ILICITUDE DAS PROVAS PROVENIENTES DO WHATSAPP[1]

UNLAWFULNESS EVIDENCE ORIGINATING FROM WHATSAPP

Júlia Salomão ARRUDA[2]

Márcio de Freitas CUNHA[3]

RESUMO
Foi explicitado o uso do aplicativo de mensagens WhatsApp como meio de prova, as situações em que poderia ser considerada ilícita, através da análise de correntes doutrinárias e princípios. A pesquisa destaca a necessidade de evitar a onerosidade e morosidade no processo penal. Considera o uso de *backdoor* e metadados para permitir acesso a informações sobre os dados criptografados, sem despender tempo em descodificá-los. Pondera a possibilidade da autoridade policial mediante situação de prisão em flagrante, acessar os dados do WhatsApp, sem necessariamente requisitar mandado de busca e apreensão.
Palavras-chave: WhatsApp. Provas ilícitas. Criptografia. Teoria da árvore dos frutos envenenados. Princípio da proporcionalidade. Princípio da serendipidade. Internet. Aplicativo.

ABSTRACT
Were explicit, the use of the message app WhatsApp as means of prove, in situations that could be considered illicit, through analysis of doctrinal current and principles. The research contrasts the necessity of avoid the onerous and slowness in the penal process. Perform the use of backdoor and metadata to allow access to the information about encrypted data, without spend time decoding them. Consider the possibility of the police authority upon prison situation in the act, will be able to access the WhatsApp data, without necessarily requesting search warrant and apprehension.
Keywords: *WhatsApp. Illicit prove. Encrypted. Fruit of poisonous tree. Principle of proportionality. Principle of serendipity. Internet. Privacy law.*

---

[1] O presente artigo sintetiza a monografia de conclusão da pesquisa, realizada para o Programa Interno de Bolsas de Iniciação Científica (PIBIC 2020-2021) da Faculdade de Direito de Franca (FDF), Franca/SP.

[2] Discente da Faculdade de Direito de Franca (FDF), Franca/SP. Bolsista do Programa Interno de Bolsas de Iniciação Científica (PIBIC 2020-2021).

[3] Graduado em Direito pela FDF (2000), Especialista em Direito Penal pela UNIFRAN - 2010 e mestre em Direito pela UNAERP - 2013.

1 INTRODUÇÃO

A pesquisa tem como principal enfoque o aplicativo de mensagem WhatsApp, contudo, por analogia, abrange outros aplicativos de mensagens e redes sociais que possibilitam troca de mensagens. Os aplicativos de mensagens em 2019, segundo o relatório da consultoria americana eMarketer *Global Messaging Apps 2019*,[4] responsável por analisar o setor de aplicativos de mensagens no mundo, atingiram, em nível global, a impressionante quantia de 2.52 bilhões de usuários de aplicativos de mensagens em geral.

A essência dos dados presentes nesta pesquisa, objetiva unicamente demonstrar de maneira explícita a importância do WhatsApp, pois trata-se de um dos aplicativos mais populares do Brasil, além de ser conhecido e usado de modo amplo por outros países. O Brasil se encontrava no ano de 2019, um ano antes da pandemia, com 120 milhões de usuários ativos mensalmente.

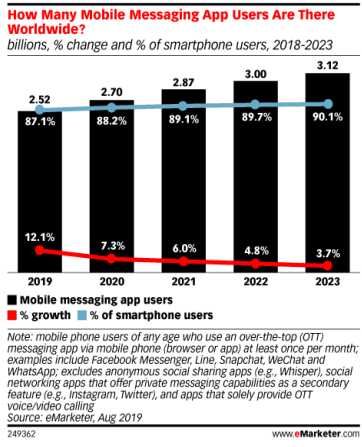
Professores e estudantes do Núcleo de Marketing e Consumer Insights (NUMA), da Escola Superior de Propaganda e Marketing (ESPM), realizaram uma pesquisa para compreensão e análise do impacto dos usos do aplicativo no período da pandemia da Covid-19.[5] A pesquisa contou com a participação de uma amostra de 387 usuários de diferentes redes sociais e o WhatsApp foi apontado como aplicativo mais usado, o qual 97% dos entrevistados afirmaram usar com frequência, na excepcional situação de isolamento social.[6]

---

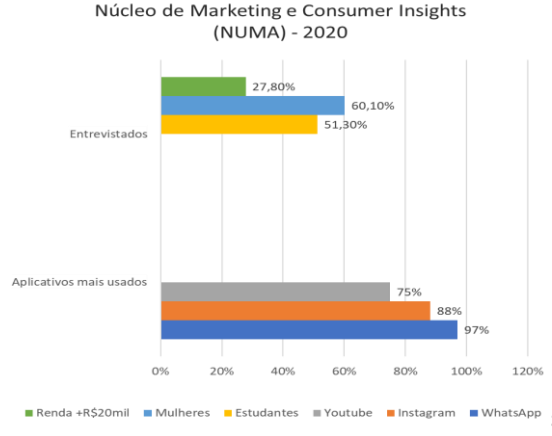
[4] ENBERG, Jasmine. Global Messaging Apps 2019. Insider Intelligence. Disponível em: <https://www.emarketer.com/content/global-messaging-apps-2019>. Acesso em: 17 Nov. 2020.

[5] HADDAD, H.. WhatsApp é o aplicativo mais usado na pandemia - Estudo ESPM. 2020.

[6] Com a pandemia houve uma tentativa generalizada de estabelecer vínculos de maneira virtual, com o propósito de evitar o contágio e simultaneamente manter interação maior entre os indivíduos. As videochamadas, apesar de serem uma opção que atende a todos os objetivos, faz-se necessário que as pessoas estejam disponíveis naquele período, em local mais reservado. Entretanto, as mensagens além de atender aos objetivos de interação, podem ser visualizadas em qualquer local e em qualquer momento, não exige disponibilidade de tempo simultânea entre as partes durante a conversa.



