A polícia pode forçar alguém a desbloquear o dispositivo móvel celular em uma busca pessoal?

Já se imaginou em uma situação em que você estava na rua e, durante uma busca, os policiais te obriguem a desbloquear o celular?

A questão tem gerado debates, tanto nas cortes brasileiras como dos Estados Unidos, conforme detalharemos a seguir.

Nos Estados Unidos, durante o início das discussões se a conduta dos policiais violava a quinta emenda, que veda a autoincriminação, os tribunais começaram a entender que as impressões digitais e o reconhecimento facial não se enquadravam no conceito de senha.

É posição da EFF (*Eletronic Forntier Foundation)* que a descriptografia forçada, seja por senha biométrica ou alfanumérica, deve ser protegida pela quinta emenda porque a descriptografia é sempre testemunhal. A recomendação dos especialistas é que jamais se utilizasse apenas a biometria, mas uma senha forte.

No entanto, o entendimento dos tribunais está mudando e alguns julgados já entendem que obrigar o desbloqueio de um dispositivo usando dados biométricos é uma violação dos direitos da quinta emenda. Assim, os mecanismos biométricos de login passam a ter a mesma proteção. Juízes já entendem que impressões digitais e varreduras de rostos não são o mesmo que evidências físicas e, portanto, policiais não têm o direito de forçar suspeitos a se incriminarem.

Nesse sentido, em 2014, no caso *Riley vs. Califórnia,* a

Suprema Corte dos Estados Unidos decidiu pela necessidade de prévia ordem judicial para que a polícia pudesse validamente acessar o conteúdo de aparelhos celulares apreendidos em buscas incidentais e prisões.

Também em 2019, numa decisão histórica, uma juíza da Califórnia determinou que as autoridades não podem obrigar suspeitos a desbloquear o seu próprio smartphone usando impressão digital ou reconhecimento facial. Ainda, declarou que o governo não tinha o direito, mesmo com um mandado, de forçar os suspeitos a se incriminarem, destrancando seus dispositivos com suas características biológicas.

Em relação ao ato de forçar os fabricantes a destravarem os dispositivos, é importante destacar que a Apple e outros fabricantes têm resistido ao desbloqueio forçado.

Em 2016, o FBI, por meio de uma ordem judicial, obrigou a Apple a desbloquear o iPhone de Syed Rizwan Farook, o atirador falecido em um ataque terrorista em dezembro de 2015 em San Bernardino, na Califórnia (EUA).

A Apple alega que utiliza a criptografia para proteger os dados pessoais dos clientes porque acredita que é a única maneira de manter suas informações seguras.

Tim Cook, CEO da Apple, em uma carta aberta (https://www.apple.com/customer-letter/), diz que "não tem simpatia por terroristas", e que a Apple, normalmente, coopera com pedidos oficiais para dados aos quais ela tem acesso.Contudo, o FBI quer que a Apple faça uma nova versão do sistema operacional do iPhone, contornando vários recursos de segurança importantes, e o instale em um iPhone recuperado durante a investigação.

No Brasil, o tema também já chegou nas cortes.

O Supremo Tribunal Federal, iniciou a discussão do Tema 977 da Repercussão Geral: "aferição da licitude da prova produzida

durante o inquérito policial relativa ao acesso, sem autorização judicial, a registros e informações contidos em aparelho de telefone celular, relacionados à conduta delitiva e hábeis a identificar o agente do crime". O tema está em discussão no Recurso Extraordinário nº 1.042.075, da relatoria do ministro Dias Toffoli, que ainda não foi julgado.

O caso vem do Rio de Janeiro, onde o Tribunal de Justiça absolveu acusado por considerar ilícita a prova produzida após apreensão de seu telefone e acesso ao registro de chamadas e contatos, sem ordem judicial.

No STF, o relator Dias Toffoli entendeu que é lícita a prova obtida com o acesso a registro telefônico ou agenda de contatos do celular mesmo sem autorização judicial, por não configurar ofensa ao sigilo das comunicações, à intimidade ou à privacidade do acusado.

