WHATSAPP COMO MEIO DE PROVA NO JUDICIÁRIO BRASILEIRO: UMA ANÁLISE SOBRE OS RISCOS DE FRAUDE DESTE MEIO DE PROVA

Whatsapp as means of proof in brazilian judiciary: an analysis on the fraud risks of this means of proof

Whatsapp como medio de prueba en el poder judicial brasileño: un análisis sobre los riesgos de fraude de este medio de prueba

Revista Desafios

Artigo Original
Original Article
Artículo Original

Eduardo Carvalho Martins[1], Italo Schelive Correia[*1],

[1]Laboratório Universitário de Assistência Regional Ambiental, Curso de Graduação em Direito, Universidade Estadual do Tocantins – Câmpus Dianópolis, Dianópolis, Tocantins, Brasil.

**Correspondência: Praça Aurélio Antônio Araújo, 02. Centro, Dianópolis, Tocantins, Brasil. CEP: 77300-000. e-mail eduardo@unitins.br.*

Artigo recebido em 21/08/2020 aprovado em 22/09/2020 publicado em 10/06/2021.

RESUMO

O presente artigo buscou analisar a integridade das mensagens do aplicativo WhatsApp na qualidade de provas judiciais, tendo em vista as suas recentes e reiteradas utilizações por parte da justiça brasileira. Para tanto, este trabalho dedicou-se a demonstrar os avanços tecnológicos do aplicativo, bem como, as suas incapacidades técnicas, ao não verificar a integridade das mensagens por ele enviadas. Para isso, o artigo baseia-se em pesquisa explicativa, com sua metodologia baseada em revisão bibliográfica e os dados se apresentam de forma qualitativa ao longo do trabalho. Em suma, o conteúdo contido no celular do usuário, a que se extrai as mensagens, é tido, de pronto, como verdadeiro. Porém, existem possibilidades, ora ignoradas, deste sofrer adulterações. Neste sentido, serão expostas – sem o objetivo de ensinar – algumas técnicas de adulteração, onde, mesmo com a lavratura de uma ata notarial, conteúdos manipulados se edificam como probos e verdadeiros, dotados de fé pública, na qualidade de prova pré-constituída, ainda que analisadas e extraídas por peritos, o que pode resultar em grandes prejuízos na busca da verdade processual.

Palavras-Chave: Ata notarial; Conteúdos manipulados; Mensagens do aplicativo WhatsApp; Provas judiciais; Técnicas de adulteração.

ABSTRACT

This article sought to analyze the integrity of WhatsApp application messages as judicial evidence, in view of its recent and repeated uses by the Brazilian justice system. To this end, this work was dedicated to demonstrating the technological advances of the application, as well as its technical incapacities, by not verifying the integrity of the messages sent by it. For this, the article is based on explanatory research, with its methodology based on bibliographic review and the data are presented qualitatively throughout the work. In short, the content contained in the user's cell phone, from which the messages are extracted, is readily considered to be true. However, there are possibilities, now ignored, of this to suffer adulterations. In this sense, some adulteration techniques will be exposed - without the objective of teaching - where, even with the drafting of notary minutes, manipulated contents are built as evidence and true, endowed with public faith, as pre-constituted evidence, although analyzed and extracted by experts, which can result in great losses in the search for procedural truth.

Keywords: *Adulteration techniques; Judicial evidence; Manipulated content; Notary minutes; WhatsApp application messages.*

Introdução

O uso de aplicativos de redes sociais já é uma realidade no cotidiano da população mundial. Uma gama de pessoas utiliza aparelhos tipo *smartphone*, que viabilizam esse tipo de usabilidade, sendo um exemplo de aplicativo colaborativo e interativo, o WhatsApp é um instrumento que promove a dinamização social. O uso desta ferramenta possibilita inúmeras vantagens para o usuário, uma delas a capacidade de armazenar conversas. Em uma projeção do uso constante deste meio de comunicação baseando-se em sua popularidade, o poder judiciário acabou acatando o aplicativo como um importante meio de comprovação de fatos, contudo, verificou-se a necessidade de averiguar se estes fatos armazenados devam ser questionados tecnicamente de alguma forma.

