

Golpe do novo número em aplicativos de celular

No golpe do *perfil fake* ou do *novo número*, o estelionatário utiliza-se de técnicas de engenharia social para enganar a vítima e a convencer a transferir dinheiro a suposto título de empréstimo, fingindo ser



Adriano Sousa Costa
Delegado da Polícia Civil de GO

Para tanto, o *golpista* entra em contato com a vítima, geralmente via

aplicativo de celular, seja ele Instagram, WhatsApp ou outro semelhante, utilizando-se de uma imagem de alguém próximo como foto de perfil e, imediatamente, diz que mudou de número. Em seguida, pede para ela anotar esse novo contato telefônico e apagar o anterior.

Superada essa etapa, o criminoso mantém um diálogo com a vítima e, no decorrer da conversa, pede dinheiro emprestado (via transação bancária eletrônica, especialmente *pix*), sob a alegação de que o seu aplicativo bancário está inoperante ou o telefone está com algum problema.

A vítima, na crença e no afã de ajudar o suposto *conhecido*, transfere o numerário para a conta bancária indicada pelo criminoso. Este, na posse do produto do crime, o transfere rapidamente para outras contas bancárias de asseclas ou saca o valor, dificultando a ação da Polícia Judiciária e o bloqueio dos valores.



Eduardo Fontes
Delegado da Polícia Federal

Capitulação jurídica

De início, importante dizer que o fato de o golpe ter sido perpetrado via digital não promove a incidência automática do novel delito de estelionato eletrônico.

Até porque, caso o golpe se concretize sem a vítima fornecer quaisquer outras informações para a construção de um contexto enganador, não há que se falar em fraude eletrônica. O estelionato comum, do *caput* do artigo 171 do CP, é que deve incidir.

Só será possível sair dessa capitulação ordinária de estelionato simples (e partir para a tipicidade especial do estelionato eletrônico) se outras nuances ocorrerem.

Elementares do estelionato eletrônico

Perceba-se que, enquanto o crime de furto qualificado pela fraude eletrônica se contenta com a subtração ocorrida *no meio virtual*, o crime de estelionato eletrônico (artigo 171, §2º-A, do CP) requer outras modalidades de quadramento do golpe de perfil *fake* nesta modalidade delitativa.



Henrique Hoffmann
Delegado da Polícia Civil do PR

Vejamos as diferenças dos tipos penais de furto qualificado pela fraude

§ 2º-A do CP):

"Art. 155. § 4º-B. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se o furto mediante fraude é cometido por meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem a violação de mecanismo de segurança ou a utilização de programa malicioso, ou por qualquer outro meio fraudulento análogo." (grifo nosso)

"Art. 171. § 2º-A. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo." (grifo nosso)

Diferentemente das elementares do crime de furto qualificado pela fraude virtual, no caso do estelionato eletrônico idealizou-se para a sua incidência o somatório de duas circunstâncias muito específicas: a) criminoso ter conseguido informações com a vítima ou com terceiro enganado; b) conduta praticada no meio eletrônico ou análogo. Ou seja, é preciso perquirir necessariamente a *fonte da informação* e o *meio de captura dos dados*.

Informações de validação

Inegável que o criminoso desenha a sua estratégia ilícita antes mesmo de abordar a vítima do crime. Parte das informações coletadas é pretérita, alcançada, amiúde, pelo acesso subterrâneo a bancos de dados privados, ou seja, sem qualquer participação da vítima ou de um terceiro induzido a erro. Portanto, se não houver a coleta de nenhuma outra informação adicional com a vítima ou com um terceiro (induzidos a erro), o tipo penal a incidir é mesmo o do artigo 171, *caput*, do CP.

Contudo, se a fraude demandar um pouco mais de conversa, cabe a reapreciação da capitulação prevalente. É aqui que se discute sobre a relevância das informações de validação.

É muito comum que exista a necessidade de um diálogo convincente entre vítima e criminoso, até mesmo para se esclarecer o motivo de o dinheiro estar sendo encaminhado para uma conta bancária em nome de um estranho (pois geralmente a conta indicada não é de titularidade do pretense amigo ou parente).

O desenvolvimento da conversa entre vítima e estelionatário garantirá a verossimilhança da alegada necessidade de transferência valores, podendo fazer incidir o estelionato eletrônico.

Substância das informações de validação

É importante dizer que tais informações angariadas pelo criminoso não precisam consistir nos dados bancários da vítima (por exemplo, a senha ou código de verificação). Até mesmo porque isso é mais característico do furto qualificado pela fraude eletrônica, pois, no estelionato eletrônico, é a vítima que encaminha, voluntariamente, o dinheiro para o criminoso.

A vítima dá informações que parecem banais, mas que, para a fraude, são essenciais. Fala o ofendido sobre nomes de parentes, onde moram, onde estão, quem namoram, indicam doenças a que estão acometidos, etc. Isto é, *um conjunto de informações cotidianas* que, conjugadas e devidamente utilizadas na conversa, reforçam a confiança da vítima na versão do criminoso.

