O ‘sequestro’ de contas do Instagram por SIMswap

O sequestro de contas do Instagram (ou de qualquer outra rede social) pode se dar por diversos meios. O usuário pode deixá-la aberta em um computador, usar senhas fracas, compartilhá-las com terceiros ou ser vítima de obtenção de dados e informações pessoais. As técnicas mais utilizadas para fraudes são: a) *phising* (envio de e-mails ou links com aparência de fontes confiáveis); b) *vhising* (uso do telefone e contatos se passando por empresas ou pessoas); c) *SMiShing* (envio de mensagens com *links* ou armadilhas); d) roubo de identidade (passar-se pelo titular com o fim de obter dados pessoais e/ou sensíveis); e) obtenção dos dados em fontes abertas ou em *databrokers*. As duas primeiras são mais utilizadas em fraudes bancárias. O acesso aos dados e informações da vítima pode se dar por negligência do usuário ou ação do golpista. As invasões de rede social, na sua grande maioria, ocorrem por *SIMswap* ou engenharia social.

A noção de engenharia social ganhou relevo diante das reiteradas práticas de fraudes pelo meio digital. O termo é ambíguo, como bem demonstra Spencer Toth Sydow , porque engloba no mesmo significante dois campos de incidência (Ciências Sociais e segurança de dados). No campo da segurança da informação, está associada, diz Spencer Toth Sydow, à *"manipulação psicológica individual, de uma pessoa específica, para fazê-la acreditar em uma informação e, assim, ser induzida a fazer algo que normalmente e sem aquela influência ou intervenção, não faria"* . ("Direito Penal Informático". Salvador: Juspodivm, 2020, p. 577). Em resumo, ainda com Spencer Toth Sydow: *"Enquanto que o termo da ciência social trata de uma modificação de conceitos coletivos, o termo de segurança da informação trata de situações individuais de tomada de decisões a partir dos vieses cognitivos"*. (p. 578). Associada à origem da palavra *ingenium* (habilidade e talento), denomina-se *scammer*, a *"qualidade do indivíduo dotado de capacidade inventiva, criatividade e talento"* ainda que com fins ilícitos, já que *"o* scammer *é o estelionatário que age no meio virtual, que se utiliza das armadilhas e golpes construídos especialmente para uso na virtualidade e com o intuito de obter vantagens patrimoniais"* (p. 571-584).

É que os dados da vítima, diante a quantidade de vazamentos noticiados, tendem a estar disponíveis em vários sítios de domínio público ou pago, facilitando a atuação de terceiros oportunistas. A *internet* proporciona imensas oportunidades de pesquisa em "fontes abertas", tanto para fins lícitos, como também ilícitos. A aquisição de habilidades mínimas do ambiente digital, associadas a cuidados de *cybersecurity*, transforma o conjunto de dados e informações disponíveis em suporte para prática de fraudes (Mendes, Carlos Hélder C. Furtado. "Tecnoinvestigação Criminal". Salvador: Juspodivm, 2020). Desde endereços, passando por reconhecimento de fotos, pesquisa de patrimônio, de redes de relacionamentos etc., enfim, a pesquisa não termina. Pode ser realizada na internet de superfície, na *darkweb* ou na *deepweb*, com recursos e cuidados específicos (*browser* TOR, por exemplo). Em todas as hipóteses, os parâmetros analógicos de atribuição de culpa dependem do respectivo ajuste digital.

Vamos nos ater aos casos de *SIMswap*. Os ataques *SIMswap* e a invasão de contas do Instagram têm se multiplicado no contexto da pandemia, dadas as oportunidades digitais. Escondidos através de conexões de internet e com farta engenharia social, os oportunistas incrementaram seus ganhos no ciberespaço e demonstram que o crime nunca entrou em quarentena. Aproveitando-se da "confiança cega dos usuários", o *scammer* assume a identidade da vítima, passando a ofertar produtos e/ou serviços por preços convidativos com a condição de transferência prévia, em geral por Pix. O "sequestro" do *chip* da vítima se dá por meio de dois *modus operandi*: a) engenharia social por meio da utilização de dados da vítima obtidos conforme acima ou em *databrokers* ilegais; e/ou b) conivência ou acesso promovido por funcionário(s) da operadora, obtendo a troca indevida do *chip*. De posse do número telefônico, o infrator solicita o *reset* de senha do Instagram para recebimento do código por SMS. Após modificar o e-mail e número de telefone da rede social, o usuário encontra dificuldades na recuperação, sobretudo por deficiência no suporte disponibilizado pela rede social.