Em razão do uso constante de tecnologias, o uso do aplicativo destaca uma característica muito usual das relações contemporâneas, que são as trocas de mensagens instantâneas, com imagens, textos, documentos, entre outros, em vista da facilidade de acesso, insere-se como meio de comunicação usual de toda a sociedade moderna global.

Desta forma, o poder judiciário acabou por utilizar-se deste instrumento, acatando o conteúdo do WhatsApp por atas notariais e perícias técnicas judiciais. Ressalta-se o fato que o uso de um *screenshot*[1] como meio de prova usualmente não é aceito como prova, em razão da facilidade em se editar um conteúdo como este, não necessitando de habilidades técnicas especializadas para tal feito.

Contudo, não há no mundo jurídico registro de questionamentos quanto a veracidade dessas provas quando obtidas com aval de um tabelião ou perito, pois estes constatarão a autenticidade do conteúdo apresentado no aplicativo, conteúdo este que também, assim como uma imagem por *screenshot*, é passível de edição conforme o presente artigo irá evidenciar.

Neste trabalho, será apresentado uma análise da veracidade do aplicativo WhatsApp como meio de comprovação de fato jurídico no poder judiciário brasileiro. Demonstrando a impossibilidade de autenticação e validação da veracidade de uma mensagem diante de sua criptografia ponta-a-ponta, bem como a possibilidade de edição de mensagens, como o WhatsApp é utilizado no judiciário brasileiro como meio de prova e por fim foram expostas exemplificações do porquê esse uso de prova é questionável.

Respondendo aos seguintes questionamentos: Como o poder judiciário utiliza o aplicativo WhatsApp como meio de prova? Quais as funcionalidades que o tornam um mecanismo confiável de prova para o poder judiciário? Quais as fragilidades que este tipo de aplicativo pode apresentar que o impossibilitem de ser meio de prova judicial?

O estudo se apresenta por meio de pesquisa explicativa, sendo a metodologia baseada em revisão bibliográfica, valendo-se de artigos nacionais e internacionais para construção do referencial bibliográfico do assunto, os resultados serão apresentados de forma qualitativa por meio de figuras e tabelas, que serão disponibilizadas ao longo do texto como forma de demonstrar o manuseio do próprio aplicativo com conhecimentos técnicos do pesquisador, constatando o funcionamento do WhatsApp e possível manipulação de dados, desta forma o seu uso será utilizado como experimento da teoria apresentada.

O tema possui relevância social e jurídica, uma vez que tem como objetivo a demonstração de possíveis avanços tecnológicos do WhatsApp, bem como, evidenciar que o mesmo possui inconsistências, ao não verificar a integridade das mensagens por ele

[1] "As capturas de tela são imagens de conteúdo apresentado em uma tela, ou parte dela, e normalmente fornecem uma representação estática da tela em um determinado momento" (FRANK; WRIGHT, 2016, tradução nossa).

enviadas uma vez que esta falha permite fraudar a justiça e a possibilidade de se fabricar uma prova que influenciará na convicção do magistrado justifica seu estudo.

Sobre o WhatsApp

O WhatsApp é um aplicativo para *smartphones* que é utilizado para troca instantânea de informações, surgindo como alternativa para o sistema de mensagens SMS[2] (WHATSAPP, 2020a). Este, funciona através da *internet* e vem ganhando popularidade mundial, especialmente fora dos Estados Unidos que é seu país de origem. Em pesquisa realizada pelo *site* Panorama com população amostra 2.072 brasileiros, constatou-se que o aplicativo está presente em 99% dos *smartphones* dos entrevistados e que este, é usado diariamente por 98% dos mesmos (PAIVA, 2020).

Mantido pelo *Facebook* desde o ano de 2014, quando a rede social comprou todos os direitos do aplicativo (REUTERS, 2014), o aplicativo vem recebendo gradualmente atualizações, isto, lhe garante acréscimos de recursos e segurança de dados como é o caso da criptografia, contudo, não houve atualização que tratasse especificamente sobre a integridade de conversas registradas no aparelho celular.

Criptografia

Diferente dos serviços fornecidos por uma operadora de telefone, o WhatsApp é criptografado com tecnologia "ponta-a-ponta", quesito no qual, em tese, garante que a conversa do remetente será enviada de forma criptografada e será descriptografada quando chegar ao destinatário (WHATSAPP, 2020b). Desse modo, somente os participantes de uma conversa poderão ter acesso às informações contidas em uma mensagem utilizando-se do aplicativo.

