Bloqueio do WhatsApp não resolve nenhum problema da investigação

A velocidade com que as tecnologias progridem em sua *usabilidade* nem sempre são acompanhadas pelos profissionais e cientistas (se nos permitirem o uso do termo) do Direito. É o que Virilio, na análise da dromologia do tempo, tentou demonstrar. Os atores judiciários não acompanham a velocidade social e as novas tecnologias, tendo assim imensa dificuldade em obter provas em comunicadores como o WhatsApp, pensando ainda (erroneamente) na lógica das interceptações telefônicas. Sem falar no profundo desconhecimento técnico acerca da forma como a comunicação é realizada.

A decisão da 2ª Vara Criminal de Duque de Caxias apontou dentre seus fundamentos uma interessante singeleza mandamental — descumprida, anteriormente, segundo o mesmo juízo, outras três vezes: "*Em verdade, o Juízo requer, apenas, a desabilitação da chave de criptografia, com a interceptação do fluxo de dados, com o desvio em tempo real em uma das formas sugeridas pelo MP, além do encaminhamento das mensagens já recebidas pelo usuário e ainda não criptografadas, ou seja, as mensagens trocadas deverão ser desviadas em tempo real (na forma que se dá com a interceptação de conversações telefônicas), antes de implementada a criptografia.*"

Logo, a decisão exigia:
1. A desabilitação do sistema de criptografia das mensagens trocadas entre determinados interlocutores do WhatsApp (supostos autores das infrações penais investigadas) cumulada com o espelhamento de dados por um terceiro (interceptação propriamente dita);
2. A disponibilização das mensagens, preteritamente trocadas entre os mesmos usuários, e, eventualmente, ainda não criptografadas.

Apesar da sutil e aparente singeleza do advérbio de exclusão contido na polêmica decisão ("requer, *apenas*"), em se tratando de ligações de VoIP — estamos falando, portanto, em interlocuções de dados no formato de voz, como aquelas feitas pelo Whatsapp — e, também, de comunicações por dados — por exemplo, por troca de mensagens simples de texto do aplicativo — a interceptação, tal qual sua instrumentalização processual, não é tão simples como aquela da telefonia usual (física).

Mesmo diante da obrigatoriedade de armazenamento de registros por seis meses impostas aos servidores de conteúdo pelo artigo 15 do Marco Civil (Lei 12.965/2014), os dados armazenados no WhatsApp, desde abril, e desde que os interlocutores tenham a versão mais atualizada do aplicativo, estarão criptografados. Ou seja, o seu conteúdo só será acessível e interpretável se o usuário final possuir uma *chave* (*cipher key*) que soluciona o *segredo* de um algoritmo de criptografia (ponto a ponto, ou seja, de dispositivo a dispositivo). Logo, quando duas pessoas trocarem informações pelo aplicativo, o remetente e o destinatário receberão e armazenarão uma mesma *chave*. As mensagens antes de serem enviadas para o destinatário com *ela* serão criptografadas pelo remetente. O destinatário, ao receber o conteúdo criptografado, *a* usará para descriptografar e ler o real conteúdo da mensagem. Logo, o interceptador, terceiro que *escuta* o diálogo, poderá até obter a informação enviada, mas sem a *chave* não conseguirá saber o que nela está contido (a informação estará ininterpretável e será constituída de caracteres estranhos e desconexos).

2023 - www.conjur.com.br - Todos os direitos reservados.

Restariam as questões: conseguiriam os órgãos de segurança pública e seus setores periciais, sem a *chave* , descriptografar uma mensagem *armazenada* e/ou *interceptada*? Ou ainda, seguindo o comando contido na decisão de ontem, poderiam os mesmos órgãos — ou quem sabe, o próprio detentor do aplicativo. — obter a desabilitação da criptografia em determinados dispositivos (mais especificamente, daqueles em posse dos supostos autores de infrações penais em investigação)?

A resposta à primeira indagação (possibilidade de descriptografar-se um texto sem o uso da *chave* correta) é: talvez, com processos de força bruta (tentativa e erro) e com equipamentos avançados, mas levaria anos de esforços. O problema é que a criptografia utilizada no WhatsApp envolve a combinação de diferentes criptoalgoritmos — *Off the Record* (OTR), *Perfect Forward Secrecy* (PFS) e o *Double Ratchet Algorithm* (DRA) — o que dificulta, e muito, o trabalho de sua *quebra* por setores periciais especializados em crimes cibernéticos.

A origem da reiterada contenda judicial, porém, está na segunda pergunta (possibilidade de desabilitação da criptografia). A resposta aqui dependerá da análise do modo como se tentará implementar a desabilitação: se pelo *lado do cliente* (*client side*), ou seja, pelo *desativamento* diretamente no dispositivo que se quer interceptar, ou pelo *lado do servidor* (*server side*), isto é, pela inabilitação da criptografia diretamente no provedor de serviço e conteúdo (*Whatsapp*).

Pelo *client side*, a menos que se tenha privilégios suficientes (de administrador) e acesso (remoto ou físico) ao dispositivo, a alteração não é viabilizada, permitida ou disponibilizada pelo aplicativo. Logo, mesmo querendo, o usuário final ou terceiros não poderão desativar a criptografia diretamente no dispositivo, a menos que haja um processo de desativação por meio de edição do código do aplicativo (o que se impossibilitaria pela simples compilação final do *software* e pela inexistência de tal opção no código fonte originário). Logo, a resposta à pergunta aqui é: não, não é possível.