7



8

O WhatsApp é um aplicativo com a função originária de ser um meio de comunicação alternativo ao sistema de SMS. Contudo, mediante atualizações do sistema, passou a disponibilizar opções de envio e recebimento de variados arquivos. Atualmente, são compostos por textos, áudios, fotos, vídeos, documentos, localização, contatos e "figurinhas", além de videochamadas e ligações simples.[9]

[7] ENBERG, Jasmine. Global Messaging Apps 2019. Insider Intelligence. Disponível em: <https://www.emarketer.com/content/global-messaging-apps-2019>

[8] HADDAD, H.. WhatsApp é o aplicativo mais usado na pandemia - Estudo ESPM. 2020.

[9] Sobre o WhatsApp. WhatsApp.com. Disponível em: <https://www.whatsapp.com/about/?lang=pt_br>.

O sistema que gera segurança e privacidade em conversas entre os usuários no WhatsApp Messenger é a criptografia de ponta a ponta, responsável por dificultar drasticamente a possibilidade de visualizações realizadas por terceiros ou qualquer tipo de invasão do sistema.[10] Isso ocorre pelo fato de garantir ao receptor e destinatário ou destinatários - se forem enviadas em grupos com mais de duas pessoas - o acesso restrito ao conteúdo das mensagens, áudios, fotos, vídeos, atualizações de status, documentos, chamadas, dentre outros anexos enviados. Esses materiais não poderão nem mesmo ser acessados pelo próprio servidor do WhatsApp.

No Brasil, ao ser implantada a criptografia de ponta a ponta, essa tecnologia deu origem a expressivas ocorrências de bloqueios do aplicativo de mensagens WhatsApp, em toda extensão do território nacional. Os bloqueios foram aplicados para repreender a atitude omissa durante investigações criminais, de não revelar o conteúdo de mensagens, punindo o desauxílio prestado pelos donos do aplicativo. Os responsáveis pelo tema alegam não serem mais detentores de informações referentes ao conteúdo das mensagens de seus usuários, pois não possuiriam uma chave especial de acesso, responsável por descodificar as mensagens, de modo a torná-las passíveis de leitura e possíveis provas para anexo no processo judicial.

Desse modo, permite que tais informações não sejam fornecidas pelo WhatsApp, ou seja, as autoridades policiais, mesmo que detenham um mandado judicial não poderão obter as informações da própria empresa. Além disso, o WhatsApp descumpriu variadas determinações judiciais, as quais requisitaram revelações do conteúdo das mensagens, que eram negados, de modo a ofender à Lei nº 12.965/2014 (Marco Civil da Internet)

Na busca por medidas mais efetivas, foi considerado estipular às empresas a obrigatoriedade em criar uma "*backdoor*", como meio para acessar o conteúdo das plataformas e dispositivos criptografados, durante investigações criminais. Contudo, líderes setoriais alertam que qualquer sistema que apresente o "backdoor" iria comprometer a totalidade da privacidade. No ano de 2020, nos Estados Unidos da América, os Senadores Republicanos apresentaram um projeto de lei que objetivava

[10] Central de ajuda do WhatsApp - Sobre a criptografia de ponta a ponta. WhatsApp.com. Disponível em: <https://faq.whatsapp.com/general/security-and-privacy/end-to-end-encryption/?lang=pt_br>.

enfraquecer a legitimidade em utilizar criptografia.[11] Assim com a presença de um mandato, ficaria disponível o acesso dos oficiais da lei a dispositivos e serviços de comunicação.

Nesse sentido, em uma entrevista, os pesquisadores responsáveis pela área de criptografia, Riana Pfefferkorn e Tobias Boelter, coadunam com a dificuldade de quebrar a criptografia, mas afirmaram que desabilitar ou proibir o processo de criptografia não resultaria em uma solução para seus problemas. Sugeriram uma atitude alternativa por parte das autoridades policiais, com enfoque em uma investigação pautada pelo uso de metadados[12].

A lei brasileira do Marco Civil da Internet no artigo 5º incisos VI e VIII aborda justamente o registro de metadados como uma alternativa para responsabilização de usuários e investigação policial. No artigo 13 da mesma lei é esclarecido quem é o responsável por armazenar os registros de conexão, além de estipular o período de armazenamento desses dados; os parágrafos 2º e 3º são destinados a disponibilizar à autoridade policial, administrativa ou ao Ministério Público a possibilidade de estender o prazo previsto em lei, objetivando através de autorização judicial ter acesso aos metadados.

> Art. 5º Para os efeitos desta Lei, considera-se:
> VI - registro de conexão: o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados;
> VIII - registros de acesso a aplicações de internet: o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP.[...]
> Art. 13. Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento.

[11] S.4051 - 116th Congress (2019-2020): Lawful Access to Encrypted Data Act. Congress.gov. Disponível em: <https://www.congress.gov/bill/116th-congress/senate-bill/4051/>.

[12] Os metadados são dados que descrevem outros dados, os quais contém explicações que visam informar e revelar outros dados acessados. Os metadados permitem traçar a localização de documentos específicos, através de esclarecimentos sobre o conteúdo das páginas e das palavras-chave relacionadas com as pesquisas acessadas.

> § 1º A responsabilidade pela manutenção dos registros de conexão não poderá ser transferida a terceiros.
> § 2º A autoridade policial ou administrativa ou o Ministério Público poderá requerer cautelarmente que os registros de conexão sejam guardados por prazo superior ao previsto no **caput.**
> § 3º Na hipótese do § 2º, a autoridade requerente terá o prazo de 60 (sessenta) dias, contados a partir do requerimento, para ingressar com o pedido de autorização judicial de acesso aos registros previstos no **caput.**[13]

Consequentemente, após a legislação acima indicada, os bloqueios judiciais entraram em desuso para solucionar as desavenças criadas entre as determinações judiciais e o aplicativo de mensagens. Não apenas o Marco Civil, mas movimentos jurídicos iniciados internamente no judiciário têm impulsionado a utilização de ferramentas digitais, como é o caso da demonstração da viabilidade da intimação mediante o uso do Whatsapp pelo juiz Gabriel Consigliero Lessa. A tecnologia é voltada às partes, aos membros do Ministério Público, às autoridades policiais e aos integrantes de outros órgãos públicos, após solicitação expressa.[14]

O uso da tecnologia responsável por fornecer agilidade e desburocratizar procedimentos judiciais, fez-se facultativa, assim as partes que detiverem interesse, podem, voluntariamente, aderir aos termos. Além disso, faz-se necessária uma confirmação do recebimento da mensagem durante o dia em que fosse enviada, se a confirmação não fosse enviada, a intimação da parte decorreria de modo convencional. Exceção se dá nos processos que tramitam em segredo de justiça, os quais necessitam de intimação convencional.[15]

2 ILICITUDE DE PROVA

[13] BRASIL, L12965. Planalto.gov.br. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>.