Desta forma, não há espaço para técnicas de captura de dados como *man-in-the-middle-attack*[3] ou grampos telefônicos, impedido em sua desenvolvedora o acesso aos dados e as conversas de seus usuários.

A criptografia "ponta-a-ponta" permite que quaisquer dados enviados entre usuários sejam criptografados com uma chave de criptografia, a qual, somente os participantes da conversa possuem. Apenas o possuidor dessa chave terá acesso as mensagens trocadas, em contrapartida, se qualquer pessoa tentar capturar esses dados sem a chave verá apenas vários símbolos e letras aleatórias sem sentido algum, como exemplificado na Figura 1.

Figura 1. Funcionamento da criptografia ponta-a-ponta.

Fonte: Elaboração dos autores, 2020.

Com base na teoria apresentada da interceptação e criptografia, percebe-se a impossibilidade de se ter acesso a conversa sem estar com um dos aparelhos participantes, o WhatsApp não disponibiliza a conversa de seus usuários ou histórico de conversas de seus usuários para a justiça, mesmo em casos de ordem judicial (como já ocorreu com o Tribunal de Justiça do Estado de São Paulo[4] e

[2] Serviço de Mensagem curta, inicialmente projetado para o serviço GSM (TOORANI; BEHESHTI, 2008).

[3] O ataque homem do meio é meio pelo qual um invasor posiciona-se entre duas pessoas interceptando sua conversa e passa-se por uma das partes (MALENKOVICH, 2013).

4 Processo com determinação judicial de quebra de sigilo de dados que em 2015, devido ao WhatsApp não ceder os dados requisitados, bloqueou o aplicativo em todo o país (TJSE, 2020).

Sergipe[5]), o aplicativo ficou limitado a fornecer somente dados simples como informações como: recados; fotos de perfil; informações de grupo; e lista de contatos, se disponível (WHATSAPP, 2020).

Ademais, a criptografia também remete a outro problema no contexto jurídico, que é a impossibilidade de se comprovar a autenticidade de uma mensagem do aplicativo, uma vez que existem técnicas que podem vir a alterar o seu conteúdo, conteúdo este que pode vir a ser usado em ação judicial ou passar a ter fé pública diante de uma possível transcrição para ata notarial.

(Im)possibilidade de verificar autenticidade de mensagem

Conforme apresentado, todas as conexões de dados do WhatsApp são criptografadas, desta forma, há impedimentos operacionais que limitam qualquer tipo de investigação ou averiguação de suspeitas, como por exemplo grampos telefônicos, para analisar se o teor de mensagens quanto a sua veracidade, uma vez que, conforme demonstrado somente o remetente e o destinatário teriam acesso a essa conversa.

Uma possibilidade de verificação de autenticidade de mensagens, que não exigem captura de dados, seria a comparação do conteúdo de mensagens entre os aparelhos dos participantes de uma conversa. No entanto, há possibilidade de que mensagens possam não estar idênticas e/ou terem sido deletadas de forma integral ou parcial dos aparelhos investigados.

Desta maneira, dentre as vertentes apresentadas, percebe-se a negativa quanto a autenticidade de provas oriundas do aplicativo WhatsApp, pois não há possiblidade técnica em suas funcionalidades quanto a comprovação de que mensagens apresentadas não foram modificadas.

Técnicas que podem alterar o teor das mensagens

Para discussão de das possíveis técnicas que podem alterar o teor de mensagens, parte-se da definição do que se trata um banco de dados. Date (2003), conceitua banco de dados como:

> *um sistema computadorizado cuja finalidade geral é armazenar informações e permitir que os usuários busquem e atualizem essas informações quando as solicitar. As informações em questão podem ser qualquer coisa que tenha um significado ao indivíduo ou à organização a que o sistema deve servir* (DATE, 2003, p.06).

O banco de dados do WhatsApp é o local onde estão armazenados todos os dados que o aplicativo possui sobre o usuário: mensagens, grupos, número de telefone, foto de perfil, chave da criptografia ponta-a-ponta, etc.

