Por Gilton Batista Brito

A Prisão Preventiva na Operação Replicante

Em setembro de 2006, a Polícia Federal efetuou diligências para cumprir dezenas de mandados de prisão e de busca domiciliar nos Estados de Goiás, Rio de Janeiro, Tocantins, Distrito Federal e Rio Grande do Norte, na fase ostensiva da chamada *Operação Replicante,* destinada à prevenção e repressão de crime cibernético.

A investigação sigilosa, autorizada pela 11ª Vara Federal de Goiás,[1] apurou que grupos criminosos acessavam ilicitamente contas bancárias, violando o sigilo de clientes de várias instituições financeiras. Descobriu-se então que transações ocorriam após a captura de dados pessoais, especialmente senhas de acesso, por meio de programa *spyware* conhecido como "cavalo de tróia" ou *trojan*. De posse das informações, efetuava-se a transferência de valores das contas das vítimas para contas "compradas" ou "alugadas" de terceiros participantes do esquema, seguindo-se o saque. Realizava-se ainda a aquisição de produtos e serviços em transações *on line* ou o pagamento de boletos diversos na rede mundial de computadores.

A captura dos dados bancários geralmente acontecia após envio de mensagens, não raro, contendo alertas chamativos e inverídicos. Tais mensagens solicitavam às vítimas dados financeiros: banco, agência, conta e senha. Outra forma comum de atuar era a criação de páginas-clone de bancos, acessadas mediante direcionamento irregular dos clientes. Para instalação do *spy* no computador da vítima, utilizava-se ainda o Orkut e o MSN. Depois de digitados, os dados bancários eram então enviados pelo programa espião para um servidor ou caixa de *e-mail* dos participantes do esquema. O *modus operandi*, assim, objetiva inicialmente "pescar" a senha de clientes bancários.[2]

A captura dos dados bancários acontecia após envio de mensagens, não raro, contendo alertas chamativos e inverídicos

Além do uso intensivo e constante da *internet* e da comunicação telefônica pelos integrantes do esquema, a investigação evidenciou a grande facilidade na obtenção de programas maliciosos e a formação de grupos em atividade criminosa constante, com estilo de vida voltado para a delinquência cibernética, pois, de modo geral, não possuíam os participantes ocupação profissional lícita. Além disso, com considerável grau de organização, os grupos estabeleceram certa estrutura funcional para cometimento dos ilícitos, atuando de maneira coordenada, com diferentes níveis de relacionamento, hierarquia e subordinação, distribuição de lucros e base territorial alcançando diferentes Estados.

[1] A presença da CEF como prejudicada firmou a competência federal (art. 109, IV, CF), havendo prevenção da Seção de Goiás quanto aos crimes praticados em outras circunscrições (art. 71, CPP), bem assim conexão com delitos envolvendo instituições financeiras privadas, de competência estadual (art. 76, CPP).

[2] Por isso, a prática tem sido chamada de *pishing*, junção das palavras *password* (senha) e *fishing* (pescar).

Johnathan Mateus

Gilton Batista Brito é juiz federal em Salvador, ex-advogado da União, ex-defensor público estadual

Assim, os *programadores*, chamados de *crackers,* eram responsáveis pela criação de páginas falsas, mensagens eletrônicas e programas viciados *trojan.*[3] Eram remunerados pela venda e atualização (*upgrade*) de tais programas, cobrando, às vezes, participação no lucro obtido pelo uso.[4] Os *usuários* utilizavam os programas e remetiam milhares de *e-mails* em busca de vítimas para coleta das mensagens retornadas com os dados financeiros. Também efetuavam pagamento de boletos e realizavam transferência entre contas. De regra, não realizavam pessoalmente o saque nas contas de destino, tampouco conheciam os titulares de tais contas (*laranjas)*. Os *carteiros, biscoiteiros* ou *cartãozeiros* arrecadavam boletos ou mantinham contato com terceiros para obtenção de contas, destino das transferências *on line* irregulares. Em seguida à posse dos cartões bancários (no esquema, chamados de *cartas* ou *biscoitos)* ou dos boletos de pagamento, ocorria a consumação da subtração, com o saque na conta titulada pelo *laranja* do valor transferido da conta da vítima ou pagamento *on line* diretamente nesta, havendo ainda a hipótese de os valores serem creditados em contas das empresas beneficiadas com pagamentos de boletos.[5] Os *laranjas* emprestavam as contas para receber a transferência ou forneciam boletos.[6] Em geral, apresentavam papel de menor importância na associação criminosa, obtendo pequenos ganhos, com participação eventual, pois a conta de destino normalmente era bloqueada pela instituição financeira logo após a contestação da operação pelo cliente-vítima, quando era identificado.[7]