[14] CNJ - PCA - Procedimento de Controle Administrativo, Portaria Conjunta n. 01/2015, Relatora Daldice Santana, Plenário Virtual, 23 de junho de 2017.

[15] FLÁVIA TEIXEIRA ORTEGA. Afinal, é possível o uso do WhatsApp para intimações judiciais? Jusbrasil. Disponível em: <https://draflaviaortega.jusbrasil.com.br/noticias/473474379/afinal-e-possivel-o-uso-do-whatsapp-para-intimacoes-judiciais>.

A admissibilidade processual da prova ilícita é defendida por uma minoria[16]. Essa corrente acredita na permissibilidade do uso de provas ilícitas no processo, se não fosse proibida pelo ordenamento processual. Contudo, outro processo seria realizado para apurar possíveis violações da norma do direito material causadas pelo obtentor da prova ilícita[17].

Já a inadmissibilidade absoluta é uma corrente fundada na interpretação literal do art. 5º, LVI, da Constituição Federal. Nessa corrente, defende-se que a obtenção de provas de cunho ilícito é uma clara violação dos direitos constitucionais. Porém, o uso do termo absoluto resulta em amplas críticas, pois até mesmo o direito constitucional nega qualquer caráter absoluto de interpretação das normas, sendo aceitas análises que divergem da gramatical ou literal.

Outra corrente admite prova ilícita em algumas circunstâncias, aplicando o princípio da proporcionalidade ou razoabilidade, no qual o interesse público deve ser protegido e preservado independentemente da origem das provas que o garante[18]. Esses são casos excepcionais ou graves. Uma crítica vinculada a essa teoria é a amplitude do conceito de proporcionalidade, constantemente sujeita à mutação, sendo um conceito jurídico indeterminado.

O Princípio da Contaminação, também conhecido como a Teoria da Árvore dos Frutos Envenenados, é aplicado para avaliar a admissibilidade das provas usadas no processo, ponderando se serão consideradas ilícitas ou não. As provas devem sofrer minuciosa verificação com o objetivo de averiguar eventual contaminação que possa ter produzido nas demais provas do processo. O artigo 573, § 1º do CPP, deixa claro que ao ser declarado a nulidade de um ato, causará nulidade aos atos que sejam diretamente dependentes do ato nulo.

Ademais a Lei nº 11.690/2008, art. 157 §1º, aborda especificadamente a inadmissibilidade de provas originárias das ilícitas. Já nos §2º e §3º são abordados o conceito de independência entre as provas e a inutilização das provas contaminadas por decisão judicial, respectivamente, os quais afirmam que:

---

[16] LOPES JÚNIOR, Aury. Direito processual penal. 16. ed.São Paulo: Saraiva, 2019 CAP. VIII.

[17] LOPES JÚNIOR, Aury. Direito processual penal. 16. ed. São Paulo: Saraiva, 2019

[18] LOPES JÚNIOR, Aury. Direito processual penal. 16. ed.São Paulo: Saraiva, 2019 CAP. VIII.

> Art. 157. (...) § 1º São também inadmissíveis as provas derivadas das ilícitas, salvo quando não evidenciado o nexo de causalidade entre umas e outras, ou quando as derivadas puderem ser obtidas por uma fonte independente das primeiras.
> § 2º Considera-se fonte independente aquela que por si só, seguindo os trâmites típicos e de praxe, próprios da investigação ou instrução criminal, seria capaz de conduzir ao fato objeto da prova.
> § 3º Preclusa a decisão de desentranhamento da prova declarada inadmissível, esta será inutilizada por decisão judicial, facultado às partes acompanhar o incidente.[19]

Atualmente, a teoria da contaminação é atenuada, diminuída, tornando-se quase ineficaz por conta da aplicação da teoria da fonte independente e suas variações[20]. Essas teorias atacam o nexo causal, já que consideram o fato de a prova ilícita ter chances de não ser, em grau algum, determinante para a manifestação da prova derivada, ou considera que possa derivar de fonte própria e, dessa forma, não ficar contaminada, possibilitando sua produção em juízo.

Já o Princípio da Serendipidade, a nomenclatura tem origem do inglês *Serendipity*. A palavra é considerada de árdua tradução, mas significa o "ato ou capacidade de descobrir coisas boas por mero acaso, sem previsão". A palavra também se tornou conhecida pelo uso na Sociologia, ao ser analisada pelo sociólogo Robert King Merton.

Essas descobertas de relevante importância, apesar de inicialmente não terem sido procuradas, exigem atenção a indícios que com a devida interpretação, podem resultar em um novo fato.[21]

O significado jurídico de Serendipidade segundo Charles M. Wynn e Arthur W. Wiggins[22] é que em alguns momentos, por acaso, podem ser encontradas evidências que não eram inicialmente visadas,

---

[19] BRASIL. L11690. Planalto.gov.br. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/lei/l11690.htm>.

[20] LOPES JÚNIOR, Aury. Direito processual penal. 16. ed.São Paulo: Saraiva, 2019 p 485 A teoria das fontes independentes desconsidera a conectividade entre as provas consideradas ilícitas e as demais provas que compõe o processo. Uma de suas variações é a teoria do encontro inevitável, apesar de considerar a existência do nexo com a prova ilícita, será prova lícita por ter sido produzida conforme a lei.

