

Matheus de Sequeira: Print de Whatsapp e a cadeia de custódia

27/10/2022

O surgimento dos *smartphones* com internet móvel revolucionou a forma como as pessoas se comunicam, sendo fato notório que a sociedade brasileira adotou como forma de comunicação principal as mensagens instantâneas, trocadas principalmente pelo aplicativo *Whatsapp*. Uma das consequências disso é que o acesso ao aparelho passou a se tornar uma das melhores formas — senão a melhor — para revelar com quem a pessoa se comunica e quais os assuntos tratados com cada interlocutor. Assim sendo, na esfera da investigação criminal, o acesso a conversas é de enorme valia ao investigador e pode se traduzir no limiar de sucesso ou insucesso de uma persecução penal.



Entretanto, diferentemente do que acontecia com as

ligações telefônicas e trocas de SMS, não é possível ter acesso a estas conversas por meio de uma interceptação telefônica, por exemplo, por conta da tecnologia usada pelo aplicativo, que utiliza do mecanismo de criptografia assimétrica para codificar as mensagens trocadas entre dois terminais, no que a empresa chama de "criptografia de ponta a ponta" (*end-to-end*). Significa que quando o remetente envia a mensagem em texto, ao deixar o terminal (celular), a mensagem é codificada e só é decodificada e traduzida novamente em texto quando é recebida pelo outro terminal, de forma que nem mesmo a empresa consegue decifrar o código enquanto não é recebida pelo destinatário.

Sendo assim, a única forma de se ter acesso às conversas de *Whatsapp* de uma pessoa é tendo acesso a um dos terminais, ou seja, um dos *smartphones* onde o aplicativo está instalado, pois somente estes possuem as respectivas chaves de criptografia para decodificar aquela conversa.

No cotidiano do direito penal, o efeito disso é que, quando se articula uma grande investigação criminal, o que vemos é que em algum momento são deflagradas operações policiais para efetivar medidas de busca e apreensão, nas quais um dos objetivos principais é a apreensão de telefones celulares dos alvos. É a partir desse momento que começam a surgir questões

extremamente relevantes no âmbito da produção probatória.

A primeira delas é que, no que pese a apreensão do celular e até que o alvo informe a senha do aparelho, o acesso ao conteúdo dos celulares apreendidos imprescindivelmente deve ser precedido de decisão judicial provocada a partir da representação do Ministério Público e/ou da autoridade policial pela quebra do sigilo de dados do investigado. Somente a partir da autorização judiciária, Polícia e Ministério Público poderão ter conhecimento de todos dados contidos no *smartphone*.

Neste ponto é fundamental discernir que, apesar do conhecimento, aquelas informações contidas no aparelho telefônico só poderão produzir valor probatório caso se preserve intacto todo o material obtido pelo acesso ao telefone celular (mensagens, fotos, áudios, etc.) e, ainda, que seja possível conceder à defesa, posteriormente, o mesmo acesso pleno à integralidade desse material. Isso porque é preciso manter intacta a cadeia de custódia da prova, positivada no artigo 158-A do Código de Processo Penal, tendo em vista que *"toda vez que a investigação envolver a coleta, armazenamento ou a análise de fontes reais, isto é, de coisas, será necessária a adoção de determinados cuidados para garantia de sua autenticidade e integridade, no sentido de que o objeto levado ao processo para ser valorado pelo juiz é exatamente a mesma coisa tal qual encontrada e apreendida"* [1].

No que tange às conversas do aplicativo *Whatsapp* encontradas em um aparelho celular, a preservação da prova em estrito cumprimento à cadeia de custódia, deve ser feita a partir da extração das mensagens armazenadas no aparelho mediante atuação de perito, que por sua vez, deve utilizar *softwares* específicos para isso, que servem justamente para garantir a fidelidade da prova, como, por exemplo, aqueles desenvolvidos pela empresa *Cellebrite* [2], que ficou famosa no Brasil por ser de origem israelense.

Contudo, o que vemos amplamente na praxe é que em inúmeras investigações os órgãos de persecução penal acessam as informações contidas no telefone, devidamente amparados por ordem judicial, mas não realizam a devida extração dos dados e seu armazenamento em outra unidade de mídia, o que se chama de "espelhamento de dados". O que se vê é que, por falta de conhecimento e/ou de recursos, as polícias judiciárias apenas elaboram relatórios descrevendo e colacionando as imagens dos dados que foram encontrados no armazenamento do telefone e, especificamente no que tange às conversas de *Whatsapp*, apresentam as capturas de tela (*printscreens*), popularmente conhecidas como *prints*, o que não é minimamente suficiente para atender os requisitos da regular cadeia de custódia, na medida em que a não preservação dos dados digitais ou mesmo a preservação parcial deles torna a prova ilícita. Sobre o assunto leciona o professor Gustavo Badaró:

"Nos casos de computer forensics, os elementos de prova são conservados e transmitidos em linguagem não natural, mas digital. Assim, ainda que os dados digitais, em seu conteúdo informativo, possam ser diretamente percebidos por quem está em contato com eles, esses não possuem materialidade imediatamente constatável. (...).