O fato típico principal, ao resultar em subtração de valores sem entrega voluntária da quantia pela vítima, configurava furto qualificado, previsto no artigo 155, § 4º, II e IV do CP. O furto cibernético, com o uso crescente da rede mundial de computadores, tem-se notabilizado pela prática em larga escala e seu cometimento exige a presença de outras condutas penalmente ilícitas, como quadrilha ou bando (art. 288, CP), violação de sigilo bancário (art. 10, LC 105/2001) e lavagem de dinheiro (art. 1º, Lei 9.613/98). Daí ser legítimo afirmar que é da natureza desses crimes cibernéticos a reiteração, presente na habitualidade delitiva, no crime continuado e no concurso material.

Sintomático, assim, que durante a investigação, que durou 1 ano e foi acompanhada pela Procuradoria da República em Goiás, tem sido

[3] O programa, comprado então pelo valor de 5 a 15 mil reais, frequentemente possuía "prazo de validade" e exigia manutenção constante, o que serve de controle dos *programadores* sobre os *usuários*.

[4] Com frequência, a aquisição era "financiada" pela própria atividade criminosa.

[5] Já o *subcarteiro* não conhecia o *usuário* do programa malicioso e se limitava a "comprar" ou "alugar" cartões para venda a outros *carteiros* que se relacionavam, estes sim, com os *usuários*.

[6] Com isso, liquidava integralmente o débito e pagava àquele que ofereceu tal oportunidade ilegal, em regra, metade do valor do título.

[7] Sem embargo, no pagamento de boletos, é comum a habitualidade criminosa, diante do uso de diversos títulos do mesmo *laranja*. Há ainda a prática de instrumentalizar o pagamento do título, sem que tenha havido efetiva operação comercial, servindo a operação para encobrir verdadeira transferência para a conta da empresa beneficiada, emissora do boleto e integrante do esquema.

constante e mesmo crescente a prática delitiva, com acesso indevido a dados bancários de milhares de contas, realização de milhares de operações financeiras ilegais[8] vitimando os mais diversos bancos, pagamento irregular de milhares de boletos e participação em número ascendente de dezenas de pessoas, identificadas ou não, numa verdadeira teia criminosa[9] que tornou difícil, senão impossível, o alcance de todas as condutas ilícitas investigadas e a quantificação integral do dano.

Ora, nos termos dos artigos 312 e 313 do CPP, impõe-se a prisão preventiva quando houver prova da existência de crime doloso e indícios razoáveis da autoria e fundado risco à ordem pública, à instrução criminal ou à certeza da aplicação da lei penal.

Numa interpretação constitucionalmente adequada, a proteção à ordem pública decorre do dever estatal de garantir a segurança, protegendo eficazmente o meio social e a incolumidade das pessoas e do patrimônio (art. 195, CF), pois o princípio da proporcionalidade em sentido positivo impede a proteção deficiente dos direitos fundamentais, o que plenamente conforme a configuração de um Estado Social.

No caso, a necessidade, a utilidade e a adequação da prisão preventiva mostraram-se evidentes, sobretudo para um fim peculiar, qual seja, a interrupção da intensa reiteração criminosa própria do esquema, desenvolvida em ritmo altamente acelerado, assegurando-se a ordem pública. A orientação poderia ter sido fundamentada, a propósito, em precedente paradigmático do Supremo Tribunal Federal. Com efeito, em agosto de 2005, cumprindo dezenas de mandados expedidos pela Justiça Federal de Goiás, a Polícia Federal já havia deflagrado a *Operação Pégasus*, tendo como investigados suspeitos da prática dos mesmos crimes cibernéticos. Após inúmeras impugnações em segundo e terceiro graus, a prisão preventiva foi mantida na quarta instância, o Supremo Tribunal Federal.[10]

O crime cibernético é praticado em ambientes fechados, sem contato pessoal do ofensor com a vítima e cujo traço peculiar se encontra na reiteração criminosa por parte de agentes jovens

A decisão, ao tratar pela primeira vez de prisão cautelar em delitos de tal espécie, elencou as principais circunstâncias presentes no conceito de garantia da ordem pública: preservação da integridade física do preso; obstáculo à concreta possibilidade de reiteração criminosa; eficácia visível e transparente da política pública de persecução penal. Fez referência ainda à atuação criminosa em diferentes Estados e à utilização ampla do meio tecnológico empregado pelos investigados. Convém registrar que a legalidade da prisão foi mantida ainda que a primariedade e os antecedentes dos investigados fossem favoráveis e não tivesse havido ofensa à integridade física nas condutas praticadas.