[21] ISADORA, Lorena. O princípio da serendipidade no direito processual penal brasileiro. Frutal/MG: Prospectiva, 2016.

[22] WYNN, Charles M., WIGGINS, Arthur W. As Cinco Maiores Idéias da Ciência. Tradução de Roger Maioli. São Paulo: Ediouro, 2002. p.172.

mas que podem originar descobertas valiosas como novas provas ou pessoas envolvidas no caso. Assim, Luís Flávio Gomes[23], aplica a Serendipidade na ocorrência das escutas telefônicas:

> Mas no curso da captação da comunicação telefônica ou telemática podem surgir outros fatos penalmente relevantes, distintos da "situação objeto da investigação". Esses fatos podem envolver o investigado ou outras pessoas. De outro lado, podem aparecer outros envolvidos, com o mesmo fato investigado ou com outros fatos, diferentes do que motivou a decretação da interceptação. É nisso que reside o fenômeno da serendipidade, que significa procurar algo e encontrar coisa distinta (buscar uma coisa e descobrir outra, estar em busca de um fato ou uma pessoa e descobrir outro ou outra por acaso).[24]

O Princípio auxilia a validar as novas provas que podem ser essenciais no processo investigatório. O surgimento dessas provas é propício a ocorrer durante medidas cautelares, como a busca e apreensão e a interceptação telefônica. Essas medidas são praticadas com a presença de um mandado que descreve e limita as atitudes usadas para a obtenção das provas visadas. Contudo, durante o cumprimento do mandado expedido, pode ocorrer de uma prova inesperada, sem a devida descrição, ser encontrada. A polêmica se dá na consideração ou não da prova como algo ilícito.

Logo, a sagacidade dos infratores em ocultar e simular provas, sem a aplicação do Princípio da Serendipidade, poderia resultar em benefícios aos criminosos, ao tornar as novas provas absolutamente nulas. A validação dessas provas beneficia a investigação e auxilia na aplicação da justiça.

O Princípio da Serendipidade é o oposto da Teoria da árvore dos frutos envenenados, já que o primeiro visa legalizar provas obtidas ao acaso que possam resultar em expressivo auxílio à investigação realizada pela autoridade policial. Já a Teoria da árvore dos frutos envenenados

[23] GOMES, Luiz Flávio; CUNHA, Rogério Sanches. Legislação Criminal Especial. Coleção Ciências Criminais. Vol. 6. São Paulo: Editora Revista dos Tribunais, 2009. p.474.

[24] GOMES, Luiz Flávio; CUNHA, Rogério Sanches. Legislação Criminal Especial. Coleção Ciências Criminais. Vol. 6. São Paulo: Editora Revista dos Tribunais, 2009. p.474.

frisa a ilicitude de provas originadas de prova ilícitas, devendo estar a prova desconexa para ser considerada lícita.

Logo a Lei nº 12.965/14, conhecida como a Lei do Marco Civil da Internet, foi promulgada no dia 22 de abril de 2014, com o objetivo de disciplinar o uso da internet no Brasil, impondo limites a seus usuários. De modo a evidenciar com maior precisão a conduta tanto dos usuários, quanto das empresas que integram a Rede Mundial de Computadores; o objetivo primordial é pautado na privacidade, segurança e neutralidade durante o uso da Internet, assim garantindo que os direitos individuais assegurados pela Constituição Federal de 1988 sejam cumpridos.

O principal enfoque da Lei nº 12.965/14 é garantir a defesa dos consumidores, usuários da internet, os quais usam a rede para adquirirem produtos e serviços; regular as empresas que usam a internet como meio comercial, assegurando a livre iniciativa e a livre concorrência; impõe normas sobre os serviços prestados pelos fornecedores de internet, estes que devem garantir a segurança e a funcionalidade da rede disponível para os seus usuários.[25]

Desse modo, o objetivo principal da Lei se iguala ao objetivo da grande maioria do ordenamento jurídico brasileiro, não foi algo inovador ou inédito. Trata-se do aproveitamento de princípios anteriormente existentes, cuja aplicabilidade ao mundo virtual dependia de muitas interpretações pelo operador jurídico, como a aplicação do princípio da inviolabilidade da vida privada de acordo com o artigo 7º da Lei 12.965/14.

A referida Lei é responsável por garantir a segurança dos dados pessoais através do sigilo das informações, dados, comunicações e registros armazenados, contudo, há uma exceção nesse aspecto, pois mediante consentimento do usuário, seus dados podem vir a serem utilizados por determinação judicial ou hipóteses previstas em lei. O consentimento do usuário em deixar seus dados disponíveis para aplicativos e para o fornecedor de internet garante que este possa armazenar os dados e os disponibilizar para investigações criminais caso seja solicitado através de mandado judicial.

Segundo o Marco Civil da Internet, cabe à empresa realizar o armazenamento dos registros de conexão e o acesso aos aplicativos,

[25] CARLOS HENRIQUE GALO. Lei nº 12.965/11: o Marco Civil da Internet – análise crítica. Jusbrasil. Disponível em: <https://henriquegalo.jusbrasil.com.br/artigos/118296790/lei-n-12965-11-o-marco-civil-da-internet-analise-critica>.

contudo devem garantir que a honra, vida privada e imagem dos usuários venham a ser preservadas. As informações apenas devem ser acessadas através de ordem judicial. Além disso, as informações que permitam qualificar a pessoa devem ser fornecidas pela empresa competente para adquirir os dados. Ainda, informações são impedidas de entrar em conflito com o art.7º.

Um ano, este é o prazo estabelecido para as empresas roteadoras de conexão armazenarem de modo sigiloso os registros de seus usuários em um ambiente adequado e com segurança garantida. Trata-se de uma responsabilidade exclusiva da provedora de internet e intransferível para terceiros. Todavia, a autoridade policial ou o Ministério Público podem requerer que este armazenamento esteja disponível por tempo superior a um ano. A autoridade que o requisitar detém prazo de 60 dias, a partir do requerimento, para ingressar com pedido de autorização judicial para ter acesso aos dados armazenados pela empresa. O provedor deve manter sigiloso o requerimento das informações, já que podem influenciar no andamento do julgamento.

