celulares para acesso à internet triplicou, saltando de 15% em 2011 para 47% em 2014 (PANORAMA, 2016).

Desta forma pesquisar sobre os mensageiros instantâneos, com foco principal ao aplicativo WhatsApp, a segurança de sua criptografia e qual o impacto dela na sociedade brasileira, nos remete a uma análise sobre a sua utilização para troca de mensagens que não podem ser decodificadas para que a polícia e justiça tenham acesso as informações pertinentes as prisões de possíveis suspeitos e resoluções de crimes.

2 REVISÃO DA LITERATURA

2.1 CRIPTOGRAFIA

Desde a criação da internet, seu principal objetivo foi manter a comunicação entre pessoas por longas distâncias, com isso a necessidade de se criar os comunicadores instantâneos. Estes comunicadores nada mais são do que aplicações que permitem o envio e o recebimento de mensagens instantaneamente. Com o passar do tempo, esses comunicadores foram evoluindo e ganhando novas funções. Hoje não só as mensagens, mas outros dados como imagens, vídeos, e até mesmo documentos são lançados nestes ambientes com a possibilidade de serem recebidos em tempo real. E isso tomou conta do mundo.

Com o crescimento dos aplicativos de comunicação, também começaram a surgir nas redes, programas espiões e técnicas de interceptação de mensagens, criados para roubar dados e informações vulneráveis nestes locais. O fato de a internet ser uma rede totalmente aberta facilitou o surgimento destes crimes e com eles a necessidade de proteger estas informações.

Em decorrência disso:

> As conversas podem ter o histórico salvo para consulta futura, e ser transmitida de forma criptografada para aumentar a privacidade, mas é importante observar que os administradores do sistema podem ter acesso também a este histórico, pois pode ser salvo nos servidores envolvidos. Os programas de mensagens instantâneas não devem ser considerados como imunes à monitoração por terceiros a menos que utilizem programas especiais que codifiquem (utilizando métodos de Criptografia) os dados transmitidos entre o transmissor e o receptor (e vice-versa) (THIMOTTAS, 2013).

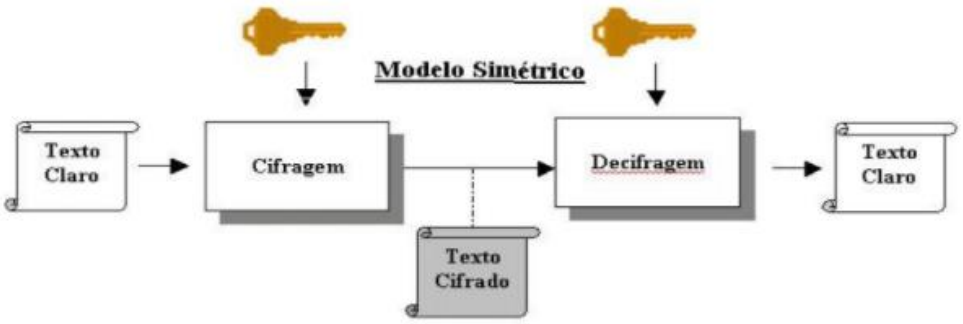
O termo Criptografia consiste no estudo de técnicas que usam maneiras inteligentes de enviar mensagens, e que no caminho entre o emissor e o receptor a mensagem sofra alterações e se torne inelegível. Sendo assim, apenas quem envia e quem recebe conhecem a mensagem na sua forma original, e qualquer outro que tente invadir, interceptar ou roubar a comunicação entre eles não entenda de forma alguma o conteúdo desta mensagem.

Seguindo esse estudo, pode-se destacar alguns métodos de criptografia conhecidos para uma melhor compreensão:

> A criptografia simétrica consiste em um processo no qual a cifragem e decifragem da informação ocorre por meio de uma única chave que é distribuída igualmente a todos os receptores da mensagem. A distribuição desta chave ocorre antes do envio da informação, possibilitando assim que seja entregue aos receptores errados (MORENO; PEREIRA; CHIARAMONTE, 2005).