Esta técnica consiste em alterar diretamente o banco de dados do aplicativo através outros específicos, para edição de banco de dados, que podem facilmente ser encontrados em pastas do aparelho. Com conhecimento intermediário sobre o funcionamento de um sistema operacional de *smartphone*, qualquer usuário pode acessar a pasta interna onde fica instalado o aplicativo no sistema e realizar edições, manipulando seu conteúdo.

Acrescenta-se que há possibilidade de exportação do banco de dados de um aparelho para o computador, uma vez que ele é um arquivo na extensão ".db[6]", realizar edições externamente, e importar o arquivo de volta para o aparelho.

5 Processo de investigação de tráfego interestadual de drogas que bloqueou o WhatsApp em todo o país após o mesmo não cumprir determinação de quebra de sigilo (TJSP,2015).

6 Extensão de bancos de dados genéricos de aplicativos, podendo incluir textos, imagens, gráficos que ficam gravados no celular.

Como o propósito do presente artigo é demonstrar tais realidades e não ensiná-las, cabe explicar que essa pasta não é facilmente acessada dentro do aparelho, mas que através de métodos específicos, podem ser encontrados pela internet, desta forma, é possível desbloquear o acesso às pastas do sistema operacional de um do aparelho e torná-la acessível para o usuário que desejar manipular.

Deste modo, é possível realizar edições, injetando o contexto inverídico desejado, e depois desfazer o processo de desbloqueio de um sistema, camuflando quaisquer rastros que a pasta do sistema, onde os dados estão armazenados, possam ter sido editados externamente e não pelo WhatsApp.

Técnica de injeção de memória

Diferentemente da técnica de alterar o banco de dados de aplicativos, que consiste na alteração permanentemente de dados em um arquivo escrito no aparelho, a técnica de injeção de memória ou *in-memory attack* consiste em alterar dados temporários presentes na memória RAM (*Random Access Memory*) do dispositivo.

A empresa de tecnologia Dell (2020) conceitua memória RAM como um espaço temporário de informações do sistema operacional e de aplicativos em uso. Esta, comparada a um disco rígido (*HDD*) é mais rápida, porém é uma memória volátil, desta forma entende-se que o processador terá rápido acesso a quaisquer dados escritos nela, no entanto, assim que faltar energia elétrica ou o dispositivo for desligado, todos os dados armazenados serão apagados (BONIATI; PREUSS; FRANCISCATTO, 2014).

Nesta memória ficam armazenados temporariamente todos os dados processados pelo processador, seja a resposta de um cálculo matemático, uma imagem que está sendo visualizada, seja as mensagens de uma conversa que o WhatsApp acabou de acessar no seu banco de dados para exibir ao usuário.

A técnica de injeção de memória consiste em alterar esses dados já processados e manipulá-los para que o dispositivo exiba o conteúdo desejado. Desta forma, o conteúdo demonstrado na tela do dispositivo não é o que realmente consta no banco de dados da aplicação, mas sim o que foi alterado na memória do aparelho. Este conteúdo alterado poderá ser exibido ao usuário que fez a modificação ou, possivelmente, um tabelião transcrevendo uma ata notarial.

Há-se o risco de que as mensagens do aplicativo tenham sido modificadas antes de serem entregues ao tabelião, que poderá não percerber qualquer alteração, uma vez que este terá acesso ao aplicativo funcional, no entanto seu conteúdo já terá sofrido modificação.

Essa técnica de alteração de dados em específico não é indetectável, mas tem usualmente enseja-se conhecimento técnico dos meios para sua descoberta. Desta forma, um tabelião ou preposto sem conhecimento técnico na área da informática poderá encontrar dificuldade em identificar uma alteração, mesmo que se por ventura, este, minimizasse o aplicativo e explorasse o que há dentro do *smartphone* do manipulador.

Técnica de inspeção de elemento no navegador

Valendo-se de ferramentas para desenvolvedores que está presente em quase todos os navegadores de internet (*browsers*), é possível alterar o teor de mensagens presentes em um *site* utilizando a ferramenta inspeção de elemento.

A técnica de inspeção de elemento no navegador consiste em alterar o conteúdo das mensagens não diretamente pelo aplicativo, mas pelo

navegador, especificamente pelo *site* do WhatsApp, no qual exibe todas as conversas do aparelho.