As mensagens criptografadas são extremamente complexas, independentemente de terem sido feitas por uma inteligência artificial ou por um ser humano. Um caso ilustrativo é do conhecido Assassino do Zodíaco, um assassino em série americano, responsável pelo homicídio de cinco pessoas na Califórnia nos anos 60. Há 51 anos, foi encontrada uma mensagem criptografada pelo autor dos assassinatos, o qual jamais teve sua identidade descoberta. O assassino utilizou diversos métodos criados por ele mesmo para tornar a mensagem sem solução, a qual permaneceu indecifrável por tempo considerável.[26]

Apenas recentemente, em 2020, uma equipe de decifradores amadores desvendou a mensagem secreta, composta por 340 caracteres. A quantidade de simulações necessárias para desvendar uma mensagem codificada por um ser humano é considerável, além disso, foi necessária a utilização de um programa de computador criado com essa função pela equipe para permitir o entendimento da mensagem.

É impressionante o tempo dispendido na ignorância do conteúdo da mensagem, a qual poderia ser fundamental para efetuar a devida punição do autor dos assassinatos. A mensagem é composta pela diminuta quantidade de 91 palavras.

---

[26] STANLEY, Alyse. Após 51 anos sem solução, mensagem de assassino em série finalmente é decifrada. Gizmodo Brasil. Disponível em: <https://gizmodo.uol.com.br/mensagem-assassino-em-serie-decifrada/>.

Desde modo faz-se necessário refletir sobre o fato de o programa de computador, o qual é capaz de realizar um número imensurável de combinações diversas, demorar semanas para chegar a um veredicto sobre uma mensagem criptografada. O processo pode ser acelerado se o programa usufruir de inteligência artificial, pois automaticamente descartaria as combinações que não formassem um entendimento satisfatório. A autoridade policial nos âmbitos investigativos não pode dispender tanto tempo em mensagens codificadas, como as do aplicativo de mensagens WhatsApp.

As conversas virtuais, preferencialmente, devem ser acompanhadas de documentação que ateste a legitimidade de modo a comprovar que se trata da conversa original, sem alterações ou omissões de informações. Qualquer manipulação ou contaminação da prova poderia torná-la tendenciosa e, consequentemente, uma prova ilícita.

O documento que atesta a veracidade das mensagens não é obrigatório por lei, contudo, para evitar contestação e abrir precedentes para que a prova possa ser considerada ilícita, esse documento assume um papel preventivo.

3 PRECEDENTE RELEVANTE

O ato de provar, de acordo com o entendimento da maior parte da doutrina, está diretamente relacionado com a revelação da verdade. Contudo, o doutrinador Marcos Eberhardt[27] defende em sua obra, a impossibilidade de ser obtida a verdade real em um processo, de modo a resultar em semelhanças entre as alegações expostas pelas partes e os fatos que decorreram na realidade.[28]

Essas provas responsáveis por comprovar a veracidade da confissão poderiam ser obtidas com maior facilidade ao fazer uso dos dados contidos em aparelhos celulares. Deste modo, tratar-se-iam de provas indiretas, pois, mediante a análise das informações contidas nos celulares, pode ser comprovado fato diverso do que está sendo investigado, como por exemplo, localização do indivíduo no momento da

[27] EBERHARDT, Marcos. Provas no processo penal: análise crítica, doutrinária e jurisprudencial. 2. Ed. rev. e atual. – Porto Alegre: Livraria do Advogado 2018.

[28] LOPES JÚNIOR, Aury. Direito processual penal. 16. ed. São Paulo: Saraiva, 2019, p. 20.

ocorrência do delito. As provas indiretas podem permitir o descobrimento de detalhes relevantes sobre o delito e até mesmo a confirmação da autoria. Nesse caso, provas contidas em dispositivos poderiam ser classificadas em sua maioria, como provas não plenas, às quais permitem reforçar uma convicção.

A produção antecipada de provas é passível de ser realizada, contudo é extremamente excepcional, pois é necessário: (i) haver risco de perecimento; (ii) o conteúdo deve ter capacidade de influenciar na decisão; (iii) deve ser urgente e relevante a obtenção da prova naquele momento. Além disso, é necessária a existência de indicativos ínfimos de materialidade autoral. A antecipação ocorre antes da ação penal de ofício pelo magistrado, ou seja, é determinada no curso da investigação. Deve ser irreparável e não recorrível durante a fase judicial, assim alguns elementos apresentados na fase preliminar podem ser desconsiderados.[29]

Já os documentos (CPP, no art. 232) são instrumentos destinados a representar um fato ou ato juridicamente relevante. Desse modo, o objetivo não é deter credibilidade perante a fé-pública, apenas possuir eficácia probatória, ser redigido por "alguém definido e com "intuito de perturbar um direito através de sua fixação material."[30] Alguns documentos podem ser prejudicados, pois não são originais ou detêm origens que podem resultar em questionamentos sobre a veracidade das informações; para possuir o valor probatório do original é necessária autenticação, ou seja, deve ser reconhecida como verdadeira pelo funcionário público competente.

Segundo o entendimento do STF por meio do HC nº 372.762/MG[31], o e-mail e o aplicativo de celular WhatsApp, através de uma interpretação abrangente da lei, foram considerados análogos, sendo possível a aplicação do art.5º, X, da CF nessa situação. Desse modo, passou a ser necessária a obtenção das informações após a autorização judicial. Caso não haja essa autorização, a prova é ilícita e desvinculável dos autos.

Há entendimento de que o destinatário da correspondência poderá fazer uso do conteúdo compartilhado entre ele e o remetente. Assim, o "direito à intimidade" não poderá ser aplicado, pois é amparado

[29] LOPES JÚNIOR, Aury. Direito processual penal. 16. ed. São Paulo: Saraiva, 2019, p.33

[30] LOPES JÚNIOR, Aury. Direito processual penal. 16. ed. São Paulo: Saraiva, 2019, p. 203.