Portanto, sistemas que utilizam a criptografia simétrica não são tão seguros quanto parecem, pois se por algum motivo a mensagem for interceptada e se a chave que foi utilizada para guardar esta informação for descoberta, todo o conteúdo será decifrado e a Criptografia não terá cumprido seu papel.

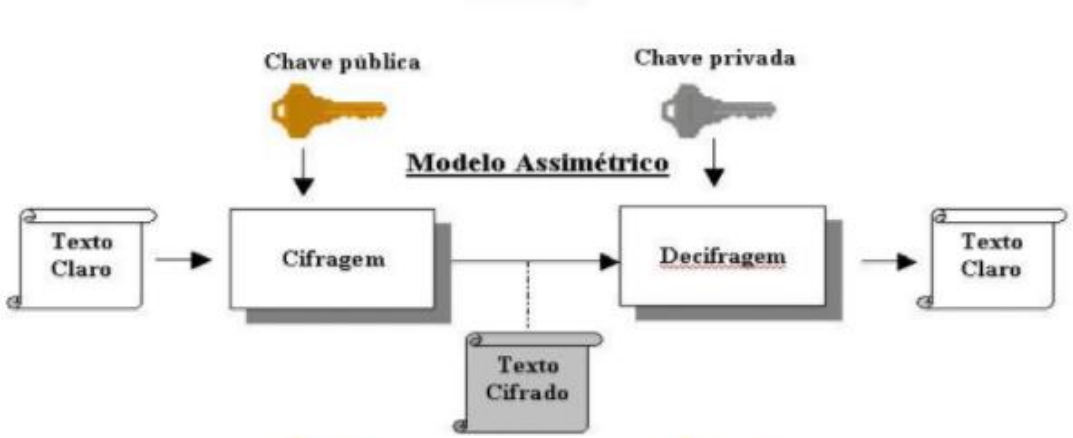
Figura 1: Criptografia Simétrica



A seguir é descrito o funcionamento da criptografia assimétrica:

> A criptografia assimétrica contorna o problema da distribuição de chaves mediante o uso de chaves públicas. A criptografia de chaves públicas foi inventada em 1976 por Whitfield Diffie e Martin Hellman, a fim de resolver o problema da distribuição de chaves. Neste novo sistema, cada pessoa tem um par de chaves denominado chave pública e chave privada. A chave pública é divulgada, enquanto a chave privada é mantida em segredo. Para mandar uma mensagem privada, o transmissor cifra a mensagem usando a chave pública do destinatário pretendido, que deverá usar a sua respectiva chave privada para conseguir recuperar a mensagem original (MORENO; PEREIRA; CHIARAMONTE, 2005).

Figura 2: Criptografia Assimétrica



Com a evolução da tecnologia e o aperfeiçoamento dos sistemas operacionais, surgiram novos programas de troca de mensagens instantâneas como Google Hangouts e Messenger do Facebook e para os aparelhos de celular e *smartphones* aplicativos como WhatsApp e Telegram.

A criptografia utilizada nesses diversos aplicativos permitia que as informações trocadas entre os usuários, fossem armazenadas nos servidores das empresas responsáveis por oferecerem o serviço.

Com o aumento do uso deste tipo de aplicativo e as bilhões de informações trocadas entre os usuários, forçou as empresas a começaram a melhorar a segurança dos dados, através da melhora no sistema de criptografia utilizado.

Segundo o Panorama Setorial da Internet (PANORAMA, 2016):

> Dentre as atividades desenvolvidas via telefone celular que requerem acesso à Internet, destacam-se a troca de mensagens de texto via aplicativos como Whatsapp e o uso de redes sociais, ambas desempenhadas por 47% dos usuários do dispositivo. Elas lideram também entre os usuários de Internet exclusivamente pelo celular, representando 87% e 74% dos casos, respectivamente.

