Fernando Moreira: Questões tecnológicas sobre “conversas vazadas”

04/07/2019

Desde o começo de junho, quando o site estrangeiro *The Intercept Brasil*[1] começou a publicar reportagens nas quais afirma que teve acesso, por meio de uma fonte anônima, a mensagens trocadas pelo aplicativo Telegram entre o então juiz Sergio Moro e o procurador Deltan Dallagnol, durante a operação “lava jato” e na pendência de julgamento do ex-presidente Luiz Inácio Lula da Silva, os mundos político e jurídico brasileiros passaram a discutir, basicamente, duas questões: *(i)* qual deveria ser a punição ao ex-juiz Sergio Moro e ao procurador Deltan Dallagnol em razão do teor das alegadas conversas[2]; e *(ii)* quando o ex-presidente Luiz Inácio Lula da Silva deveria ser solto pelo Supremo Tribunal Federal, em razão da quebra da imparcialidade jurisdicional “revelada” pelo teor das alegadas conversas, ou mesmo se todas as condenações proferidas pelo ex-juiz Sergio Moro no âmbito da operação “lava jato” deveriam ser anuladas pela mesma razão.

Todavia, nos parece que tais discussões ainda são muito precipitadas, porque decorrentes de uma percepção manifestamente errada da realidade, talvez fruto de paixões políticas ou cegueiras ideológicas e ou também do desconhecimento da tecnologia envolvida na troca de mensagens pelo aplicativo Telegram, porque o que o site *The Intercept Brasil* vem divulgando desde então não são, obviamente, mensagens trocadas pelo aplicativo, mas meras imagens, sequer das telas dos aparelhos celulares dos interlocutores das alegadas mensagens (isto é, os conhecidos *prints* das telas), que igualmente não se confundem com as reais mensagens trocadas pelo Telegram.

De fato, conforme já tivemos a oportunidade de esclarecer em sede doutrinária sobre o e-mail [3], nem mesmo as impressões de telas de mensagens do aplicativo Telegram são tecnicamente as próprias mensagens trocadas pelo referido aplicativo, como, da mesma forma, a mera impressão de um e-mail não é tecnológica e ontologicamente um e-mail. Em termos de tecnologia e, portanto, no mundo de verdade, da realidade dos fatos, as diferenças técnicas entre uma “mensagem” e uma “imagem de uma mensagem” são abissais. Quem conhece um pouquinho mais de tecnologia da informação sabe que o *print* de uma tela de computador ou de *smartphone*, ou seja, uma imagem, pode ser facilmente manipulada por qualquer criança da atualidade, com *softwares* disponíveis em qualquer computador doméstico com o sistema operacional Windows, sendo, ainda, possível produzir, de forma praticamente sem chance para perícia quanto à manipulação, sucessivas imagens da imagem que foi adulterada, o que retira qualquer força probatória autônoma de meras imagens de telas de computador e de *smartphones*, o que, aliás, felizmente já foi percebido pela jurisprudência[4].

Nesse sentido, por exemplo, Renato Opice Blum assevera que “eis que surge a grande questão jurídica: uma simples impressão de página de Internet vale como prova? Ora, qualquer pessoa com conhecimento mediano em programas editores de imagem pode adulterar uma imagem digital”[5].

Aliás, a esse respeito, para manipulações de imagens de telas de *smartphones*, digamos, mais "sofisticadas" do que a facílima manipulação caseira, basta esclarecer que as próprias lojas de aplicativos do Google (a Playstore) e da Apple (a App Store) disponibilizam gratuitamente aplicativos geradores de *fakechats*, isto é geradores de mensagens falsas, para os usuários "brincarem" uns com os outros, criando e enviando imagens de mensagens com teores absurdos ou, para alguns, "engraçado", mas todos faticamente falsos[6].

Por outro lado, a manipulação e adulteração dos arquivos gerados nos *smartphones* pelos aplicativos de troca de mensagens, tais como WhatsApp e Telegram, não podem ser feitas por qualquer pessoa, pois requerem conhecimentos bem mais profundos de tecnologia da informação e do funcionamento dos *smartphones*, e, de qualquer forma, deixam rastros nos arquivos digitais que podem ser identificados numa perícia digital bem-feita.