[31] HC nº372.762/MG, 5º Turma, Rel. Min. Felix Fischer, j. 03/10/2017.

pela excludente de ilicitude da legítima defesa própria, ou seja. é destinado a preservar o direito do destinatário. Considerando que o WhatsApp é equivalente ao correio eletrônico, e, portanto, à correspondência, este fato permitiria ao(s) receptor(es) envolvido(s) no diálogo fazer uso do WhatsApp como meio de prova sem que se torne prova ilícita.

A jurisprudência ARE 1042075 RG / RJ, é decisão proferida com Repercussão Geral no recurso extraordinário com agravo 1.042.075 RJ. A decisão foi unânime, de modo a julgarem constitucional a questão tratada, além de considerarem a existência de repercussão geral.[32]

O acusado era investigado por roubo duplamente circunstanciado, com emprego de arma de fogo e concurso de agentes. Juntamente com um indivíduo não identificado, fez-se uso de emprego de grave ameaça, exercida com manuseio de arma de fogo, somada ao emprego de violência concretizada através de empurrão e batidas da cabeça da vítima contra o chão. A vítima reagiu, ao segurar a bolsa e sofreu as agressões. Após subtrair a bolsa o delinquente fez uso de uma motocicleta dirigida por seu comparsa, o qual aguardava para efetuar a fuga. Nesse momento, o delinquente deixou cair um aparelho de telefonia celular, o qual foi levado pela vítima até a delegacia e analisado por policiais civis. Através de fotografias armazenadas no aparelho, na manhã do dia seguinte dos fatos, foi possível identificar e efetuar a prisão do recorrente. A atitude da autoridade policial em analisar o aparelho de telefonia trata-se de inegável cumprimento do dever policial.

A manipulação do aparelho de telefonia celular realizado pela autoridade policial foi abordada como ilícito e desautorizado. Somente após analisar o conteúdo armazenado no smartphone, permitiu-se identificar o implicado, endereço de seu domicílio e da namorada, para a qual havia efetuado uma ligação antes do ocorrido. Assim, o histórico de chamadas e a galeria de fotos foram violados.

Mediante a decisão proferida pelo Tribunal de Justiça do Estado do Rio de Janeiro, absolveu-se o recorrido com base no art. 386, inc. VII, do Código de Processo Penal. O artigo foi passível de aplicação ao considerar a ilicitude de prova, além de possuir como fundamento de incidência da teoria dos frutos da árvore envenenada, responsável por proceder na desconsideração de toda e qualquer informação direta e indiretamente relacionada com a prova considerada ilícita.

[32] STF - ARE n.1042075 RG / RJ, Rel. Min. Dias Toffoli, DJ 23-11-2017 https://portal.stf.jus.br/processos/downloadPeca.asp?id=313464292&ext=.pdf

No voto do Relator Ministro Dias Toffoli, é apresentada a permissibilidade de acesso a informações e registros armazenados em smartfones apreendidos, os quais podem ser usados como instrumento ou objeto do crime praticado. Para efetuar a análise dos dados do aparelho, encontrado no local do crime, não haverá a obrigatoriedade da autorização do proprietário ou mandado judicial. Essa situação é válida para cidadãos detidos em situações idênticas.

A autoridade policial é responsável por apreender quaisquer objetos e instrumentos relacionados com a conduta delitiva, de modo a verificar a licitude das provas produzidas durante a instauração do inquérito policial.

A apreensão do celular do recorrente é lícita, pois além de ter sido encontrado no local do crime, o objeto era essencial para provar a infração penal quando a autoridade policial detiver conhecimento da prática de crime de ação penal pública. Efetuar a verificação do conteúdo armazenado no dispositivo não resultaria em prejuízo ao direito do sigilo das comunicações telefônicas, apenas permitiria acesso aos dados do objeto apreendido, cuja perícia deve ser efetuada, obrigatoriamente, pela autoridade policial.

Assim, as autoridades policiais são responsáveis por apreender objetos e instrumentos relacionados à conduta delitiva. Mediante tal premissa, acessar dados e registros armazenados nos celulares é legítimo, de modo algum configura violação do sigilo da comunicação telefônica e de suas informações. Conclui-se que é desnecessária a aquisição de mandado de busca no caso abordado, ou seja, se o celular for obtido no local do crime.[33] Principalmente ao considerar a obrigatoriedade da apreensão e perícia realizadas pela autoridade policial.

4 CONSIDERAÇÕES FINAIS

O aplicativo de mensagem WhatsApp é frequentemente acessado no Brasil, além disso, teve um intenso aumento na quantidade de usuários durante a pandemia causado pela Covid-19. O aplicativo sofre constantes atualizações que disponibilizaram funções que ultrapassam a

[33] Aplicação das Súmulas no STF :: STF - Supremo Tribunal Federal. Stf.jus.br. Disponível em: <http://www.stf.jus.br/portal/jurisprudencia/menuSumarioSumulas.asp?sumula=2174>.

simples troca de mensagens, as quais tornaram o aplicativo uma valiosa fonte de informações sobre os usuários.

Contudo, acessar essas informações é dificultado pela criptografia de ponta a ponta, destinada a garantir sigilo e segurança às informações dos usuários. A criptografia gera acesso restrito ao conteúdo das mensagens, dificulta o acesso de terceiros ou invasões ao sistema. Simultaneamente, é favorável à empresa que se isenta de fornecer o conteúdo das mensagens através da alegação de inexistência de armazenamento ou de uma chave de acesso capaz de descodificar o conteúdo. A emissão do mandado judicial não resultou em colaboração da empresa responsável pelo aplicativo, situação que gerou vários bloqueios como sanção pelo descumprimento da medida. Os bloqueios afetavam nocivamente o coletivo, que teve de encontrar outro meio de comunicação quando o aplicativo deixou de funcionar. Atualmente os bloqueios entraram em desuso, pois não geraram resultados e nem incentivaram a empresa a colaborar com o poder judiciário.