2.2 HISTÓRIA DO WHATSAPP

Criado em 2009 por Jan Koum, o WhatsApp preza pela privacidade e a não mercantilização do aplicativo, onde segundo Koum *"se assegurou desde o início do WhatsApp há cinco anos que o aplicativo recolha a menor quantidade possível de dados dos usuários, que só precisam de seu número de celular para se identificar e ter acesso ao serviço (2014). " (EFE, 2014)*

Em fevereiro de 2014, foi anunciado pelo Facebook, a compra do WhatsApp, por 16 bilhões de dólares, e finalizado a sua negociação por 22 bilhões de dólares em outubro do mesmo ano, na época o aplicativo já contava com mais de 600 milhões de usuários por mês. (BARROS, 2014)

Em novembro de 2014 o WhatsApp começa a alterar a sua criptografia em uma parceria com a *Open Whisper Systems(OWS)*, baseado nos protocolos de segurança do aplicativo de troca de mensagens via SMS *TextSecure* para Android e do *Signal* para IOS, o WhatsApp de forma a incorporar a criptografia de ponta-a-ponta, solicitou a OWS a adaptação aos seus protocolos, não permitindo mais aos seus servidores a captura das informações e decifrar as mensagens, mesmo que a empresa seja obrigada pela aplicação da lei. (OPEN, 2014; BRANDOM, 2014 a, tradução nossa)

> Segundo a equipe, o Signal não deixa nenhum metadado, nos registros que as companhias de telefone produzem de quem você chamou e quando. [...] A criptografia é feita localmente em seu telefone, então, mesmo que a empresa desejasse decodificar suas mensagens, seria difícil fazê-lo depois do fato. E de acordo com seus aplicativos anteriores, Whisper não tem sido tímido sobre a abertura de seu código para a inspeção pública para garantir essas promessas de verificação. O Signal é de código aberto, o que significa que toda a base de código está configurada para ser postada na conta GitHub da Whisper (2014). (BRANDOM, 2014 b, tradução nossa)

Em abril de 2016, passou a ser utilizada a criptografia de ponta-a-ponta, onde é assegurado 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 (ENTENDA, 2016).

"A Criptografia de "ponta-a-ponta" refere-se a um sistema em que a mensagem sai codificada do dispositivo que envia e só é decodificada quando chega ao destinatário". (WHATSAPP, 2016 a)

2.3 CRIPTOGRAFIA WHATSAPP

Segundo a visão geral apresentado pelo WhatsApp em seu site, a criptografia de ponta a ponta inicia no momento da instalação, quando o aplicativo cria as chaves de identidade, chave de pré-assinatura, que é assinada pela chave identidade e tem sua alteração em períodos estabelecidos e chave de utilização, que pode ser reposta quando necessária (MARTINELLI, 2016; WHATSAPP, 2016 b, tradução nossa).

As chaves de sessão são criadas para a criptografar as mensagens, sendo a Chave Raiz criada para gerar a Chave de Cadeia, que criará a Chave de Mensagem, que irá encriptar as mensagens. (MARTINELLI, 2016; WHATSAPP, 2016 b, tradução nossa)

Registro do cliente

> No momento da inscrição, um cliente do WhatsApp transmite sua Chave de identidade pública, chave de pré-assinatura (com sua assinatura) e chave de utilização para o servidor, que armazena as Chaves públicas associadas com o identificador do usuário. Em nenhum momento o servidor do WhatsApp tem acesso a qualquer uma das chaves privadas do cliente. (WHATSAPP, 2016 b, tradução nossa).

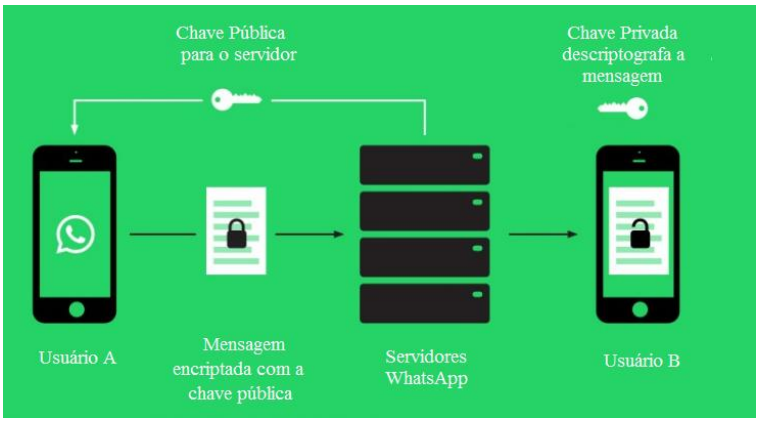
A troca de mensagens ocorre após o estabelecimento da primeira sessão criptografada entre os clientes, não sendo necessário estabelecer novas sessões para novas mensagens. Em caso de encerramento de sessão, por reinstalação do aplicativo ou troca do dispositivo, será necessário estabelecer uma nova sessão (WHATSAPP, 2016 b, tradução nossa).