Em suma, tais elementos de prova consistiriam, originariamente, em dados digitais, para que minimamente seja atestada a sua autenticidade e integridade, devem ser seguidos os métodos informáticos de obtenção, registro, armazenamento, análise e apresentação de tal espécie de

prova. Sua apresentação judicial, para que tenha potencial epistêmico adequado, deverá se dar por meio de prova pericial. E nesse caso, sem que haja a documentação da cadeia de custódia, não será possível ter qualquer segurança quanto à autenticidade e conteúdo da prova digital, sendo ela imprestável para o acerto judicial [3]."

É que o *print*, por si só, é a imagem da prova e não a prova materialmente, que são os dados digitais correspondentes àquelas conversas, ao passo que nada garante que aquela imagem reflete estritamente as conversas que foram encontradas no aparelho de celular, já que os *prints* podem ser facilmente manipulados através de diversos *softwares* de edição de fotos, por exemplo, e não há como comparar a imagem com a mídia digital propriamente dita. Como bem explica Alexandre Morais da Rosa:

"(...) Nós acreditamos que ao ver a imagem, aquilo que o professor Rui Cunha Martins em Portugal fala do 'excesso da evidência', está tão evidente ali que eu consegui extrair um print. Só que este print, além de ser insuficiente para demonstrar a validade, porque é facilmente manipulável, ele precisa da compreensão de que a inclusão digital não é só ter o computador (...), a inclusão digital no plano da advocacia pressupõe a aquisição de alguns softwares para poder realizar essa extração. (...)

O fato de nós termos uma imagem não é confundido com o plano da existência da prova, porque a prova digital não é a mesma coisa do que a imagem. (...) O tratamento de provas digitais, ou seja, como é que eu posso mostrar o percurso dela, eu preciso ter uma cópia, que é a aquisição, que é uma primeira fase. A aquisição não se confunde com um print e tem regras técnicas para que nós possamos fazer isso [4]."

Neste sentido, não importa, frise-se, neste ponto, se as mensagens retratadas no *print* são verdadeiras ou não, pois, ainda que consideradas perfeitamente fidedignas, é imperioso que a defesa tenha acesso à íntegra dos dados obtidos a partir da quebra de sigilo de dados para deles dispor e explorar no exercício da defesa, sendo inadmissível que a defesa tenha acesso apenas ao que foi selecionado, pinçado da íntegra dos dados pelos órgãos de persecução penal e representado nos *prints*.

De forma a facilitar a compreensão da gravidade de se conferir legalidade ao *print* de uma conversa de *Whatsapp*, seria como validar a foto da arma de um crime, sem que ela fosse apreendida e periciada, ou a cópia de um documento supostamente falso, sem que o original fosse periciado. Como se disse, a foto da prova se distingue totalmente da prova materialmente, que deve ser coletada, acondicionada e armazenada devidamente, no caso das provas digitais extraídas de um *smartphone*, através do espelhamento de dados em outra unidade de armazenamento de mídia digital, em outras palavras, copiados de forma específica para preservar toda a sua origem para um HD externo ou um pen-drive (dependendo da extensão do arquivo).

No mesmo sentido, a ausência da atuação de um perito na extração destes dados de aparelho de telefonia celular, poderia analogicamente levar à equivocada conclusão de que seria desnecessária também a atuação de um médico legista no exame cadavérico da vítima ou de um perito no exame sobre material entorpecente, podendo a análise ser feita pela própria autoridade policial ou pelos policiais que compõe o efetivo da delegacia, o que, por certo, é um

autêntico absurdo e pode contaminar toda a prova a partir da falta de *expertise* na extração dos dados digitais.

Soma-se a tudo isto uma consequência positiva de se realizar imediatamente a extração e o espelhamento de dados dos celulares para outras unidades de armazenamento de mídia, qual seja, a pronta possibilidade de restituição do bem apreendido ao alvo da medida, o que vemos que na praxe demora em demasia.