Por isso, é fundamental perceber que, em regra, as informações de validação são orbitárias e circunstanciais, sendo geralmente deixadas de lado no relatório policial ou mesmo da denúncia. E não deveriam sê-lo, pois possuem relevo, servindo para a demonstração do contexto criminal e de convencimento da vítima.

Em suma, o fato de parte das informações terem sido alcançadas na conversa com a vítima, além daquelas iniciais que foram acessadas anteriormente em bancos de dados, justifica a incidência do estelionato virtual.

Fraude protraída

No golpe do WhatsApp, a fraude se protraí e se fortalece no desenrolar da conversa, sendo portanto por nós conceituada como *fraude protraída*. Existem vários momentos do golpe que poderiam se tornar pontos de inflexão e, portanto, permitir a desconfiança da vítima. Mas o conjunto gradativo de informações vai afastando dúvidas que inicialmente poderiam existir sobre a história mentirosa que está sendo contada.

Habilmente, o criminoso, utilizando-se das informações acumuladas anteriormente, arrasta a história até um ponto em que a vítima não resiste mais e acaba realizando a transferência bancária.

Sai-se do ponto inicial (quando o criminoso apresenta dados qualificativos falsos para a vítima) e se evolui até o ponto de a vítima acreditar na necessidade econômica de quem lhe solicita auxílio, transferindo valores (inclusive para a conta de pessoa desconhecida).

Depósitos de repique e crime continuado

É preciso falar também sobre o relevo jurídico dos *depósitos de repique*. Após conseguir o proveito ilícito principal, aproveita-se o criminoso de tal realização para pedir — logo em seguida — outros depósitos ou transferências complementares.

Nesse caso, até mesmo pela consideração da fraude protraída, os depósitos ou transferências posteriores são considerados como parte integrante do prejuízo inicial, ou seja, como parcela de um único estelionato. Não se pensa em crime continuado, mas somente na dilação do estelionato original, desde que todos os depósitos ou transferências sejam realizados pela mesma vítima.

Tentativa de estelionato

Quando a vítima percebe que as fraudulentas informações iniciais do delinquente (de qualificação, inclusive) não são verossímeis, sequer dá continuidade à conversa.

Nesse panorama, se o criminoso, utilizando-se somente das informações propedêuticas coletadas em banco de dados, não consegue *abertura* com a vítima, seu desiderato criminoso se frustra por motivos alheios à sua vontade. Daí, há que se falar em tentativa, e não em consumação. E, como não houve qualquer fornecimento de dados relevantes por parte da vítima ao longo de uma conversa, não ocorre tentativa de fraude eletrônica, mas sim *conatus* de estelionato simples (artigo 171, caput, c/c artigo 14, II, do CP).

Cenário diverso ocorre quando já tenha havido substantiva troca de informações entre vítima e estelionatário, mas, por motivos alheios à vontade do criminoso, o crime não se aperfeiçoa. Nesse caso, é possível a incidência da tentativa de estelionato eletrônico (artigo 171, §2º-A, c/c artigo 14, II, do CP).

Por exemplo, a vítima efetua a transferência, mas a agência da conta-corrente de destino bloqueia os valores preventivamente, não vindo o criminoso a ter acesso ao numerário. Nesse caso, perfeitamente possível a incidência do *conatus* de estelionato eletrônico.

Bloqueio cautelar e tentativa de estelionato

O Banco Central disciplinou a possibilidade de a vítima solicitar o bloqueio cautelar de valores transferidos para contas bancárias de criminosos, desde que tais transações sejam derivadas de fraudes minimamente comprovadas.

Tal mecanismo de retenção cautelar, funda-se no artigo 39-B da Resolução 147/2021 do Banco Central.

Conquanto seja inegável a importância de tal mecanismo no contexto prático, poderia ser aperfeiçoado. Sua implementação seria mais eficiente se o bloqueio fosse requerido pela vítima ao delegado de polícia, quando do registro da ocorrência policial, o qual requisitaria a providência às instituições financeiras por intermédio de ofício ou plataforma com interface direta.

Isso agilizaria as comunicações com os bancos, garantiria maior comodidade para as vítimas, faria um melhor filtro sobre pedidos de bloqueios infundados e, por fim, garantiria elementos mais contundentes sobre as suspeitas de fraude.

De toda sorte, ainda que não se tenha aperfeiçoado tal engenharia administrativa a esse ponto, o referido bloqueio é extremamente relevante, pois cria um empecilho para que o dinheiro chegue efetivamente nas mãos dos criminosos.

Apropriação parcial de recursos e consumação

Mesmo que, em virtude do bloqueio cautelar ou por qualquer outra causa alheia à vontade do criminoso, o valor for somente parcialmente bloqueado, ou seja, o criminoso tenha conseguido se apossar de parte do dinheiro, haverá consumação.

A consumação não versa sobre a quantidade de dinheiro que chega às mãos do criminoso, e sim acerca da obtenção de vantagem patrimonial ilícita em prejuízo da vítima. Em outras palavras, ainda que o valor visado pelo criminoso não seja alcançado *in totum*, as elementares estarão devidamente contempladas, assegurando-se a consumação.