Uma vez estabelecida uma sessão, os clientes trocam mensagens que são protegidas com uma chave de mensagem. A Chave de Mensagem muda para cada mensagem transmitida, e é efêmera, tal que a Chave de Mensagem usada para criptografar uma mensagem da sessão

não pode ser reconstruída, depois de uma mensagem ter sido transmitida ou recebida. A Chave de Mensagem é derivada da Chave de Cadeia de um remetente que se acopla com cada mensagem enviada. De acordo com cada mensagem de ida e volta uma nova Chave Da Corrente é criada. Isto proporciona segredo para a frente através da combinação. (WHATSAPP, 2016 b, tradução nossa)

Anexos grandes de qualquer tipo (vídeo, áudio, imagens ou arquivos) também são criptografados de ponta a ponta. A figura 03 demonstra o processo descrito sobre a criptografia de ponta-a-ponta utilizado pelo WhatsApp.

Figura 3: Criptografia ponta-a-ponta do WhatsApp



No ano de 2014, a *Eletronic Frontier Foundation*, analisou diversos aplicativos e como sua criptografia garante a segurança de seu usuário, demonstrando ser o WhatsApp um dos mais seguros para a troca efetiva de mensagens instantâneas em comparação aos concorrentes como o Telegram, Facebook bate-papo e Google Hangouts, que mesmo criptografando as mensagens, permite que o servidor possa armazenar informações, permite a identificação dos contatos e não garante a segurança caso ocorra algum roubo de chaves de codificação. (EFF, 2014 tradução nossa).

Figura 4: ***Eletronic Frontier Foundation***

	Criptografado em transito?	Criptografado para o provedor não poder lê-lo?	Você pode verificar as identidades dos contatos?	As comunicações são seguras mesmo se as chaves forem roubadas?	É o código aberto a revisões independentes?	É o projeto de segurança devidamente documentado?	Houve alguma auditoria de código recente?
Facebook bate-papo	✓	✗	✗	✗	✗	✗	✓
Google Hangouts / "Chat of de record"	✓	✗	✗	✗	✗	✗	✓
Signal/ RedPhone	✓	✓	✓	✓	✓	✓	✓
Telegram	✓	✗	✗	✗	✓	✓	✓
Telegram (chats secretos)	✓	✓	✓	✓	✓	✓	✓
TextSecure	✓	✓	✓	✓	✓	✓	✓
WhatsApp	✓	✓	✓	✓	✗	✓	✓

Demonstra também que os aplicativos *TextSecure* e *Signal*, por possuírem seus códigos abertos a revisões independentes, chamaram a atenção do WhatsApp para melhorar a sua criptografia, possibilitando chegar a utilizada atualmente.

2.4 CUMPRIMENTO JUDICIAL

Com o aumento da segurança na troca de informações, o mundo moderno começou a enfrentar uma nova batalha, a obtenção de informações de pessoas sob investigação criminal que utilizam estes tipos de aplicativos para a troca de mensagens.

Uma vez que a criptografia utilizada não regista e nem salva em seus servidores as mensagens e somente quem envia e recebe possuem permissão para sua leitura, as investigações tem enfrentado a falta de colaboração das empresas fornecedoras do serviço.