Este assunto, inclusive, já foi apreciado pelo Superior Tribunal de Justiça em relação a *prints* das telas do aplicativo *Whatsapp Web*, que é a modalidade do *Whatsapp* para desktops:

"AGRAVO REGIMENTAL NO RECURSO EM HABEAS CORPUS. CORRUPÇÃO ATIVA E PASSIVA. NOTÍCIA ANÔNIMA DO CRIME APRESENTADA JUNTO COM A CAPTURA DA TELA DAS CONVERSAS DO WHATSAPP. INTERLOCUTOR INTEGRANTE DO GRUPO DE CONVERSAS DO APLICATIVO. POSSIBILIDADE DE PROMOÇÃO DE DILIGÊNCIAS PELO PODER PÚBLICO. ESPELHAMENTO, VIA WHATSAPP WEB, DAS CONVERSAS REALIZADAS PELO INVESTIGADO COM TERCEIROS. NULIDADE VERIFICADA. DEMAIS PROVAS VÁLIDAS. AGRAVO REGIMENTAL PARCIALMENTE PROVIDO.

(...) 3. Esta Sexta Turma entende que é inválida a prova obtida pelo WhatsApp Web, pois 'é possível, com total liberdade, o envio de novas mensagens e a exclusão de mensagens antigas (registradas antes do emparelhamento) ou recentes (registradas após), tenham elas sido enviadas pelo usuário, tenham elas sido recebidas de algum contato. Eventual exclusão de mensagem enviada (na opção Apagar somente para Mim) ou de mensagem recebida (em qualquer caso) não deixa absolutamente nenhum vestígio, seja no aplicativo, seja no computador emparelhado, e, por conseguinte, não pode jamais ser recuperada para efeitos de prova em processo penal, tendo em vista que a própria empresa disponibilizadora do serviço, em razão da tecnologia de encriptação pontaaponta, não armazena em nenhum servidor o conteúdo das conversas dos usuários' (RHC 99.735/SC, relator ministra LAURITA VAZ, SEXTA TURMA, julgado em 27/11/2018, DJe 12/12/2018). 4. Agravo regimental parcialmente provido, para declarar nulas as mensagens obtidas por meio do print screen da tela da ferramenta WhatsApp Web, determinando-se o desentranhamento delas dos autos, mantendo-se as demais provas produzidas após as diligências prévias da polícia realizadas em razão da notícia anônima dos crimes [5]."

Neste julgado, a 6ª Turma do STJ chama atenção que o *print* das telas do *Whatsapp Web*, mesmo que se assumisse a veracidade em relação às conversas correspondentes, somente retrataria o estado momentâneo da prova material, que seria a mídia digital da conversa que foi fotografada, a qual, contudo, poderia ser posteriormente alterada através das ferramentas "apagar para mim" ou "apagar para todos", caracterizando claríssima violação à cadeia de custódia já que não haveria qualquer registro da alteração da prova e, tampouco, seria a prova dotada de originalidade. Isto tudo porque não foi feita a devida extração de dados no momento da apreensão da unidade de armazenamento, seja o computador ou o celular.

Em síntese, o que temos é que é imperiosa a compreensão por parte de todos os atores do processo penal, delegados, advogados, membros do Ministério Público e magistrados, de que o *print* da tela não é a prova material em si, mas apenas uma fotografia da prova, o qual a única

utilidade no processo é ser usado em peças processuais para destacar um trecho da prova digital que se faz referência, prova esta que invariavelmente deve estar presente no processo em estrita harmonia com a devida cadeia de custódia. Portanto, os atores devem se atentar que, no que pese a apreensão do aparelho celular do acusado, o manuseio dos dados ali armazenados por um agente público imperito para realizar a devida extração de dados tem grande potencial de contaminar toda a prova e violar a cadeia de custódia, maculando a prova de ilicitude por violação ao artigo 158-A e seguintes do Código de Processo Penal.

[1] BADARÓ, Gustavo Henrique. Processo Penal. 10. ed. rev. atual. e ampl. São Paulo: Editora Revista dos Tribunais, 2022, p. 517.

[2] <https://celebrite.com/en/home>

[3] BADARÓ, Gustavo Henrique. Processo Penal. 10. ed. rev. atual. e ampl. São Paulo: Editora Revista dos Tribunais, 2022, p. 527 e 531.

[4] ROSA, Alexandre Moraes da. Criminal Player Ep.053: O Que Você Deveria Saber Sobre Provas Digitais. Florianópolis/SC. Emais Editora, 09 out. 2021. *Podcast*. Disponível em: <https://open.spotify.com/episode/0mbJtAAR05AVDd3xRI9d10> . Acesso em 03 mai. 2022.

[5] STJ — AgRg no RHC: 133430 PE 2020/0217582-8, relator: ministro NEFI CORDEIRO, Data de Julgamento: 23/02/2021, T6 — SEXTA TURMA, Data de Publicação: DJe 26/02/2021).

Fonte: <https://conjur.jumps.com.br/2022-out-27/matheus-sequeira-print-whatsapp-cadeia-custodia/>