Estado do Tocantins
Tribunal de Justiça
3ª Vara Criminal de Palmas

Processo nº 0009855-73.2019.827.2729

DECISÃO

Cuida-se de representação formulada pela delegada de polícia **Milena Santana de Araújo Lima**, da Delegacia de Repressão a Crimes Cibernéticos - DRCC, no bojo de investigação encetada para apurar a suposta prática de furto qualificado, ocorrido mediante invasão de conta bancária de titularidade do Conselho Regional de Odontologia do Tocantins, fato ocorrido no dia 27/10/2017.

O Ministério Público opinou pelo deferimento.

Destaco que o fato está sendo investigado no Inquérito Policial nº 0007206-38.2019.827.2729/TO, ao qual esta representação está relacionada.

Eis a síntese dos fatos, de acordo com o que foi descrito pela autoridade policial na petição inicial:

"Foi instaurado o Inquérito Policial nº023/2019, nesta Especializada, após ter sido declinada a competência da Justiça Federal para a Justiça Estadual, dando continuidade às investigação, iniciada pela Polícia Federal (Inquérito Policial n° 30/2018-SR/DPF/TO), para apurar a prática de furto qualificado, ocorrido mediante invasão de conta bancária ([redacted] de titularidade do [redacted], fato ocorrido no dia 27/10/2017.

Após burlar o sistema de segurança do Banco do Brasil S.A., o suspeito efetuou o pagamento de imposto (SEFAZ ARREC ICMS/IPVA), no valor de R$ 5.235,45 (cinco mil, duzentos e trinta e cinco reais, quarenta e cinco centavos), configurando o crime capitulado no Art. 155, § 4.°,II, do Código Penal.

Conforme relato de [redacted], secretária do [redacted], a prática delitiva se iniciou no dia anterior, com ligação telefônica de funcionário de suposta empresa de telefonia, conforme abaixo:

"(...) 26/10/2017, por volta das 12 horas e 40 minutos, onde o interlocutor se fez passar por um funcionário de uma empresa de telefonia, alegando que precisava que fosse encaminhado um comprovante de pagamento, pelo que, teria sido encaminhado um e-mail, sendo a declarante orientada para que acessasse o link encaminhado em anexo; QUE esse anexo corresponderia a um documento que deveria ser assinado pela declarante; QUE ao abrir o anexo, o documento não correspondia ao descrito na ligação; QUE verificou que na verdade, o documento baixado correspondia a um documento de nome — Autorização de Figuração", similar a um contrato,(...) QUE não possui registro do terminal de telefone responsável pelo contato fraudulento se passando pela empresa de

telefonia, pois o conselho não possui bina no telefone que recebeu a ligação; QUE as possíveis linhas que receberam a ligação foram 63 3[redacted]/321[redacted]914".

Para fins de instruir o feito, foi juntado aos autos a cópia do email enviado do endereço virtual aten[redacted]@gmail.com e tendo como destinatário a caixa eletrônica do Conselho de Odontologia, contendo um provável malware (programa malicioso) que viabilizou a técnica de phishing (furto de dados), bem como expediente da Instituição Bancária informando ter restituído a vítima, assumindo integralmente o prejuízo financeiro, motivo que ensejou a declinação da competência".

Essa narrativa encontra respaldo no inquérito policial referido, donde constam a mesmas declarações acima, que demonstram que a secretária do CRO/TO foi aparentemente induzida a instalar um programa espião em um dos computadores da entidade, por meio do qual se obtiveram os dados da conta bancária desta.

Comprovou-se ainda a realização de pagamento de boleto bancário no valor de R$ 5.235,45, pagamento que, segundo informado, foi efetuado indevidamente, provavelmente mediante a utilização dos dados furtivamente obtidos.

Como se vê nos autos do procedimento investigatório, há indícios da existência do crime, por isso a autoridade policial pretende obter dados que levem à identificação dos autores.

Neste caso, exige-se a continuidade das investigações do que foi noticiado pela autoridade policial, ainda mais que há possibilidade de que as ações venham se repetindo, com novas vítimas ainda não identificadas. Neste aspecto, as medidas postuladas são de fundamental importância, pois sem elas a autoridade policial dificilmente terá condição de aprofundar na apuração do fato e muito menos desvendar a autoria.

Neste tipo de crime, em que se usa a rede mundial de computadores para o enriquecimento ilícito, a investigação torna-se virtualmente impossível, caso se utilizem apenas os meios tradicionais de investigação. Afinal, as pessoas envolvidas nas práticas criminosas podem estar em qualquer lugar do globo terrestre, o que dificulta sobremaneira sua localização.