A não colaboração tem levado a justiça a utilizar a legislação brasileira em favor de sentenças que vão desde multas milionárias a bloqueios temporários do aplicativo, baseados nos incisos I, II e III do Artigo nº 12 da lei n 12965/2014, que trata sobre o Marco Civil da Internet:

> Art. 12. Sem prejuízo das demais sanções cíveis, criminais ou administrativas, as infrações às normas previstas nos arts. 10 e 11 ficam sujeitas, conforme o caso, às seguintes sanções, aplicadas de forma isolada ou cumulativa:
> I - advertência, com indicação de prazo para adoção de medidas corretivas;

> II - multa de até 10% (dez por cento) do faturamento do grupo econômico no Brasil no seu último exercício, excluídos os tributos, considerados a condição econômica do infrator e o princípio da proporcionalidade entre a gravidade da falta e a intensidade da sanção;
> III - suspensão temporária das atividades que envolvam os atos previstos no art. 11; (BRASIL, 2016)

Nos últimos 2 anos o WhatsApp enfrentou 4 pedidos de bloqueios e já teve mais de R$ 57 milhões bloqueados, por descumprimento ao Artigo nº 11 e seus parágrafos 1º e 2º da lei nº 12.965/2014, no qual trata sobre as informações trocadas em território nacional, mesmo que as sedes das empresas estejam localizadas no exterior, uma vez que um dos responsáveis pela troca das mensagens estejam em solo brasileiro.

> 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.
> § 1º O disposto no **caput** aplica-se aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil.
> § 2º O disposto no **caput** aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil (BRASIL, 2016).

Em fevereiro de 2015, um juiz do Piau determinou o 1º pedido de bloqueio do WhatsApp, por descumpri decisões anteriores, cujo processo teve início em 2013 e se referia a crimes envolvendo crianças e adolescentes.

Segundo o juiz Luiz de Moura Correia, do Piauí, "*Até pouco tempo atrás nós fazíamos interceptações telefônicas, mas hoje ninguém usa telefone [para falar], usa o WhatsApp. Para que se possa saber o que criminosos comunicaram, onde estão, é através dos apps*" (WHATSAPP, 2016 c).

O aplicativo não chegou a ser bloqueado, pois uma determinação de um desembargador do Tribunal de Justiça do Piauí suspendeu o bloqueio.

O bloqueio ocorre através de determinações judiciais enviadas as empresas de telefonia e segundo explicação do especialista em telecomunicações e segurança da informação André Jaccon:

> O WhatsApp é bloqueado pelo IP e não pela rede móvel das operadoras. [...] 'O bloqueio é feito pelo IP (Internet Protocol) dos servidores. Quando o aplicativo se conecta, ele estabelece um endereço no servidor. É aí que as operadoras vão barrar o acesso aos usuários do Brasil', explica, lembrando que isso vale tanto para conexões por rede fixa ou móvel. (UOL, 2016)

Em dezembro de 2015, ocorre o 2º pedido de bloqueio, desta vez o desembargador Xavier de Souza, da 11ª Câmara Criminal do Tribunal de Justiça de São Paulo, determinou que fosse bloqueado por 48 horas, com base na lei do Marco Civil da Internet, pelo não cumprimento de mandados anteriores de julho e agosto de 2015. (WHATSAPP, 2016 c)

O aplicativo permaneceu inativo por 12 horas, voltando a funcionar por determinação do Tribunal de Justiça de São Paulo.

Em maio de 2016, o juiz Marcel Montalvão, da comarca de Lagarto, estado de Sergipe, pediu o bloqueio do aplicativo, pois queria que a companhia repassasse informações sobre uma quadrilha interestadual de drogas para uma investigação da Polícia Federal, o que a companhia se negava a fazer. "O bloqueio, no entanto, durou 25 horas. O desembargador Ricardo Múcio Santana de Abreu Lima, do Tribunal de Justiça de Sergipe, diz que a proibição do app no Brasil gerou '**caos social em todo o território**' e determinou o desbloqueio " (WHATSAPP, 2016 c).

Em 19 de julho de 2016, ocorre o 4º pedido de bloqueio do WhatsApp, onde a juíza Daniela Barbosa de Souza, município de Duque de Caxias, estado do Rio de Janeiro, determina que " 'As mensagens trocadas deverão ser desviadas em tempo real (na forma que se dá com a interceptação de conversações telefônicas), antes de implementada a criptografia', escreveu a juíza " (DECISÃO, 2016).

O aplicativo permaneceu bloqueado por mais ou menos 4 horas, até o presidente de plantão do Supremo Tribunal Federal, ministro Ricardo Lewandowski, decidiu derrubar a decisão do Tribunal de Justiça do Rio de Janeiro.