O entendimento não poderia ser diverso, já que se trata de crime cibernético, praticado em ambientes fechados (computador doméstico ou *lan house*), sem contato pessoal do ofensor com a vítima e cujo traço peculiar se encontra na reiteração criminosa por parte de agentes jovens, de regra, pertencentes à classe média e sem "passagem" pela polícia. Circunstâncias todas presentes na *Operação Replicante*.

[8] O elevado número de ilícitos era necessário a fim de aumentar os lucros, diante do número de participantes e de algumas limitações bancárias (valor diário máximo para transações).
[9] Era frequente que integrantes dos diversos grupos se relacionassem ilegalmente.
[10] STF, HC 88905/GO, Relator Min. GILMAR MENDES, 12/09/2006, 2ª Turma, LEXSTF v. 28, n. 336, 2006, p. 480-500).

Conflito de competência provocado pelo MPF/GO perante a Justiça Federal de Goiás, em face da declinação de competência oriunda da Justiça Federal em Campos Mourão/PR. Naquela subseção judiciária, entendeu-se que o acesso espúrio à conta bancária via internet, com a subsequente retirada do dinheiro, seria delito de estelionato e, portanto, a competência deveria ser fixada no local da obtenção da vantagem ilícita. O MPF/GO argumentou, perante a JF/GO, que tal prática caracteriza, na realidade, delito de furto e, dessa forma, o local do crime seria onde ocorreu o dano. O STJ, ao decidir o conflito, acolheu a tese esposada pelo MPF/GO.

Acórdão

Origem: STJ
Processo: CC 67343 / GO (2006/0166153-0)
Classe: Conflito de Competência
Relatora: Ministra Laurita Vaz
Órgão Julgador: Terceira Seção
Data do Julgamento: 28/03/2007
Data da Publicação/Fonte: DJ 11/12/07, p.170

Ementa

CONFLITO NEGATIVO DE COMPETÊNCIA. PENAL E PROCESSO PENAL. FRAUDE ELETRÔNICA NA INTERNET. TRANSFERÊNCIA DE NUMERÁRIO DE CONTA DA CAIXA ECONÔMICA FEDERAL. FURTO MEDIANTE FRAUDE QUE NÃO SE CONFUNDE COM ESTELIONATO. CONSUMAÇÃO. SUBTRAÇÃO DO BEM. APLICAÇÃO DO ART. 70 DO CPP. COMPETÊNCIA DA JUSTIÇA FEDERAL PARANAENSE.

1. O furto mediante fraude não se confunde com o estelionato. A distinção se faz primordialmente com a análise do elemento comum da fraude que, no furto, é utilizada pelo agente com o fim de burlar a vigilância da vítima que, desatenta, tem seu bem subtraído, sem que se aperceba; no estelionato, a fraude é usada como meio de obter o consentimento da vítima que, iludida, entrega voluntariamente o bem ao agente.

2. Hipótese em que o agente se valeu de fraude eletrônica para a retirada de mais de dois mil e quinhentos reais de conta bancária, por meio da "Internet Banking" da Caixa Econômica Federal, o que ocorreu, por certo, sem qualquer tipo de consentimento da vítima, o Banco. A fraude, de fato, foi usada para burlar o sistema de proteção e de vigilância do Banco sobre os valores mantidos sob sua guarda. Configuração do crime de furto qualificado por fraude, e não estelionato.

3. O dinheiro, bem de expressão máxima da idéia de valor econômico, hodiernamente, como se sabe, circula em boa parte no chamado "mundo virtual" da informática. Esses valores recebidos e transferidos por meio da manipulação de dados digitais não são tangíveis, mas nem por isso deixaram de ser dinheiro. O bem, ainda que de forma virtual, circula como qualquer outra coisa, com valor econômico evidente. De fato, a informação digital e o bem material correspondente estão intrínseca e inseparavelmente ligados, se confundem. Esses registros contidos em banco de dados não possuem existência autônoma, desvinculada do bem que representam, por isso são passíveis de movimentação, com a troca de titularidade. Assim, em consonância com a melhor doutrina, é possível o crime de furto por meio do sistema informático.

4. A consumação do crime de furto ocorre no momento em que o bem é subtraído da vítima, saindo de sua esfera de disponibilidade. No caso em apreço, o desapossamento que gerou o prejuízo, embora tenha se efetivado em sistema digital de dados, ocorreu em conta-corrente da Agência Campo Mourão/PR, que se localiza na cidade de mesmo nome. Aplicação do art. 70 do Código de Processo Penal.

5. Conflito conhecido para declarar competente o Juízo Federal de Campo Mourão - SJ/PR.