Contudo, há divergência já que os ministros Gilmar Mendes e Edson Fachin entenderam que a verificação dos dados contidos nos celulares depende de "prévia decisão judicial que justifique, com base em elementos concretos", a necessidade e adequação da medida, bem como "delimite a sua abrangência".

O caso, no entanto, não enfrenta, diretamente, o acesso forçado de policiais à senha ou a coação para que o suspeito destrave o equipamento.

No Superior Tribunal de Justiça, no Habeas Corpus nº 89.981/MG, a corte entendeu que o acesso a mensagens de WhatsApp, sem autorização judicial, fere o inciso X do art. 5º da Constituição Federal, e no caso determinou o desentranhamento das conversas do mensageiro dos autos.

No mesmo sentido, o STJ decidiu no Recurso em Habeas Corpus nº 101.119/SP, em dezembro de 2019:

RECURSO EM HABEAS CORPUS. TRÁFICO DE DROGAS. PRISÃO EM FLAGRANTE.**ACESSO A DADOS CONTIDOS NO CELULAR DO RÉU. AUSÊNCIA**

DE PRÉVIA AUTORIZAÇÃO JUDICIAL. ILICITUDE DAS PROVAS OBTIDAS. RECURSO EM HABEAS CORPUS PROVIDO. 1. Os dados armazenados nos aparelhos celulares – envio e recebimento de mensagens via SMS, programas ou aplicativos de troca de mensagens, fotografias etc. -, por dizerem respeito à intimidade e à vida privada do indivíduo, são invioláveis, nos termos em que previsto no inciso X do art. 5º da Constituição Federal, só podendo, portanto**, ser acessados e utilizados mediante prévia autorização judicial, com base em decisão devidamente motivada que evidencie a imprescindibilidade da medida, capaz de justificar a mitigação do direito à intimidade e à privacidade do agente**. 2. No caso, por ocasião da própria prisão em flagrante – sem, portanto, a prévia e necessária autorização judicial -, **o celular do réu foi apreendido, desbloqueado e nele verificada a existência de mensagens de texto que indicavam prévia negociação da venda de entorpecentes, sem, portanto, a prévia e necessária autorização judicia**l. A autorização do juiz deferindo a quebra do sigilo das informações e das comunicações (como aplicativos, fotografias e demais dados armazenados nos aparelhos de telefonia apreendido) somente foi feita em momento posterior, já na audiência de custódia e, mesmo assim, sem nenhuma fundamentação concreta que evidenciasse a imprescindibilidade da medida. 3. Pelos documentos constantes dos autos, não se verifica nenhum argumento ou situação que pudesse justificar a necessidade e a urgência, em caráter excepcional, de as autoridades policiais poderem acessar, de imediato (e, portanto, sem prévia autorização judicial), os dados armazenados no aparelho celular do recorrente.Ao contrário, pela dinâmica dos fatos, o que se depreende é que não haveria nenhum prejuízo às investigações se os policiais, após a apreensão do telefone celular, houvessem requerido judicialmente a quebra do sigilo dos dados nele armazenados. 4. A denúncia se apoiou em elementos obtidos a partir da apreensão do celular pela autoridade policial, os quais estão reconhecidamente contaminados pela forma ilícita de sua colheita. Não é possível identificar, com precisão, se houve