> Para o presidente do Supremo, o bloqueio foi uma medida desproporcional porque o WhatsApp é usado de forma abrangente, inclusive para intimações judiciais, e fere a segurança jurídica. [...]destacou que o entendimento da juíza do Rio foi 'pouco razoável e desproporcional' porque deixou milhões de brasileiros sem o meio de comunicação. [...] destacou que o Marco Civil da Internet tem como princípio a garantia da liberdade de expressão e comunicação. E afirmou que a lei tem preocupação com a segurança e com a funcionalidade da rede. [...] considerou que as mensagens instantâneas têm grande impacto na vida dos cidadãos e que a própria juíza do Rio destacou que o WhatsApp tem mais de 1 bilhão de usuários no mundo – o Brasil é o segundo país com mais usuários. (OLIVEIRA, 2016)

Em outra determinação judicial, desta vez da Justiça Federal do Mato Grosso, através de um pedido do Ministério Público Federal do estado, o Facebook empresa proprietária do WhatsApp, teve bloqueado de seus cofres a quantia de "R$ 6,9 milhões da empresa Facebook Serviços On-line Brasil Ltda por causa do descumprimento de decisões judiciais referentes à interceptação de mensagens enviadas e recebidas pelo aplicativo WhatsApp. " (JUIZ, 2016)

> Segundo o MPF, a empresa WhatsApp justificou o descumprimento da decisão

> judicial dizendo que o conteúdo das mensagens trocadas pelo aplicativo transitam instantaneamente pelos servidores, não ficam armazenadas e têm encriptação feita pelo aparelho telefônico dos usuários, tornando-as indecifráveis pela empresa. (JUIZ, 2016)

Em pesquisa realizada no site do próprio WhatsApp, é possível encontrar uma afirmativa da empresa quanto a recuperação dos dados do aplicativo:

> *O WhatsApp pode me ajudar a recuperar meus dados?*
> *Infelizmente, não temos como ajudá-lo a restaurar suas conversas, documentos, arquivos multimídia, backups ou histórico de ligações.*
> *Por favor, entenda que nós não armazenamos suas mensagens em nossos servidores após elas terem sido entregues. Lembre-se, também, que suas mensagens são criptografadas de ponta-a-ponta quando você e os seus contatos estão usando as versões mais recentes do nosso aplicativo. A criptografia de ponta-a-ponta do WhatsApp garante que somente você e a pessoa com quem você está se comunicando podem ler o que foi enviado e ninguém mais, nem mesmo o WhatsApp. Na maioria dos casos esses históricos e arquivos de mídia podem ser encontrados somente no seu aparelho ou no aparelho da pessoa com quem você conversou ou para quem você ligou.* (FAQ, 2016)

Nota-se que o WhatsApp faz questão de deixar claro que não armazena nenhum dado em seus servidores e a sua criptografia não deixa registros, somente nos equipamentos em que as contas de quem enviou e recebeu a mensagem utilizou.

A ausência de responsabilidade pelas empresas que prestam o serviço dos mensageiros instantâneo acaba por dificultar o trabalho da justiça nas investigações de crimes como o tráfico de drogas e de influência, corrupção, terrorismo, pedofilia entre outros.

3 METODOLOGIA

A metodologia utilizada foi a pesquisa bibliográfica, por se tratar de um assunto de importância a sociedade digital e não possuir muitos periódicos e artigos relevantes sobre o assunto, a pesquisa foi realizada através da análise das publicações disponíveis sobre criptografia para os aplicativos de mensagens instantâneas, com ênfase principal nas informações disponíveis sobre o WhatsApp, encontradas principalmente em páginas da internet, com o devido cuidado sobre a veracidade das informações, assim como as publicações sobre os descumprimentos de ordens judiciais, as penalidades ao aplicativo e a legislação brasileira vigente sobre o assunto.

4 DISCUSSÃO E ANÁLISE DOS DADOS

O uso da criptografia, como forma de codificação das mensagens utilizada nos aplicativos de mensagens, realmente proporciona a segurança do usuário, mas ao mesmo tempo em que protege suas informações, pode estar acobertando a prática de crimes no mundo real e cibernéticos, com a alegação das empresas que oferecem o serviço, onde afirmam não possuírem acesso ao conteúdo das mensagens.