Como bem salientado na petição inicial, ***"as medidas administrativas possíveis pela Autoridade Policial que iniciou a investigação, não foram o suficiente para individualizar a Autoria e participação dos envolvidos, o que somente será possível após o afastamento do sigilo telefônico, telemático e bancário que se propõe com a presente representação"***.

Desta forma, no tocante à quebra dos sigilos, o deferimento da representação é medida que se impõe para viabilizar a atuação policial. Ressalto que a tutela jurisdicional ora prestada assegurará que sejam respeitados os direitos individuais dos usuários das redes sociais e dos terminais telefônicos usados para a consecução dos crimes, assim como dos titulares das contas bancárias envolvidas.

Diante do exposto, defiro a representação e concedo autorização para que a autoridade policial obtenha as seguintes informações das pessoas jurídicas indicadas a seguir:

a) da *Brasil Telecom S.A. (Oi Fixa)*, por meio de seus representantes no Brasil: o histórico de chamadas recebidas no dia 26/10/2017, das linhas telefônicas abaixo (número chamado), bem como, se possível, os números telefônicos, IMEI, dados cadastrais e ERB do número chamador:

(63) 3[redacted]
(63)3[redacted];
(63)3[redacted]

b) do *Google Brasil Internet Ltda*, por meio de seus representantes no Brasil:

b.1) os registros de criação do email aten[redacted]@gmail.com, contendo números de IP, data, hora, fuso horário, portas de origem, eventual email de recuperação e telefones, bem assim os acessos ao referido endereço eletrônico nos dias 25/10/2017 a 28/10/2017, bem como dos últimos 60 dias a contar do recebimento desta decisão, dentre outros elementos de prova que possam colaborar com a investigação;

b.2) cópia dos dados armazenados no endereço eletrônico aten[redacted]@gmail.com e IMEI atrelado a ele, devendo conter:

b.2.1) acesso a todo o conteúdo do Google Drive;
b.2.2) acesso a todo o conteúdo da ferramenta Maps (Seus lugares, Suas contribuições, Sua linha do tempo, etc);
b.2.3) acesso ao conteúdo do Google Docs e outros serviços da Google;
b.2.4) acesso a todos os aplicativos do Google Play Store instalados no aparelho;
b.2.5) acesso ao histórico de mensagens do aplicativo Hangouts (Google Talk);
b.2.6) acesso ao histórico de localização (Location History), disponibilizando o trajeto efetuado pelo alvo;
b.2.7) acesso ao conteúdo da ferramenta de backup de Fotos (Google Fotos).

A empresa deverá ainda preservar os registros de acesso/conexão pelo prazo que durar a investigação;

c) do *Banco do Brasil S.A.*, por meio de seus representantes:

c.1) os dados referentes ao pagamento do imposto no valor de R$ 5.235,45 (cinco mil, duzentos e trinta e cinco reais, quarenta e cinco centavos), após acesso não autorizado à conta [redacted] do Banco do Brasil) de titularidade do [redacted], fato ocorrido no dia 27/10/2017, especificando o código de barras e possível beneficiário;

c.2) os registros de conexões referentes à mencionada operação, bem como de eventuais outras transações realizadas por meio de internet banking na referida conta entre o dia 26/10/2017 a 28/10/2017, fornecendo número de IP, data, hora, fuso horário, porta lógica, número MAC, entre outros dados que possam corroborar com a investigação;

c.3) informação sobre se o número de IP eventualmente descoberto está associado a outras invasões bancárias ocorridas no mesmo período.

Esta decisão servirá como ofício requisitório endereçado a todas as pessoas jurídicas acima referidas, com as seguintes observações:

a) as respostas deverão ser apresentadas no prazo de 15 dias, a contar da data de recebimento por elas;

b) as respostas deverão ser encaminhadas diretamente à autoridade policial por meio do endereço eletrônico drcc@ssp.to.gov.br, com expressa referência ao número do processo, podendo ainda ser disponibilizado link, com login e senha para download;

c) alternativamente, as respostas poderão ser encaminhadas a este juízo por meio do endereço eletrônico criminal3palmas@tjto.jus.br, com expressa referência ao número do processo;

d) o sigilo da investigação deve ser preservado, portanto as empresas devem abster-se de informar aos

usuários e correntistas o fornecimento dos dados acima.

A entrega da decisão/ofício às empresas destinatárias será feita pela autoridade policial, que, para tanto, poderá valer-se de qualquer meio, inclusive eletrônico.

Intimo o Ministério Público e a autoridade policial.

Palmas/TO, 14 de março de 2019.

Rafael Gonçalves de Paula

Juiz de direito