Tornou-se essencial analisar outras medidas passíveis de serem aplicadas: a "*backdoor"* foi proposta como uma ferramenta obrigatória integrada a aplicativos, detentora da possibilidade de acessar o conteúdo das plataformas e dispositivos criptografados mediante mandado judicial, entretanto especialistas da área indicam que a criação desse método iria originar vulnerabilidade generalizada no sistema, afetaria a todos os usuários e não exclusivamente o indivíduo indicado no mandado judicial. Outra medida possível de ser aplicada é o uso de metadados: trata-se de dados que descrevem outros dados.

Ademais, as tecnologias têm recursos capazes de proporcionar oportunidade de evolução, de modo a garantir celeridade processual, como a iniciativa de realizar intimação e comunicações de atos processuais através do aplicativo de mensagem WhatsApp. A mudança pode dar origem à resistência, como a expressa pela corregedoria do Tribunal de Justiça de Goiás, a qual é extremamente importante para analisar aspectos negativos e positivos da implantação do método de intimação, mas houve maiores benefícios a serem considerados.

As evoluções tecnológicas devem ser acompanhadas pelas inovações das normas. A ausência de previsão legal sobre alguns temas na Lei Geral de Proteção de Dados ocorre pela existência de informações muito genéricas. A Lei nº 12.965/14 pretende proteger os dados pessoais, como meio para regular o uso da internet no Brasil.

Antes da promulgação da LGPD e da Lei 12.965/14, houve um período considerável entre a implantação da internet e de normas específicas para regulá-la, de modo que a violação de direitos era solucionada através do Código Civil ou do Código de Defesa do Consumidor, os quais, depois da implementação das leis específicas, passaram a serem usados em caso de ausência de dispositivos. A lei estipula que o fornecedor de internet nacional deve armazenar registros de conexão e o acesso aos aplicativos, dados dos usuários e, caso seja solicitado através de mandado judicial, deve disponibilizar as informações para investigações criminais. Caso haja descumprimento, gera sanções.

Sobre a admissibilidade de provas ilícitas, uma das correntes defende o uso do princípio da proporcionalidade; resulta em permissibilidade do uso das provas ilícitas em algumas circunstâncias se for favorável ao réu; protege o interesse público independente do modo pelo qual a prova teve origem. Discrepa da teoria da árvore dos frutos envenenados, responsável por realizar uma análise da influência das provas ilícitas no processo, averiguando se houve contaminação de outras provas do processo, sendo inadmissível aplicação de provas originárias das ilícitas. Essa teoria atualmente, é subjugada pela teoria da fonte independente e suas variações, pois considera que a prova ilícita pode não ser responsável pela manifestação de prova derivada, além da alegação de possuir fonte própria.

Já o princípio da serendipidade é pautado no acaso de encontrar evidências que não eram o objetivo inicial, mas que resultem em novas descobertas benéficas. O princípio auxilia a validação de provas surgidas durantes medidas cautelares como busca e apreensão ou interceptação telefônica e, no cumprimento do mandado, podem surgir provas que não haviam sido descritas. Essas provas não deveriam ser consideradas ilícitas por serem aptas a auxiliar no processo, pois a desconsideração poderia resultar em prejuízos ao processo, beneficiar delinquentes, situação essa inadmissível, pois dificultaria a investigação e aplicação da justiça.

As provas obtidas no WhatsApp têm sua veracidade amplamente questionada, pois é possível praticar alterações no conteúdo das conversas, através do uso de aplicativos com essa finalidade ou até mesmo hackeando a conta do outro usuário para obter acesso a conversas particulares ou implantar mensagens com conteúdo condenatório. Para evitar esse tipo de questionamento sobre a veracidade, é necessária a

presença de documentação que ateste a legitimidade de tratar-se de conversa original.

O FBI já realizou invasão ao sistema da marca Apple para obter dados contidos no celular do investigado e não contar com o auxílio da empresa em autorizar o acesso; o governo, então, optou por descodificar o sistema através de invasão hacker. Porém efetuar essa atitude em outros casos é inviável, as mensagens criptografadas são morosas de serem desvendadas, mesmo se forem feitas por um ser humano, o qual possui menor habilidade de codificar do que uma inteligência artificial ou software. O Assassino do Zodíaco codificou uma breve mensagem composta por 340 caracteres, sem auxílio de uma inteligência artificial, 51 anos atrás. O FBI não obteve êxito em descodificar, o que ilustra o quão complexo é desvendar esse tipo de conteúdo. Portanto, pode-se supor que a autoridade policial dispenderia muito tempo em uma única função. Esse tempo seria mais bem aplicado em outros aspectos do âmbito investigativo.

Os aparelhos celulares são responsáveis por armazenar uma variedade considerável de informações diversas, que auxiliariam a obtenção com maior precisão dos fatos investigados. A produção antecipada de provas deve ocorrer em casos excepcionais urgentes ou de risco de perecimento, como ocorre no WhatsApp por correr o risco das mensagens serem apagadas. Portanto, o celular pode ser considerado uma prova antecipada caso a autoria seja minimamente comprovada. Além disso, o STF considerou o e-mail e o WhatsApp equivalentes, situação que tornou necessária autorização judicial para acessar as informações, para que a prova não fosse considerada ilícita e desvinculada dos autos. Contudo, também permite ao destinatário, como ocorre no caso das correspondências, fazer uso do conteúdo das mensagens como meio de prova em um processo sendo amparado pela excludente de ilicitude da legítima defesa própria.