Verificou-se que dos tipos de criptografia utilizados nos diversos aplicativos de mensagens instantâneas, a criptografia de ponta-a-ponta vem sendo considerada o melhor método para garantir que as informações dos usuários estejam realmente seguras e livres de invasões por terceiros.

Pode-se constatar que o uso da criptografia melhora a segurança das informações trocadas entre os seus usuários, mas esta mesma segurança está levando a usabilidade dos aplicativos a estágios preocupantes por parte da polícia e da justiça quanto às investigações de crimes como o tráfico de modo geral, terrorismo, corrupção, pedofilia e muitos outros tipos, pois com a isenção das empresas, ao alegarem que somente os usuários envolvidos nas trocas das mensagens são detentores das informações, muitas investigações são prejudicadas pela falta de provas concretas que podem incriminar ou indicar os prováveis responsáveis pelos delitos.

Deve-se refletir se realmente as informações não são salvas nos servidores, uma vez que em um código não abertos a revisão, fica o questionamento quanto ao que realmente passa pelos servidores e se em algum momento algo pode ser armazenado, gerando uma dúvida quanto a efetividade da criptografia de ponta-a-ponta não armazenar dados em servidores.

Outro ponto que deve ser levado em consideração são os milhões gastos pela empresa detentora do aplicativo nas ações e multas cobradas pela justiça brasileira, por não cumprir as determinações judiciais, onde é questionável até que ponto os milhões de usuários do aplicativo são vantajosos para suprir os gastos com as cobranças. Ou seria somente uma forma de ampliar o quantitativo de usuários, mesmo que a propaganda seja negativa, por não colaborar com a justiça, mas suficiente para a divulgação de sua marca.

5 CONCLUSÕES

O uso da criptografia como segurança para os usuários é realmente o método mais seguro para garantir que seus dados compartilhados nas conversas estão realmente protegidos, mas também traz a incerteza de que muitos feitos contrários aos princípios legais do país

possam estar sendo cometidos e seus devidos responsáveis poderão ficar impunes, por não ser possível a sua identificação.

A total dependência hoje dos aplicativos de mensagens instantâneas faz com que a população vire refém de certos hábitos e consequentemente, cause certos vícios que com o tempo tendem a piorar a socialização entre as pessoas, onde a ausência, mesmo que momentânea do uso do aplicativo possa causar danos irreparáveis às gerações presentes e futuras.

REFERÊNCIAS

BRASIL. **CPI – Crimes Cibernéticos** – Relatório Final. 2015. Disponível em: http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra;jsessionid=214D61B364D3F74027CAB7F56C3E0C39.proposicoesWeb2?codteor=1455189&filename=REL+4/2016+CPICIBER+%3D%3E+RCP+10/2015. Acesso em 25 de nov. 2016.

BRASIL. LEI Nº 12.965, DE 23 DE ABRIL DE 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em 19 de out. 2016.

THIMOTTAS. **Comunicação via Internet**. Disponível em: https://thimottas.wordpress.com/2013/03/21/comunicacao-via-internet/ . Acesso em 01 de dez. 2016.

MORENO, E.D.; PEREIRA, F. D.; CHIARAMONTE, R.B. **Criptografia em Software e Hardware**. 1ªed. São Paulo: Novatec, 2005. p.21-42. Disponível em: http://www.martinsfontespaulista.com.br/anexos/produtos/capitulos/143116.pdf Acesso em 05 de dez. 2016.

EFE, Agencia. **A história (e o estilo) de Jan Koum, criador do WhatsApp**. 2014. Disponível em: http://epocanegocios.globo.com/Inspiracao/Vida/noticia/2014/02/historia-e-o-estilo-de-jan-koum-criador-do-whatsapp.html. Acesso em 02de set. 2016.

BARROS, Thiago. **Facebook finaliza aquisição do Whatsapp por US$ 22 bilhões**. 2014. Disponível em: http://g1.globo.com/economia/negocios/noticia/2014/10/preco-de-compra-do-whatsapp-pelo-facebook-sobe-us-22-bilhoes.html. Acesso em 02 de set. 2016.