Com pouco conhecimento em informática é possível modificar o teor de qualquer conversa no aplicativo, inclusive, trocar o conteúdo de imagens e áudios por outros, e modificar textos, a foto de perfil da pessoa com quem se conversa, os horários das mensagens, entre outros. Esta técnica não se limita a edição de mensagens, pois também há a possibilidade de criar toda uma conversa do zero.

No exemplo abaixo, totalmente fictício, é demonstrado um caso no qual uma mensagem comum se torna uma falsa ameaça que poderia pôr fim ser transcrita em ata notarial:

Figura 2. Exemplo de mensagem manipulada.

Fonte: Elaboração dos autores, 2020.

Esta técnica se comparada as demais, é menos complexa em termos de execução, contudo, também poderá ser questionada e/ou verificar se há manipulação, necessita-se apenas que seja atualizada a página do navegador (*refresh*). Ao fazer isso, todas as modificações do navegador serão removidas e o conteúdo original será restaurado.

Técnica "responder" (*reply*)

A técnica "*reply*" (responder) no WhatsApp é uma técnica que apresenta características de fácil entendimento. Comumente, quando deleta-se alguma conversa ou reinstala-se o aplicativo de tal forma que todas as mensagens são perdidas, há a possibilidade do usuário se deparar com algum parceiro de conversa respondendo a uma mensagem que existiu anteriormente no aplicativo, mas que mesmo assim não existe mais no aparelho.

A função *reply* do WhatsApp tem como função citar uma mensagem enviada previamente por um dos participantes de uma conversa. Contudo, o aplicativo não faz verificação que constate se de fato a mensagem é verídica ou houve modificação do seu teor. Essas mensagens podem ser modificadas de conforme será explicado abaixo.

O *site Check Point Research*, no ano de 2018, constatou falhas de segurança neste sistema, por exemplo, a possibilidade de troca do conteúdo de uma mensagem por outra. Uma mensagem que esteja escrita "Legal" enviada por membro de um grupo poderia ser alterada por "Eu estou morrendo, estou no hospital agora!" (BARDA; ZAIKIN; VANUNU, 2018).

Figura 2. Exemplo de mensagem manipulada.

Fonte: Check Point Research, 2018.

Para que os integrantes de um grupo possam ver as mensagens alteradas, aquele que manipulou necessita responder à mensagem que ele próprio modificou, citando e alterando a mensagem "Legal" para que seja enviada a todos do grupo (BARDA; ZAIKIN; VANUNU, 2018).

Diante das técnicas supracitadas, esta é a única que consegue fornecer a mensagem falsa (ou as mensagens) para o aparelho de outras pessoas do *chat*, porém, a deturpação de seu conteúdo depende daqueles que leem o conteúdo postado.

Se por acaso um participante do grupo não acompanha frequentemente os conteúdos que circulam neste, poderá ler a mensagem alterada, e acreditar que seu conteúdo é verídico, contudo, este método poderá ser identificado por um participante que acompanhe diálogos de forma simultânea às postagens, pois identificará assim que a mesma for editada e divergir da que foi enviada de início.

Ademais, aquele participante que possui todas as mensagens do grupo ainda registradas em seu *smartphone*, pois ao acessar a mensagem alterada logo verificará que a citação é alterada pois a função "responder", que deveria encaminhá-lo à mensagem citada ao toque, não funcionará pois a mensagem citada nunca existiu.

O mesmo vale para uma conversa privada, é possível constatar que a mensagem citada de fato foi alterada, caso o aparelho oposto ao do fraudador ainda possuir todas as mensagens, porém, não há como precisar quais mensagens foram editadas e qual o autor das manipulações, uma vez que o aplicativo está vulnerável aos mais diversos ataques externos, podendo mesmo ambos participantes de um *chat* alterar o diálogo original.

A problemática surge quando essas mensagens passam a ser analisadas por terceiro que atesta essas mensagens como prova judicial. Este não terá como verificar a integridade das mensagens tampouco saber o que se passou pelo *chat* e poderá transcrevendo uma falsa verdade demonstrada no aplicativo.

