Investida europeia contra criptografia dos e-mails e pesca probatÃ³ria

A notícia de que o conteúdo das comunicações, via *Whatsapp*, seriam compartilhados com a gigante *Facebook*, causou alvoroço por significar a evidência de invasão de privacidade. O sentimento de injustiça “comoveu” as redes sociais. A sensação de se dispõe de privacidade, contudo, não passa de ingenuidade tecnológica. Os dispositivos (celular, veículos, auxiliares domésticos, computadores, relógios, enfim, todo o potencial da "internet das coisas") que se utiliza diariamente disparam dados sobre os usuários, sem que se saiba o destino e para que(m) servem. Mas o contexto sempre pode ficar

Na era digital, ao velho debate entre liberdade e segurança, somou-se um terceiro elemento: a privacidade. Resta, assim, de um lado a privacidade e a liberdade, do outro a segurança (mas apenas na faceta de *security*, pois a *safety* está mais próxima dos dois primeiros). Por força dos escândalos com vazamentos de dados de todos os lados (redes sociais, órgãos públicos, empresas privadas, empresas públicas etc.), os parlamentos europeus recentemente voltaram a discutir os limites da criptografia de dados. Os inimigos da vez são os servidores de e-mail que operam com protocolos E2E (*end to end*), ou seja, têm acesso ao conteúdo das mensagens apenas o emissor e o receptor (Lomas, 2021). Os servidores de E2E são uma opção para quem deseja ter privacidade, pois não deixam portas dos fundos (*backdoor*) por meio das quais é possível acessar as contas dos usuários e ler as mensagens das caixas. Tampouco é possível armazenar uma cópia das mensagens enviadas e recebidas para fins de cumprimento de ordens judiciais. Justo por isso são tão visados.

Pode parecer que se trata de uma relevante questão de segurança pública e até mesmo de segurança nacional. É exatamente assim que os parlamentares europeus querem que se pense. A justificativa é, como sempre, a necessidade. Há um risco, tem-se medo, então é necessário agir. Direitos, nessa concepção, são obstáculos a transpor. O terrorismo opera como carta coringa no baralho parlamentar. Para evitar que terroristas promovam ataques em território europeu, é imperioso instalar uma porta dos fundos nos servidores de e-mail criptografados. Na investida atual, as palavras são escolhidas cuidadosamente, pois as tentativas anteriores foram frustradas por conta, dentre outros motivos, da má escolha das palavras.

Contudo, a questão central não é o risco de terrorismo, mas sim as consequências da proposta. A instalação de uma *backdoor* nos servidores possibilita o monitoramento constante das mensagens. O ato seguinte é criar para os servidores o dever de fiscalizar o tráfego e comunicar atos suspeitos, como já ocorre nos EUA por força do *Cloud Act* (MORAIS DA ROSA; VIEIRA, 2019). Todas as vezes que utilizamos o Gmail, o Yahoo, a Apple etc., estamos submetidos às regras americanas, mesmo não morando lá (apertamos o "concordo" dos Termos e Condições de uso), pelas quais as máquinas e/ou os humanos podem monitorar o conteúdo das comunicações, enfim, realizar "pescaria probatória" que, significa a "investigação especulativa indiscriminada, sem objetivo certo ou declarado, que 'lança' suas redes com a esperança de 'pescar' qualquer prova, para subsidiar uma futura acusação. Ou seja, é uma investigação prévia, realizada de maneira muito ampla e genérica para buscar evidências sobre a prática de futuros crimes. Como consequência, não pode ser aceita no ordenamento jurídico brasileiro, sob pena de malferimento das balizas de um processo penal democrático de índole Constitucional" (SILVA, MELO E SILVA, MORAIS DA ROSA, 2019).

Por outro lado, chega-se ao ponto de que não será possível, de nenhum modo, ter uma conversa privada, ou seja, das três esferas da privacidade, talvez não se tenha mais direito nem a ter uma que abranja a esfera violável excepcionalmente (privacidade), quem dirá as esferas invioláveis (intimidade e segredo).

Trata-se do equivalente aos mandados de busca e apreensão coletivos ou de *fishining expedition*. Aqueles mesmos, criticados há décadas, que ocorrem apenas nas comunidades carentes, mas agora com potencialidade para atingir a todos os possuidores de contas de e-mails. Não está em jogo apenas a criptografia daqueles quatro servidores, mas de todos os servidores. Tudo a pretexto de combate ao crime, mas com uma agravante: sequer é necessária a prévia decisão judicial (reserva de Jurisdição). A legislação dá conta de criar o equivalente ao *Big Brother* de 1984, com câmeras dentro das casas, algo já antecipado por Snowden.

A grande vantagem da captação de dados de *e-mails*, para a persecução penal (consequentemente, a grande desvantagem para os imputados), é a possibilidade de se obter informações que dificilmente poderiam ser obtidas no período anterior à informatização. Algo comezinho parece ter sido esquecido pelos juristas: aqueles rastros digitais não existem fora do ambiente computacional, de modo que crimes praticados sem registros digitais não podem ser provados da mesma forma — talvez sequer deixem provas. Não há porque admitir que se obtenha dados irrestritamente de contas de *e-mail*, fornecidos pelos respectivos servidores, se em situação análoga, em que a comunicação foi pessoal ou por meio de cartas/bilhetes, não seria possível produzir prova. Trata-se de invasão abusiva do conteúdo privado, da vida cotidiana das pessoas, manipulado sob o argumento dissimulado de combate ao terrorismo que, uma vez obtidos, podem ser "compartilhado" entre os governos, transformando o mundo em uma grande piscina, em que nenhum de nós sequer poderá suspirar sem que alguém saiba, portanto,

de prova ilícita, na medida em que extrapola os limites jurídicos de produção.

REFERÊNCIAS

LOMAS, Natasha. ProtonMail, Threema, Tresorit and Tutanota warn EU lawmakers over ‘anti-encryption’ push. **TechCrunch**, 27 jan. 2021. Disponível em: https://techcrunch.com/2021/01/27/protonmail-threema-tresorit-and-tutanota-warn-eu-lawmakers-against-anti-encryption-push. Acesso em: 04 fev. 2021.

MORAIS DA ROSA, Alexandre; VIEIRA, Marília Raposo. Cloud Act: Quando a investigação se dá nas nuvens americanas. **Consultor Jurídico**, São Paulo, 22 nov. 2019. Disponível em: https://www.conjur.com.br/2019-nov-22/limite-penal-cloud-act-quando-investigacao-nuvens-americanas. Acesso em: 04 fev. 2021.

SILVA, Viviani GHIZONI; MELO E SILVA, Philipe Benoni; MORAIS DA ROSA, Alexandre. Fishing Expedition e Encontro Fortuito na Busca e Apreensão. Florianópolis: EMais, 2019