No lado do servidor (*server side*), apesar de maiores as possibilidades de obtenção de desabilitação pretendida, tal objetivo demandaria, possivelmente, o implemento de um *backdoor* nas futuras versões do WhatsApp. Um *backdoor*, ou uma porta de fundos, seria uma espécie de *brecha* controlada (controlável) pelo provedor de conteúdo, ou por quem fizesse as suas vezes, criada propositalmente para se acessar (leia-se invadir) um dispositivo alvo, por exemplo, de uma interceptação telemática. O sujeito alvo dessa investigação, e invasão, provavelmente, não teria ciência do acesso (des)autorizado a seu dispositivo e a criptografia de suas mensagens, em tese, poderia — se o código fonte e a compilação final da nova versão, silenciosamente, assim viabilizassem — ser desligada. A solução, contrariando a sutileza da decisão judicial, entretanto, não é, como se imagina, tão simples assim.

A possibilidade de se explorar um *backdoor* em um comunicador, por mais que se utilize a lógica reducionista e utilitarista da persecução penal (de que *os fins justificam os meios)*, colocaria, sim, em xeque, a segurança de milhões de usuários no Brasil, já expostos, diariamente, aos mais diversos riscos da criminalidade *online*, em especial, o mais recente e custoso, sequestro de arquivos (*file hijacking*). Além disso, a vulnerabilização deliberada, propositalmente criada tendo em vista os fins do utilitarismo da persecução penal, excluída a minoria que faz uso do aplicativo para fins ilícitos, espancaria a

2023 - www.conjur.com.br - Todos os direitos reservados.

credibilidade de um aplicativo que se diz seguro e, ao mesmo tempo, afrontaria as garantias fundamentais constitucionais da liberdade de expressão e comunicação (artigo 5º, inciso IX, da Constituição Federal).

Portanto, o juízo de ponderação, tal qual aquele concretizado pelo juízo da 2ª Vara Criminal de Duque de Caxias, de que "a finalidade pública da persecução criminal sempre deverá prevalecer sobre o interesse privado da empresa em preservar a intimidade e privacidade de seus usuários, assim como também deverá prevalecer sobre os interesses desses últimos" mereceria maior atenção e deveria ser realizado, cautelosamente, com amparo nas garantias constitucionais individuais — com observância, em especial, no impacto causado a milhões de usuários que, na sua maciça maioria, utilizam o aplicativo para fins permitidos em lei — e na proporcionalidade e razoabilidade do decreto de tão gravosa decisão, sob risco de estarmos diante de um ato de censura generalizada *online*.

Da simples análise das questões pontuais acima apresentadas, hoje, diante do uso de novos instrumentos de comunicação, como o *WhatsApp*, já não basta mais à investigação criminal que se *intercepte* e *armazene* (dados). Será preciso, ainda, descriptografá-los. E para que se descriptografe a informação, como visto, se impossibilitada a desabilitação da algoritmocriptografia (pelo *client* ou *server side*), será necessário o acesso à *chave* de codificação/embaralhamento, ou, se decidido pelo método do *ataque à bruta força* (*brute-force cryptanalytic attack)*, tempo, muito tempo. Mas afinal de contas, diante do segredo criptográfico, onde estaria a tal *chave* (*cipher key*) que garantiria o acesso às mensagens trocadas?

Primeiro ponto a ser compreendido: o bloqueio do serviço no Brasil é ineficaz, pois a *chave* que garante o sigilo da comunicação está no celular dos interlocutores. Para ter acesso a ela é preciso que o usuário tenha privilégios suficientes (geralmente de administrador) no(s) aparelho(s) em que ela, a *chave*, está armazenada.

Então, façamos a seguinte pergunta: se houver *interceptação* e *armazenamento*, pelo órgão executor, de dados criptografados do WhatsApp, poderíamos buscar o *segredo* nos servidores do aplicativo ou exigir, da empresa proprietária, a *chave* comungada entre os interlocutores? A resposta parece-nos negativa, pois tais *chaves* estão, como visto, armazenadas nos dispositivos dos usuários e não nos servidores de serviço de conteúdo do aplicativo.

Logo, para que a interceptação de dados criptografados do WhatsApp possa servir à investigação, ressalvada a hipótese de desabilitação de criptografia — a nosso ver, inaplicável e incabível, pelo menos por ora — seria preciso além da *interceptação* e do *armazenamento*, a entrega, pela empresa proprietária, da *chave* utilizada pelos seus usuários. Fora desse cenário, o que se obterá serão informações ininterpretáveis (criptografadas).

O bloqueio do WhatsApp em âmbito nacional, expondo milhões de usuários a limites na sua comunicabilidade é ineficaz, inócuo e imprestável para os próprios fins da investigação. A desabilitação da criptografia do sistema de comunicação do WhatsApp, por meio da implementação/instalação de *backdoor*, de igual modo, além de medida drástica a implicar a alteração da política de privacidade do aplicativo e seu código fonte futuro, representaria, a nosso ver, afronta, direta, às garantias fundamentais constitucionais da inviolabilidade de dados (artigo 5º, inciso XII, da Constituição Federal) e da liberdade de expressão e comunicação (artigo 5º, inciso IX, da Constituição Federal), e também da garantia da

2023 - www.conjur.com.br - Todos os direitos reservados.

liberdade de expressão, comunicação e manifestação de pensamento e privacidade prevista no Marco Civil (artigo 3º, inciso I e II, da Lei 12.965/14). Uma possível solução para o impasse residiria na obtenção, *a posteriori*, mediante busca e apreensão judicial, dos dispositivos que tiveram as mensagens interceptadas e que contêm a *chave* com o algoritmo criptográfico apto a revelar o conteúdo desejado para a instrução criminal.

Date Created
22/07/2016

2023 - www.conjur.com.br - Todos os direitos reservados.