WhatsApp como meio de prova no judiciário

A Lei n° 13.105 de 16 de março de 2015, que estabelece o atual Código de Processo Civil, preocupou-se com a possibilidade de uma prova ser produzida eletronicamente. Para tal, faz-se necessário o uso de ata notarial para transcrição do conteúdo do aparelho eletrônico.

Na visão de Lenza (2016), a prova é destinada a convencer o juiz a respeito dos fatos controvertidos. É possível também, que a mesma seja obtida através de perícia técnica, porém, neste caso, faz-se necessário prévia autorização judicial para constatação dos fatos.

Ata notarial

Para que mensagens do WhatsApp tenham fé pública e não serem tratadas como um ato unilateral, há a possibilidade que estas provas sejam contestadas e/ou alegadas como inverídicas, por não haver forma certa de se confirmar sua integridade, há portanto, a necessidade que as mesmas sejam transcritas em ata notarial por tabelião (MUNARO, 2019).

As atas notariais podem ser descrevidas como laudos, feitos pelo tabelião que se locomove até a casa da pessoa ou local do fato, e descreve tudo que presencia, sem emitir juízo de valor. O Colégio Notarial do Brasil, Seção São Paulo (CNBSP) traz a definição sobre o que é ata notarial:

> *Ata notarial é um instrumento público no qual o tabelião documenta, de forma imparcial, um fato, uma situação ou uma circunstância presenciada por ele, perpetuando-os no tempo. A ata notarial tem eficácia probatória, presumindo-se verdadeiros os fatos nela contidos. É um importante meio de prova na esfera judicial, conforme disposto no artigo 384 do Código de Processo Civil (Lei*

> *13.105/2015). A ata notarial pode ser utilizada, por exemplo, para comprovar a existência e o conteúdo de sites na internet, conversas de Whatsapp, realização de assembleias de pessoas jurídicas, o estado de imóveis na entrega de chaves ou atestar a presença de uma pessoa em determinado lugar ou a ocorrência de qualquer fato. O interessado poderá solicitar a lavratura da ata notarial, bem como a realização de diligências dentro da circunscrição a qual pertence o cartório, para certificação de qualquer fato* (CNBSP, 2020, n.p.).

Para que o tabelião possa redigir a ata é necessário que ele tenha conhecimento do fato. Por isso, será necessário que ele o verifique, o acompanhe ou o presencie (LENZA, 2016).

No caso de transcrição de uma conversa que possa ter sido modificada, não haverá motivos para que o tabelião deixe de transcrevê-la, uma vez que não haverá nenhum tipo de perícia para verificar qualquer anomalia e mesmo havendo, não seria possível de fato a comprovação que o aparelho não sofreu modificações, uma vez que nem toda modificação no aplicativo é detectável.

Deste modo, toda conversa que for transcrita por tabelião em ata notarial poderá estar livre de valoração pessoal, assim como se determina em lei, mas poderá estar carregada de informações que poderão beneficiar o manipulador da conversa. Toda a conversa do WhatsApp e o juízo de valor do manipulador passarão a ser uma prova inequívoca, sem possibilidade de contestação (MUNARO, 2019).

Mandado de busca e apreensão e perícia

É possível que mensagens originadas de aparelhos *smartphones* adquiridas por mandado de busca e apreensão, também tenham seu conteúdo manipulado e também venham a demonstrar fatos inverídicos em um processo judicial.

Segundo o art. 357, § 8º, da Lei n° 13.105 de 16 de março de 2015, se o caso concreto comportar realização de prova pericial, o magistrado, em sua decisão de saneamento e de ordenação do processo, nomeará o perito com *expertise*[7] relacionada ao objeto da perícia e fixará, desde logo, prazo para entrega do laudo (BRASIL, 2015).

No entanto, mesmo através desses métodos que se tem maior facilidade de detectar o dolo prévio em modificar as mensagens antes do flagrante, o uso de provas provindas do aplicativo devem ser reconsideradas, pois há o risco de que mensagens advindas do WhatsApp possam ser forjadas previamente para ocultar infrações e infratores e prejudicar pessoas inocentes.

Conforme as técnicas de manipulação demonstradas, esse tipo de prova também está sujeita a manipulação do conteúdo de mensagens, uma vez que alguma técnica de manipulação pode ter sido empregada em aparelho antes da apreensão, podendo o manipulador dos dados valer-se desses recursos para alterar o desfecho não só de investigações, bem como de todo um processo judicial.

