SEGURANÇA PÚBLICA E DADOS PESSOAIS: ALGUMAS PALAVRAS SOBRE OS CASOS FBI X APPLE E JUSTIÇA X FACEBOOK

Desde quando Edward Snowden (ex-analista de sistemas da CIA e da NSA) revelou detalhes dos programas de vigilância da NSA a confiança das pessoas nas instituições foi abalada de forma importante. Isso porque o esquema teria envolvido renomadas empresas privadas (como Google, Facebook, Apple, Microsoft, Yahoo, entre outros) e, ainda, entidades governamentais de cinco países num grupo intitulado “Five Eyes” (FVEY), composto pela Agência Nacional de Segurança dos Estados Unidos (NSA), pela Sede de Comunicações do Reino Unido (GCHQ), pelo Escritório de Segurança das Comunicações do Canadá (CSEC), pelo Diretório de Informações Australiano (ASD) e pelo Escritório Governamental de Segurança das Comunicações da Nova Zelândia (GCSB). Com uma estrutura de vigilância deste porte, era natural que as pessoas se sentissem traídas, enganadas.

Neste contexto, para que as empresas pudessem colaborar com os governos sem prejuízo para seus negócios em face da revolta de seus clientes, seria preciso não assumirem abertamente a condição de integrantes de um esquema de vigilância. A saída para isso foi a adoção de tecnologias de segurança da informação mais complexas que – ao menos virtualmente – nem mesmo as empresas pudessem violar. Em outras palavras, a forma pela qual as empresas entenderam que não perderiam clientes a despeito de colaborem com a espionagem foi o investimento (no marketing?) da tecnologia segura.

Sob esta óptica é que se deve analisar o caso FBI x Apple, que ganhou repercussão mundial. Vamos ao caso.

Em 02 de dezembro de 2015, em San Bernardino (CA) houve um atentado ultimado por um casal de atiradores – Syed Farook, de 28 anos, e Tashfeen Malik, de 27 anos – que resultou em catorze mortos e dezessete feridos. O local onde houve o tiroteio – Inland Regional – é o departamento público de saúde onde Farook trabalhava como inspetor de saúde e onde ocorria uma festa.

Próximo aos atiradores foram encontradas nada menos que doze bombas caseiras, cinco mil balas de munição de calibre 22 e material para confecção de artefatos explosivos. Além disso, foi encontrado um iPhone 5C no veículo utilizado pelos atiradores para fugirem da polícia antes de serem mortos. O contexto sugere que o ataque tenha sido um ato terrorista, motivo pelo qual, com mais razão, a investigação pretendeu ter acesso ao conteúdo do iPhone de Farook.

Esse é o ponto fulcral da história.

O governo norte-americano pediu que a Apple fornecesse dados de Farook, o que foi atendido pela empresa. Tratavam-se de dados cadastrais do atirador.

No entanto, o pedido não parou por aí... O governo passou a requerer que a Apple "desbloqueasse" o iPhone para que a polícia tivesse acesso ao conteúdo de possíveis mensagens que auxiliassem na investigação e até mesmo na localização de outros envolvidos (algumas testemunhas disseram ter visto três pessoas agindo no massacre). Ocorre que o "desbloqueio", na verdade, se trata de um pedido para que a Apple crie uma nova versão do software do iPhone (iOS), contornando vários recursos de segurança e instalando-o no aparelho recuperado pela polícia. E isso a Apple se negou a fazer alegando que a criação de uma versão do software nestes termos seria equivalente à criação de uma backdoor (um brecha sistêmica) que poderia vir a ser utilizada para acesso em qualquer outro iPhone. Ou seja, caso fosse criada a versão requerida, em tese, o governo norte-americano poderia acessar qualquer iPhone no mundo. Com isso estava armada a confusão e a dicotomia entre segurança pública/nacional x privacidade.

Mas, afinal, a Apple tem como desbloquear o iPhone ou não?

Para responder esta pergunta é preciso compreender que nas versões mais atuais do sistema iOS há um conjunto de chaves de criptografia que depende da inserção da senha do usuário. Em outras palavras, o aparelho não identifica qual é a chave até que a senha seja inserida porque a mesma só existirá no aparelho após informada. Não há como decodificar os arquivos sem esta senha, que, portanto, traz consigo uma das chaves criptográficas. Assim, é mais fácil (ou menos difícil) obter os dados de um telefone que nunca foi desligado e que já se encontra desbloqueado (porque a chave criptográfica está na memória).

