

STJ ordena que Google quebre sigilo de e-mails guardados nos EUA

Uma decisão da Corte Especial do Superior Tribunal de Justiça chegará até o Vale do Silício, nos Estados Unidos. Em julgamento de Questão de Ordem em Inquérito, no mês de abril, os ministros condenaram a Google Brasil a quebrar o sigilo de e-mails de um investigado de corrupção, lavagem de dinheiro e outros crimes. Para isso, a filial deve entrar em confronto com a matriz nos Estados Unidos, onde estão guardadas as informações e, pela lei, os dados não podem ser divulgados.

Segundo a companhia, seria impossível romper o sigilo do serviço de e-mails, o Gmail, sem afrontar as normas dos Estados Unidos, onde a divulgação dos dados é vedada. A defesa da Google sugeriu a alternativa diplomática para conseguir as informações, por meio do acordo de assistência judiciária em matéria penal, que vigora entre Brasil e Estados Unidos (Decreto 3.810/2001).

Outro argumento é de que a Google Brasil e a matriz americana são duas pessoas jurídicas distintas, que não compartilham bancos de dados. A filial brasileira estaria, nesse sentido, de "mãos atadas" para seguir a determinação judicial. De acordo com a defesa, a legislação americana só deixa brechas em situações de perda de vida ou graves danos físicos a terceiros.

O Ministério Público Federal, responsável pelo Inquérito 784/DF, foi o autor da Questão de Ordem ao tribunal superior. O MPF alegou que a transmissão de material entre as unidades do mesmo grupo empresarial com exclusiva finalidade de entregá-lo à autoridade judicial não viola a soberania do Estado estrangeiro. O usuário dos e-mails é investigado por formação de quadrilha, corrupção passiva e ativa, fraude à licitação, lavagem de dinheiro, advocacia administrativa e tráfico de influência.

Regras pátrias

O caso exemplifica a polêmica sobre a interferência judicial, ainda não detalhada pela legislação brasileira, para requisitar a entrega de dados virtuais. Na avaliação da ministra Laurita Vaz, que relatou o caso, a expectativa é conseguir provas na troca de mensagens pelo Gmail. “O que se pretende é a entrega de mensagens remetidas e recebidas por brasileiros em território nacional, envolvendo supostos crimes submetidos indubitavelmente à jurisdição brasileira”, ressaltou a ministra.

Laurita Vaz afastou o argumento do recurso diplomático. O fato de estarem guardadas em outra nação, justifica a relatora, não transforma as informações em material de prova estrangeiro. “A ordem pode ser perfeitamente cumprida, em território brasileiro, desde que haja boa vontade da empresa.

Impossibilidade técnica, sabe-se, não há”, ponderou. Como a filial foi constituída sob as regras brasileiras, a ré está impedida de recorrer às leis estrangeiras para desobedecer à demanda judicial.

“Não se pode admitir que uma empresa se estabeleça no país, explore o [lucrativo](#) serviço de troca de mensagens por meio da internet — o que lhe é absolutamente lícito —, mas se esquive de cumprir as leis locais”, escreveu a ministra. Por maioria, o colegiado acompanhou o entendimento da relatora. O prazo para cumprimento da ordem é de dez dias, sob pena de multa diária de R\$ 50 mil, como pedido pelo Ministério Público Federal.

Os Embargos Declaratórios, interpostos em maio, foram rejeitados pelos ministros por unanimidade. A

filial brasileira da corporação já entrou com um Mandado de Segurança no STJ contra a quebra de sigilo, ainda pendente de análise, sob relatoria do ministro Arnaldo Esteves Lima. A defesa da companhia também estuda outras formas de recorrer da decisão.

Sete chaves

O debate sobre a proteção de informações na internet é capaz de fazer convergir diferentes ramos do Direito. Na área criminal, por exemplo, a regulação dos dados serve para provar delitos ou resguardar as vítimas. Por um lado, órgãos de investigação querem ampliar cada vez mais o acesso. Por outro, tanto as leis quanto a jurisprudência ainda engatinham ao delinear parâmetros no uso do material online.

O livre-docente em Direito Processual Penal da USP **Gustavo Henrique Badaró** lembra que a questão não se limita aos episódios de crimes virtuais. “Postagens nas redes sociais e até dados de localizadores de veículos são requisitados para ajudar nas investigações e julgamentos”, conta o especialista, que participou, nesta quarta (5/6), do encontro “Estado e Cidadão: Novos Desafios Jurídicos para a Proteção de Dados no Brasil”, na Escola de Direito da Fundação Getúlio Vargas. “A produção de provas no meio digital ainda gera dúvidas”, diz.

A hipótese de conseguir dados sem o aval de um magistrado é vista com ressalvas. Nos Estados Unidos, um projeto de lei tem dividido opiniões dos parlamentares: o [Cyber Intelligence and Protect Act](#). Se aprovado, permitirá às agências de inteligência pedir informações aos provedores de internet e serviços de telecomunicação ou fazer varredura em bases de dados sem mandado judicial. Como várias empresas virtuais têm sede em território norte-americano, a proposta ameaça a proteção de dados virtuais de cidadãos de outras partes do mundo.

Entre as normas brasileiras, a Lei de Lavagem de Dinheiro ([Lei 12.683/2012](#)) foi a primeira a tratar expressamente da possibilidade. Em seu artigo 17-B, o texto diz que a autoridade policial e o Ministério Público terão acesso, exclusivamente, aos dados cadastrais do investigado sobre “qualificação pessoal, filiação e endereço, independentemente de autorização judicial, mantidos pela Justiça Eleitoral, pelas empresas telefônicas, pelas instituições financeiras, pelos provedores de internet e pelas administradoras de cartão de crédito.”

A advogada **Denise Vaz** tem receios sobre a tendência de flexibilização. “Por mais que os juízes não tenham critérios bem definidos para determinar a quebra de sigilo, o cenário piora se não é necessária a autorização da Justiça”, pondera a especialista, doutora pela USP na área de provas digitais no processo penal, que também discutiu o tema na FGV.

A extensão dos dados considerados cadastrais também preocupa. “Não fica claro, por exemplo, se isso inclui a senha ou o IP [*Internet Protocol, número que identifica os computadores na rede*] do usuário”, afirma Badaró. Na falta de regulamentação abrangente sobre o assunto, a postura das empresas virtuais varia: parte delas atende aos pedidos de investigação sem mandado judicial e outras aguardam ordem clara dos tribunais antes de liberar dados dos usuários.

Date Created

06/06/2013