Ademais, quando se tratar de uma perícia, com um profissional qualificado para analisar o conteúdo do aparelho, há redução do risco se comparado a um tabelião ou outra pessoa que venha fazer destas mensagens prova judicial, contudo, como existem diversos métodos para modificação do aplicativo, alguns deles praticamente impossíveis a identificação, como a técnica de alteração do banco de dados do

[7] Do francês expertise. Significa experiência, especialização ou perícia (DICIO, 2020).

aplicativo demonstrada anteriormente, se faz questionável o uso do aplicativo como meio de prova.

Conclusão

O objetivo desta pesquisa foi demonstrar o funcionamento do aplicativo WhatsApp como meio de prova no judiciário e o porquê do seu uso como meio de prova pode ser questionado.

Fora exposto a tecnologia de segurança ponta-a-ponta e demonstrado como esta funciona, demostrou-se que não é possível confirmar a autenticidade de mensagens deste aplicativo uma vez que estas são criptografadas (não permitindo verificação por terceiro) e pelo fato de somente os aparelhos envolvidos na conversa tem acesso às mensagens trocadas. No caso de uma possível adulteração do conteúdo de uma conversa, não seria possível, em alguns casos, diferenciar o fato verídico da imitação, apenas por meio da comparação os aparelhos *smartphone* e verificar possíveis divergências.

Também foram expostos meios que tornam possíveis essas modificações, destacou-se que o aplicativo não tem como garantia a autenticidade de mensagens, que são exibidas dentro do aparelho eletrônico ao qual pertencem, e que é possível realizar a manipulação não só pelo próprio *smartphone*, mas também por meio de computador.

Além disso, apresentou-se a possibilidade de que diálogos alterados em atas notariais, possam torna-los aceitos pelo poder judiciário como prova, com fé pública e fomentá-las a serem inquestionáveis e aceitas pelo magistrado em seu julgamento.

Como sugestões de temas para novas pesquisas, identifica-se a necessidade de se pesquisa sobre a possibilidade ou o que poderia ocorrer se a justiça reconhecesse que provas originadas do WhatsApp de fato não são confiáveis e desconsiderasse todas as provas já obtidas por este meio, bem como a possibilidade de anulação de sentenças nas quais este meio de prova tiveram predominante influência na decisão do magistrado.

Outrossim, pode ser realizado estudo sobre a alegação de que uma mensagem de WhatsApp não tenha sido digitada pelo dono do aparelho em que o aplicativo está instalado, mas sim por terceiro com acesso a este, e seu valor como prova.

Como última sugestão, há também a possibilidade estudos mais aprofundados sobre a relevância material que a prova judicial extraída do teor de uma mensagem enviada por pessoa que alega não estar em condições perfeitamente racionais, como a título de exemplo alcoolizada.

Por fim, chegou-se ao entendimento que independente da forma que uma conversa for extraída para acusar-se como prova judicial, seja voluntariamente pelo possível manipulador dos dados ou por aparelho de suspeito em que uma perícia é realizada, não é possível assegurar a veracidade de um conteúdo exibido em aparelho celular, tornando assim o WhatsApp como um meio não confiável de provação de veracidade de fato, comprovando a hipótese levantada e testada pelo presente trabalho.

Todos os autores declararam não haver qualquer potencial conflito de interesses referente a este artigo.

Referências

BONIATI, B. B.; PREUSS, E; FRANCISCATTO, R. **Introdução à Informática.** Frederico Westphalen. RS: Rede e-Tec Brasil, 2014.

BARDA D.; ZAIKIN, R.; VANUNU O. FakesApp: A Vulnerability in WhatsApp. **Check Point Research**. 07 de ago. de 2018. Disponível em: https://research.checkpoint.com/2018/fakesapp-a-

vulnerability-in-whatsapp/. Acesso em: 11 de jun. 2020.

BRASIL, **Lei n° 13.105 de 16 de março de 2015**. Código de Processo Civil. Brasília: Diário Oficial da União [2015]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm. Acesso em: 30 de set. 2020.