Não fosse um erro infantil do FBI esta história não seria tão longa. Depois que o aparelho é desligado ou tem sua bateria esgotada, a chave criptográfica sai da memória, só podendo ser resgatada com a senha. Além disso, o FBI tentou alterar a senha do serviço iCloud, o que impediu que o telefone sincronizasse dados com a nuvem (e tais dados poderiam constituir indícios ou provas do crime).

Em suma, a Apple não tem a chave criptográfica e não tem como associá-la ao aparelho. Ademais, redefinir a senha não auxilia em nada porque a chave

criptográfica ficou associada à senha antiga. Trata-se de sistema desenvolvido pela Apple após as revelações de Edward Snowden. A discussão é, portanto, complexa.

Em face disso tudo, o governo norte-americano pleiteou ao Judiciário que determinasse que a Apple criasse a backdoor. Uma juíza federaldeferiu o requerimento, determinando que a empresa forneça assistência técnica razoável na busca de prover ao FBI os dados pleiteados. A Apple, por eu turno, apelou de decisão. Não há uma decisão definitiva sobre essa questão, restando a seguinte dúvida: o que deve prevalecer? A segurança do sistema e os dados pessoais? Ou a segurança nacional? Parece que ambas as partes tem bons argumentos.

Veja-se que o caso norte-americano é diferente do recente caso brasileiro onde o magistrado determinou a prisão do Vice-Presidente do Facebook no Brasil porque a empresa não teria colaborado atendendo determinação judicial para fornecer, ao juízo, dados de supostos criminosos.

No caso brasileiro os autos encontram-se sob sigilo, de modo que os dados conhecidos são os noticiados pela mídia: uma nota publicada pelo Tribunal de Justiça de Sergipe (de onde foi proferida a decisão de prisão) e comentários dos advogados do Facebook. Ocorre que, nem um, nem outro, esclarecem de fato o que aconteceu. Há algumas inconsistências nas manifestações sobre o caso, mas algumas coisas são de comentários possíveis.

A ordem de prisão decorreu de processo de natureza criminal onde se investiga crimes de tráfico de drogas e de organizações criminosas. Neste contexto, incide a lei nº 12.850/13 que trata justamente das organizações criminosas. Mencionada lei, no art. 2º, §1º determina que são punidos com penas de três a oito anos de reclusão e multa “quem impede ou, de qualquer forma, embaraça a investigação de infração penal que envolva organização criminosa”. O magistrado sergipano não teve dúvidas e interpretou o artigo acima mencionado de forma literal, imputando ao Vice-Presidente conduta criminosa e determinando sua prisão sob o argumento de que até multas diárias altíssimas haviam sido impostas e, mesmo assim, a ordem judicial não teria sido cumprida.

Mas o caso brasileiro é curioso justamente porque não tivemos acesso aos autos e, portanto, não podemos concluir se o juiz requisitou informações de fornecimento (im)possível ou se a requisição foi feita com precisão sobre o que se deseja. Por outro lado, não se justifica a negativa de cumprimento de ordem judicial, a menos que plenamente justificada, o que não parece ter sido o caso.

Por outro lado, cabe, ainda, perquirir as razões pelas quais a empresa não teria esclarecido a impossibilidade do fornecimento. Afinal, o não cumprimento de ordem judicial somente se justifica apenas em razão da sua impossibilidade. Como teria a empresa respondido ao ofício? Ou jamais ofereceu qualquer resposta?

Como não temos o acesso aos autos, as questões acima ficarão pendentes de esclarecimentos…

Fato é que estamos em tempos de grandes questionamentos sobre segurança digital em conflito com segurança nacional, social. O mundo avança com tecnologias cada vez mais sofisticadas, mas as leis não acompanham este dinamismo. Algo precisa ser feito com rapidez para que situações como estas sejam evitadas. Isso não significa dizer que apenas as empresas tenham que ajustar, sendo fundamental que os governos prevejam formas mais dinâmicas de aplicação das suas leis resguardando os direitos fundamentais dos cidadãos.

Coriolano Aurélio de Almeida Camargo Santos – Diretor Titular Adjunto do Dejur

Marcelo Crespo - Membro do subgrupo de Direito Digital da FIESP