Nesse sentido, por exemplo, nos *smartphones* com o sistema operacional Android, o mais usado do mundo[7], o aplicativo Telegram registra num arquivo chamado "cache4.db", num diretório existente na raiz do aparelho denominado "datadataorg.telegram.messengerfiles" (inacessível ao usuário comum), tabelas contendo os nomes de contatos, mensagens e todos os metadados das mensagens trocadas a partir daquele aparelho[8], isto é, todos os nomes de usuário (*user ID*), números dos telefones celulares dos destinatários e os *timestamps* (dias e horários das mensagens trocadas). Mesmo o conteúdo das mensagens enviadas no modo "secreto" (o Telegram possibilita dois modos de envio de mensagens, o "normal" e o "secreto", sendo que este seria teoricamente mais seguro, com "mais privacidade" do que aquele) já foi provado por *white hat hackers* ser acessível e decifrável, uma vez que as mensagens são gravadas no arquivo denominado "cache4.db" em *bites* e, portanto, de fato em texto tecnicamente decifrável [9].

Da mesma forma, em relação a arquivos de mídia enviados e recebidos pelo aplicativo Telegram, tais como documentos (em formato PDF, Word, txt etc), fotos, vídeos e mensagens de áudio gravadas, o Telegram os salva sem encriptação nos aparelhos dos usuários num diretório facilmente acessível denominado "/storage/emulated/0/Telegram/", (cujo acesso pode ser feito pelo usuário comum com o uso de aplicativos exploradores de arquivos disponíveis gratuitamente nas lojas de aplicativos).

Portanto, a despeito de o Telegram anunciar que armazena na *nuvem* as mensagens trocadas pelos usuários, isto é, num servidor da própria empresa, de forma criptografada, o que é verdade e por isso não se contesta, os registros dessas mensagens são gravados nos aparelhos dos usuários desse aplicativo, no arquivo denominado "cache4.db", cujo acesso e deciframento já foram provados como sendo tecnicamente possíveis, permitindo, com isso, atestar com alto grau de precisão e confiabilidade não somente os metadados das mensagens trocadas pelos usuários do Telegram instalado em cada *smartphone*, inclusive com quem e quando o usuário do aplicativo trocou mensagens, como, também, o próprio conteúdo dessas mensagens.

Assim, se realmente um *hacker* teve acesso ao aplicativo Telegram instalado no telefone celular ou do então juiz Sergio Moro ou do procurador Deltan Dallagnol (ou dos dois, mas bastaria o hackeamento do *smartphone* de somente um dos dois para ter acesso às conversas entre eles trocadas pelo Telegram), ele com certeza pôde acessar e copiar o referido arquivo "cache4.db"

(que é notoriamente de conhecimento de todo *hacker*), única prova tecnicamente confiável, a despeito de juridicamente ilícita, da qual é possível extrair o conteúdo de mensagens trocadas pelo referido aplicativo. Portanto, se for um *hacker* a fonte anônima que o *Intercept Brasil* alega que lhe entregou as mensagens atribuídas ao ex-juiz Sergio Moro e ao procurador Deltan Dallagnol, o site poderia, a bem da verdade e do bom jornalismo, pedir uma cópia do referido arquivo "cache4.db" e entregá-lo a um órgão independente para perícia e depois divulgar o resultado dessa perícia; ou, no mínimo, divulgar os reais arquivos digitais recebidos da alegada fonte anônima como sendo das mensagens trocadas pelo aplicativo Telegram entre as pessoas citadas nas notícias, para que o público com um pouco mais de conhecimento de tecnologia da informação possa examiná-los quanto à veracidade do que foi publicado como sendo as referidas mensagens. Assim procedendo, o *Intercept Brasil* faria um enorme bom serviço ao Brasil e ao povo brasileiro.

Realmente, o que não é jurídica, social e moralmente aceitável, não somente por se tratarem de questões que afetam a dignidade, a honra e, principalmente, a liberdade de várias pessoas, inclusive algumas atualmente presas, é a continuidade desse sensacionalismo feito por site estrangeiro, com a divulgação de meras imagens — que nem mesmo são de telas do aplicativo Telegram dos citados nas reportagens —, e que, por isso, são tecnicamente um "nada" em termos de prova (a despeito da ilicitude jurídica); mas que são alardeadas como sendo de mensagens trocadas pelo aplicativo Telegram, alegação que vinha sendo aceita até agora de forma servil, acrítica, sem qualquer reflexão ou questionamentos, em razão não só da credulidade, mas, principalmente, da ignorância da quase totalidade da população brasileira, inclusive das mais altas autoridades da República, sobre questões técnicas de tecnologia da informação, tais como o funcionamento do aplicativo Telegram.