COLÉGIO NOTARIAL DO BRASIL (CNBSP). **Atas Notariais**. São Paulo. Disponível em: https://www.cnbsp.org.br/index.php?pG=X19wYWdpbmFz&idPagina=6002. Acesso em: 01 de jun. 2020.

DATE, C. J. **Introdução a sistemas de bancos de dados**. 8. ed. Rio de Janeiro: Elsevier, 2003.

DELL INC. **Dell**, 2020. **O que é memória RAM e qual é a sua função**. Disponível em: https://www.dell.com/pt-br/shop/o-que-e-memoria-ram/ab/o-que-e-memoria-ram. Acesso em: 12 de jun. 2020.

DICIO. Dicionário Online de Português. **Significado de Expertise**. Disponível em: https://www.dicio.com.br/expertise/. Acesso em: 14 de jun. 2020.

FRANK L. J.; WRIGHT L. M. **Enhancing data in a screenshot**, US9245182B2. Publication 26 de jan. 2016 [online]. Disponível em: https://patents.google.com/patent/US9245182B2/en Acesso em: 30 de set. 2020.

GONÇALVES, Marcus Vinicius Rios. Coordenador, LENZA Pedro, **Direito Processual Civil Esquematizado**, ed. 6ª, São Paulo: Saraiva, 2016

MALENKOVICH, S. **O que é um Ataque Man-in-the-Middle?** Kaspersky daily. Disponível em: https://www.kaspersky.com.br/blog/what-is-a-man-in-the-middle-attack/462/ Acesso em: 30 de set. 2020.

MUNARO, T. **Whatsapp - É possível utilizá-lo como prova?** 2019. (02min50s). Disponível em https://youtu.be/wMmv3RQ0I0g. Acesso em: 01 de jun. de 2020.

PAIVA, Fernando. Mensageria no Brasil - Fevereiro de 2020. **Panorama**, mar. de 2020. Disponível em: https://panoramamobiletime.com.br/pesquisa-mensageria-no-brasil-fevereiro-de-2020/. Acesso em: 14 de jun. 2020.

SIGNIFICADOS. **Significado de Bode expiatório**. Disponível em: https://www.significados.com.br/bode-expiatorio/. Acesso em: 14 de jun. 2020.

STJ. **Recurso em Habeas Corpus: Nº 89.981 – MG**. Relator: Ministro Reynaldo Soares da Fonseca. DJ: 05/12/2017. Disponível em: https://stj.jusbrasil.com.br/jurisprudencia/505880324/recurso-em-habeas-corpus-rhc-89981-mg-2017-0250966-3/decisao-monocratica-505880334. Acesso em: 30 de set. 2020.

REUTERS. G1, 2014, **Facebook finaliza aquisição do Whatsapp por US$ 22 bilhões**. 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: 10 de jun. 2020.

TOORANI, M.; BEHESHTI, **A secure SMS messaging protocol for the m-payment systems. In Proceedings of the 2008** IEEE Symposium on Computers and Communications, Marrakech, Morocco, 6–9 Jul. 2008.

TJSE, **Processo n° 0007674-14.2015.8.25.0040** do Autor: A.P.; Réu: D.J.D. Tribunal de Justiça do Estado de Sergipe. Data:10/09/2020. Disponível em: https://www.jusbrasil.com.br/processos/101126628/processo-n-201655000183-do-tjse Acesso em: 30 de set. 2020.

TJSP, **Processo n° 0017520-08.2015.8.26.0564** do. Autor: Réu: R.R.H. Tribunal de Justiça do Estado de São Paulo. Data: 02/07/2015. Disponível em: https://esaj.tjsp.jus.br/cpopg/show.do?processo.codigo=FO0003J750000&processo.foro=564&processo.numero=0017520-08.2015.8.26.0564&uuidCaptcha=sajcaptcha_752904606c824f409f16171f3c70aa56 Acesso em: 30 de set. 2020.

WHATSAPP INC. WhatsApp, 2020a. **Sobre o WhatsApp**. Disponível em: https://www.whatsapp.com/about/?lang=pt_br. Acesso em: 10 de jun.2020

WHATSAPP INC. WhatsApp, 2020b. **Criptografia de ponta a ponta**. Disponível em: https://faq.whatsapp.com/general/security-and-privacy/end-to-end-encryption. Acesso em: 10 de jun. 2020.