OPEN Whisper Systems partners with WhatsApp to provide end-to-end encryption. 2014. Disponível em: https://whispersystems.org/blog/whatsapp/. Acesso em 02 de set. 2016.

BRANDOM, Russel. WhatsApp lança criptografia end-to-end usando o código textsecure. **The Verge**. 2014 a. Disponível em: http://www.theverge.com/2014/11/18/7239221/whatsapp-rolls-out-end-to-end-encryption-with-textsecure. Acesso em 15 de set.2016

BRANDOM, Russel. O Signal traz chama criptografada indolor para iOS. **The Verge**. 2014 b. Disponível em: http://www.theverge.com/2014/7/29/5945547/signal-brings-painless-

encrypted-calling-whisper-systems-moxie-marlinspike. Acesso em 15 de set. 2016.]

WHATSAPP. **Criptografia de Ponta-a-Ponta**. 2016 a. Disponível em: https://www.whatsapp.com/faq/pt_br/general/28030015. Acesso em 02 de set.2016.

ENTENDA como funciona o novo sistema de criptografia do WhatsApp. 2016. Disponível em: http://www1.folha.uol.com.br/tec/2016/04/1757710-entenda-como-funciona-o-novo-sistema-de-criptografia-do-whatsapp.shtml. Acesso em 01 de dez. 2016.

MARTINELLI, Gustavo G. **Whatsapp e Criptografia:** qual o limite da Justiça? - 13ª Conferência Latino-Americana de Software Livre 2016. Foz do Iguaçu. 18 de out. 2016.

WHATSAPP **Encryption Overview.** 2016 b. Disponível em: https://www.whatsapp.com/security/. Acesso em 02 de set. 2016.

EFF. Eletronic Frontier Foundation. **Secure Messaging Scorecard.** 2014. Disponível em: https://www.eff.org/node/82654 . Acesso em 21 de set. 2016.

WHATSAPP é alvo de 4ª decisão de bloqueio no Brasil; relembre outros. 2016 c. Disponível em: http://www1.folha.uol.com.br/mercado/2016/07/1793284-whatsapp-e-bloqueado-pela-4-vez-no-brasil-relembre-outros-casos.shtml . Acesso 08 de dez. 2016.

UOL. Entenda como o WhatsApp é bloqueado em todo o Brasil. 2016. Disponível em: http://tecnologia.uol.com.br/noticias/redacao/2016/05/02/entenda-como-o-whatsapp-e-bloqueado-em-todo-o-brasil.htm . Acessado em 08 de dez. 2016.

DECISÃO judicial aumenta pressão para WhatsApp abrir dados no Brasil. 2016. Disponível em: http://www1.folha.uol.com.br/mercado/2016/07/1793445-decisao-judicial-aumenta-pressao-para-whatsapp-abrir-dados-no-brasil.shtml . Acesso 08 de dez. 2016.

OLIVEIRA, Mariana. **STF suspende decisão da Justiça do Rio que bloqueou WhatsApp**. 2016. Disponível em: http://g1.globo.com/tecnologia/noticia/2016/07/stf-suspende-decisao-da-justica-do-rio-que-bloqueou-whatsapp.html . Acesso 08 de dez. 2016.

JUIZ federal de MT determina bloqueio de R$ 6,9 milhões do Facebook. 2016. Disponível em: http://g1.globo.com/mato-grosso/noticia/2016/09/juiz-federal-de-mt-determina-bloqueio-de-r-69-milhoes-do-facebook.html. Acesso em 29 de set. 2016.

FAQ-Geral - O WhatsApp pode me ajudar a recuperar meus dados? 2016. Disponível em: https://www.whatsapp.com/faq/pt_br/general/148692005347639 Acesso em 02 de Dez. 2016.

Panorama Setorial da Internet. **Acesso à Internet no Brasil**: Desafios para conectar toda a população. 2016. Disponível em: https://www.nic.br/media/docs/publicacoes/6/Panorama_Setorial_11.pdf . Acesso em 18 de ago. 2017.