Na jurisprudência HC n.372.762/mg, a defesa alegou a necessidade de autorização judicial para acessar as informações contidas nos celulares, os quais foram apreendidos mediante cumprimento de ordem judicial de busca e apreensão. Foi considerado que os celulares por estarem protegidos e armazenados inviabilizariam violações físicas no dispositivo, de modo a ser desnecessário acessar imediatamente, possibilitando a espera por uma nova autorização judicial que permite seu acesso às informações armazenadas, contudo essa espera geraria maior morosidade ao processo investigativo. A defesa solicitou que as

mensagens transcritas no laudo policial fossem desconsideradas dos autos processuais. O Ministro Felix Fischer alegou que a busca e apreensão têm a finalidade de localizar os objetos, mas não abrange acessar registro de chamadas, mensagens de texto, dados de georreferenciamento, eventos do calendário, fotos. Os quais seriam dados privados que ao serem acessados e seu conteúdo transcrito em laudo pericial infringiria o direito à privacidade. A quebra do sigilo foi condicionada a uma autorização judicial, as informações do celular deveriam ser acessadas caso outro meio probatório não seja possível. Deixar um dispositivo detentor de tantas informações como o último recurso é um retrocesso, o qual contribuiria para mais tempo dispendido para buscar outros meios de provas, os quais poderiam levar a conclusões semelhantes.

A jurisprudência ARE 1042075 RG / RJ, diverge da anterior em diversos aspectos. Neste caso a ilicitude das provas resultou na inexistência de provas suficientes para a condenação, resultando na absolvição do réu. As provas foram consideradas ilícitas por conta da aplicação da teoria da árvore dos frutos envenenados, a qual desconsiderou informações direta ou indiretamente vinculadas à prova considerada ilícita. O aparelho telefônico foi apreendido no local do delito, houve cumprimento do dever policial, contudo a defesa considerou o acesso ilícito e desautorizado o que imputou em nulidade de todas as provas decorrentes. A análise efetuada pelos policiais permitiu em um curto período, identificar a localização do infrator, sua identidade, informações essas essenciais para todo o andamento do processo. O Ministro Dias Toffoli considerou que as informações do smartphone poderiam ser usadas sem autorização do proprietário ou mandado judicial, essa situação seria válida para cidadãos detidos em casos idênticos. O celular foi um objeto essencial para provar a ocorrência da infração penal e o acesso dos dados armazenados não pode ser considerado como uma espécie de comunicação telefônica. Os avanços tecnológicos evidenciam que os smartphones possuem informações que destoam da comunicação telefônica como fotos, mensagens, blocos de notas, registro de pesquisas. Deste modo, não podem ser tratados da mesma forma.

Ter menos burocratização para acessar os dados dos aparelhos telefônicos, seria essencial para que a autoridade policial possa cumprir seu dever de preservar provas. As investigações seriam mais céleres e deteriam maiores informações sobre o delito investigado. O WhatsApp

tem potencial para ser um eficiente meio de prova, por ser o modo de obter novas provas complementares das investigações.

REFERÊNCIAS

Aplicação das Súmulas no STF :: STF - Supremo Tribunal Federal. Stf.jus.br. Disponível em: <http://www.stf.jus.br/portal/jurisprudencia/menuSumarioSumulas.asp?sumula=2174>.

BRASIL, **LEI Nº 12.965, DE 23 DE ABRIL DE 2014**. Planalto.gov.br. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>.

BRASIL. **LEI Nº 11.690, DE 9 DE JUNHO DE 2008**. Planalto.gov.br. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/lei/l11690.htm>.

CARLOS HENRIQUE GALO. **Lei nº 12.965/11: o Marco Civil da Internet – análise crítica**. Jusbrasil. Disponível em: <https://henriquegalo.jusbrasil.com.br/artigos/118296790/lei-n-12965-11-o-marco-civil-da-internet-analise-critica>.

Central de ajuda do WhatsApp - Sobre a criptografia de ponta a ponta. WhatsApp.com. Disponível em: <https://faq.whatsapp.com/general/security-and-privacy/end-to-end-encryption/?lang=pt_br>.

CNJ - PCA - Procedimento de Controle Administrativo, Portaria Conjunta n. 01/2015, Relatora Daldice Santana, Plenário Virtual, 23 de junho de 2017.

ENBERG, Jasmine. **Global Messaging Apps 2019**. Insider Intelligence. Disponível em: <https://www.emarketer.com/content/global-messaging-apps-2019>

FLÁVIA TEIXEIRA ORTEGA. **Afinal, é possível o uso do WhatsApp para intimações judiciais?** Jusbrasil. Disponível em: <https://draflaviaortega.jusbrasil.com.br/noticias/473474379/afinal-e-possivel-o-uso-do-whatsapp-para-intimacoes-judiciais>.

GOMES, Luiz Flávio; CUNHA, Rogério Sanches. **Legislação Criminal Especial.** Coleção Ciências Criminais. Vol. 6. São Paulo: Editora Revista dos Tribunais, 2009. p.474.

HADDAD, H.. WhatsApp é o aplicativo mais usado na pandemia - Estudo ESPM. 2020.

HC nº372.762/MG, 5º Turma, Rel. Min. Felix Fischer, j. 03/10/2017.

ISADORA, Lorena. **O princípio da serendipidade no direito processual penal brasileiro**. Frutal/MG: Prospectiva, 2016.

LOPES JÚNIOR, Aury. **Direito processual penal**. 16. ed. São Paulo: Saraiva, 2019

S.4051 - 116th Congress (2019-2020): Lawful Access to Encrypted Data Act. Congress.gov. Disponível em: <https://www.congress.gov/bill/116th-congress/senate-bill/4051/>.

Sobre o WhatsApp. WhatsApp.com. Disponível em: <https://www.whatsapp.com/about/?lang=pt_br>.

STANLEY, Alyse. Após 51 anos sem solução, mensagem de assassino em série finalmente é decifrada. Gizmodo Brasil. Disponível em: <https://gizmodo.uol.com.br/mensagem-assassino-em-serie-decifrada/>.

STF - ARE n.1042075 RG / RJ, Rel. Min. Dias Toffoli, DJ 23-11-2017 https://portal.stf.jus.br/processos/downloadPeca.asp?id=313464292&ext=.pdf

WYNN, Charles M., WIGGINS, Arthur W. **As Cinco Maiores Idéias da Ciência**. Tradução de Roger Maioli. São Paulo: Ediouro, 2002. p.172.