algum elemento informativo produzido por fonte independente ou cuja descoberta seria inevitável, porquanto o contexto da abordagem do ora recorrente aliado à quantidade de drogas apreendidas e aos dados obtidos por meio do acesso ao celular do agente é que formaram a convicção do Parquet pelo oferecimento de denúncia pela possível prática do crime previsto no art. 33, caput, da Lei n. 11.343/2006. 5. A própria narrativa da dinâmica dos fatos coloca **sob dúvida o "consentimento" dado pelo réu aos policiais para o acesso aos dados contidos no seu celular, pois é pouco crível que, abordado por policiais, ele fornecesse voluntariamente a senha para o desbloqueio do celular e o acesso aos dados nele contidos. 6.** Recurso em habeas corpus provido, para reconhecer a ilicitude das provas obtidas por meio do acesso ao celular do recorrente, bem como de todas as que delas decorreram e, consequentemente, **anular** o Processo n. 0001516-27.2018 ab initio, sem prejuízo de oferecimento de nova denúncia, desde que amparada em elementos informativos regularmente obtidos. Em consequência, fica determinado o relaxamento da prisão cautelar imposta ao réu, por excesso de prazo.

(RHC 101.119/SP, Rel. Ministro ROGERIO SCHIETTI CRUZ, SEXTA TURMA, julgado em 10/12/2019, DJe 13/12/2019)

É importante mencionar que o Marco Civil da Internet (Lei nº 12.965/2014), que estabelece os princípios, garantias e deveres para o uso da internet no Brasil, dispõe, no art. 7º, que: "O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: I – inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação; II – inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei; III – inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial."

Na persecução penal, o acesso a dados pessoais de indiciados demonstra-se importante, principalmente nos crimes praticados

por organizações criminosas. Essa situação, inclusive, é uma exceção da aplicabilidade da Lei Geral de Proteção de Dados (LGPD), que prevê, nos termos do art. 4º, III, que a Lei não se aplica ao tratamento de dados pessoais realizado para fins de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais.

Por outro lado, como visto, apesar da LGPD não se aplicar, deverão ser observadas as normas constitucionais e processuais penais. Neste sentido, não nos parece lícito que policiais não só acessem conteúdos privados em dispositivos móveis, sem ordem judicial expressa, como também que constranjam ou forcem um indiciado a destravar o equipamento para fins de acesso ao conteúdo ali armazenado.

REFERÊNCIAS

https://www.forbes.com/sites/thomasbrewster/2019/01/14/feds-cant-force-you-to-unlock-your-iphone-with-finger-or-face-judge-rules/?sh=1f66cf842b76

https://gizmodo.uol.com.br/fbi-ajuda-apple-atirador-base-naval-eua/#:~:text=Em%202016%2C%20o%20FBI%20conseguiu,%2C%20na%20Calif%C3%B3rnia%20(EUA)

https://portal.stf.jus.br/processos/detalhe.asp?incidente=5173898

AUTORES

JOSÉ ANTÔNIO MILAGRE

(https://app.exeed.pro/holder/badge/55319) Data Protection Officer (DPO) EXIN. Pesquisador em direito e dados do Núcleo de Estudos em Web Semântica e Análise de Dados da USP (Universidade de São Paulo). Mestre e Doutorando em Ciência da Informação pela UNESP. Pós Graduado em Gestão de Tecnologia da Informação. Advogado com atuação em Direito Digital. Perito

Judicial em Informática e Proteção de Dados. Presidente da Comissão de Direito Digital da Regional da Vila Prudente da OAB/SP. Autor de dois livros pela Editora Saraiva (Marco Civil da Internet: Comentários à Lei 12.975/2014 e Manual de Crimes Informáticos).

LAURA SECFÉM RODRIGUES

Advogada. Pós-graduanda em Direito, Tecnologia e Inovação com ênfase em proteção de dados, no Instituto New Law. Graduada em Direito pelo Centro Universitário de Bauru/SP, mantido pela Instituição Toledo de Ensino (ITE).

EMILY LUCILA DE OLIVEIRA

Consultora especializada em Privacidade e Proteção de Dados. Gerente de Direito Digital na José Milagre & Associados. Atuação em assessment e planos de adequação para empresas e órgãos públicos do Brasil, Vice-Diretora do IDCI – Instituto de Defesa do Cidadão na Internet, entidade focada na preservação dos direitos dos usuários de internet e titulares de dados pessoais.