Isso porque, como disse Umberto Eco em 2015, "a Internet pode ter tomado o lugar do mau jornalismo... Se você sabe que está lendo um jornal como EL PAÍS, La Repubblica, Il Corriere della Sera..., pode pensar que existe um certo controle da notícia e confia. Por outro lado, se você lê um jornal como aqueles vespertinos ingleses, sensacionalistas, não confia. Com a Internet acontece o contrário: confia em tudo porque não sabe diferenciar a fonte credenciada da disparatada. Basta pensar no sucesso que faz na Internet qualquer página web que fale de complôs ou que invente histórias absurdas: tem um acompanhamento incrível, de internautas e de pessoas importantes que as levam a sério"[10].

[1] O domínio "theintercept.com" não é brasileiro e foi registrado no EUA em nome de "GoDaddy.com, LLC", conforme é possível verificar isso em https://whois.net. Acesso em 1º/7/2019.
[2] Inclusive, nesse sentido, chegou-se até mesmo a, açodadamente, se fazer representação disciplinar no CNMP contra o procurador Deltan Dallagnol, o que nos parece juridicamente teratológico, por razões que não iremos aqui discutir.
[3] *Observações sobre a eficácia probatória do e-mail no processo civil brasileiro*, **Coleção Doutrinas Essenciais Processo Civil.** Vol. IV. São Paulo: RT, 2014, pp. 697/724.
[4] "Registre-se, ainda, que a reprodução de tela de computador é facilmente editável" (TJSP, 12.ª Câmara de Direito Privado, Ap. n.° 1004885-39.2015.8.26.0576, rel. Des. Ramon Mateo

Júnior, DJe 07/06/2017).
"A juntada de mera impressão de tela de computador, para comprovar a contratação, não tem valor probante" (TJMG, 13.ª Câmara Cível, Ap. n.° 0000303-73.2016.8.13.0694, rel. Alberto Henrique, DJe 02/06/2017).
“A existência de simples e parciais impressões de telas, desprovidas de indicativos de origem, não se prestam como prova mesmo indiciária para arrimar uma acusação criminal" (TJSP, 14.ª Câmara de Direito Criminal, Ap. n.° 2172998-52.2014.8.26.0000, rel. Des. Marco de Lorenzi, DJe 30/04/2015).
No âmbito jurisprudencial, a mera impressão de tela, seja de computador, seja de celulares, é majoritariamente refutada como prova, quando desacompanhada de outros elementos probatórios mais confiáveis, tais como a ata notarial.
[5] https://www.migalhas.com.br/dePeso/16,MI34620,91041-Provas+no+ambito+digital+O+desafio+da+preservacao+adequada. Acesso em 1º/7/2019.
[6] https://play.google.com/store/apps/details?id=com.eL.FakeChats&hl=pt_BR; https://apps.apple.com/br/app/fakechat/id1374527964?l=en.
[7] Com 74,45% do mercado mundial em 2018, contra com 22,85% do iOS da Apple, sendo os 2% restantes por outros sistemas operacionais, tais como o próprio Windows.
[8] Nesse sentido, SATRYA, Gandeva; DAELY, Philip; ARIEF, Muhammad. *Digital Forensic Analysis of Telegram Messenger on Android Devices*. Apresentação no International Conference on Information & Communication Technology and Systems (ICTS), outubro de 2016, em Surabaya, Indonesia.
O aplicativo WhatsApp faz uma armazenagem semelhante, no diretório denominado “data/data/com.whatsapp/databases/”, basicamente em quatro arquivos: “msgstore.db”, “wa.db” e “axolotl.db”, “chatsettings.db”.
[9] Nesse sentido, confira em https://blog.zimperium.com/telegram-hack. Acesso em 1º/7/2019.
[10] https://brasil.elpais.com/brasil/2015/03/26/cultura/1427393303_512601.html.