No contexto do caso, a invasão e o "sequestro" da conta não pode ser atribuídos ao Instagram/Facebook de modo válido, dada a ocorrência de fortuito externo, advindo da conduta de terceiros (*scammers*), sem que tenha sido demonstrado o fortuito interno. Ademais, os cuidados para reativação da conta, confirmando-se a autenticidade do pedido, a integridade do requerente, estão expostas nos termos e condições, exigindo mecanismos de "acreditação", ao mesmo tempo que demandam agilidade e atuação imediata da rede social, sob pena de configuração de ilícito civil. O Instagram/Facebook é aplicação de internet (Marco Civil da Internet) e responde pelos fortuitos internos decorrentes de falhas de serviço e, também, pela demora (modalidade de negligência) em resolver os casos de contas sequestradas. Entre a denúncia, o preenchimento de formulários e a espera, o usuário fica exposto ao comportamento ilícito do fraudador, motivo pelo qual a conduta negligente do Instagram/Facebook, embora não seja a causa do evento ilícito, ao mesmo tempo é a causa da extensão e dos efeitos advindos de sua omissão. É que além de entregar o IP (*Internet Protocol)* utilizado pelo fraudador, deve cooperar para apuração de eventuais condutas penais e com imediata cessação da conduta ilegal, além de promover a recuperação da titularidade da conta o mais breve possível (princípios da confiança e da boa-fé objetiva).

Os danos podem ser materiais e/ou morais. O posicionamento da marca (*branding*), dos negócios e das vendas é interrompido, muitas vezes com a oferta de produtos, de "oportunidades" ou de "pedidos de auxílio" (depósitos). Usuários e estabelecimentos que demoraram anos para a consolidação de seus perfis e que deles dependem para o sustento, são afetados tanto financeiro, quanto moralmente.

Mas será que esse sequestro de conta por *SIMswap* poderia ter sido evitado?

Claro que sim. A falha na prestação do serviço por parte da operadora de telefonia móvel foi crucial para que a rede social fosse invadida. Se a relação é de consumo e há evidências de que houve fortuitointerno, a responsabilidade pode ser atribuída desde que existam elementos mínimos da prática ilícita. A responsabilidade da empresa pelo ataque *SIMswap* é objetiva, ou seja, independente da demonstração de culpa. A alegação de ilegitimidade passiva da operadora de telefonia pela invasão do Instagram não deve persistir pois o *hackeamento* só ocorreu porque houve a mudança de titularidade não solicitada pelo proprietário, desprovida de mecanismos de segurança adequados e exigíveis do fornecedor. Ainda que a mudança seja realizada por telefone, deve-se ter em conta as cautelas necessárias para a confirmação de autenticidade.

O consumidor afetado deve buscar a indenização decorrente dos danos morais e materiais causados pelo *SIMswap*. Para esse propósito deve solicitar à sua operadora o protocolo de mudança de número com as seguintes informações: dia e hora da mudança, documentos informados, gravações do atendimento remoto, funcionário e/ou estabelecimento comercial; Imei após a troca e eventuais registros de conexão relacionados. O defeito na prestação do serviço é indiscutível e deve, sim, ser corrigido, sob pena da empresa arcar com custos de reparação. Medidas para mitigação do problema podem e devem ser incorporadas pelas operadoras, entre elas, a implementação do *simcode*, por meio do qual a solicitação de qualquer alteração estaria condicionada à mais um código de confirmação.

A negativa genérica da operadora de telefonia em processos judiciais, por sua vez, não pode ser acolhida sem a demonstração de que não houve a troca do *chip* ou o atendimento de pedidos em nome da vítima. A relação de consumo existente impõe à operadora de telefonia o dever de demonstração da ausência de evidências de sua participação. Não se trata de "prova diabólica" e, sim, da aquisição válida de dados e informações dos seus sistemas, não se confundindo com os meros *prints* unilaterais, insuficientes à comprovação dos requisitos excludentes, dada a disponibilidade e superioridade probatória. Por isso, a operadora deve indenizar as vítimas pelos danos causados em decorrência da prestação de serviço falha.

A questão crucial será a configuração de indicadores mínimos da responsabilidade da operadora, dado que a causa suficiente pode ser o comportamento da vítima, excludente de ilicitude (CDC, artigo 14, §3º). Aplica-se a teoria da redução do módulo da prova nos casos de controvérsia, diante da posição de hipossuficiência probatória do consumidor.

Em tempos de pandemia, em que o uso das redes sociais restou potencializado, o consumidor deve estar vigilante às vulnerabilidades digitais. As configurações de privacidade nas redes sociais e, principalmente a migração de todo e qualquer serviço que tenha como autenticador o SMS para "aplicativos autenticadores" ameniza, sobremaneira, os riscos de ataque e garante ao usuário a continuidade do seu negócio nas redes sociais. Por isso, use um e-mail somente para o cadastro na rede social, desative a opção de confirmação por SMS e utilize um "aplicativo autenticador". Todo cuidado é pouco e os mecanismos de *cybersecurity* precisam ser conhecidos e democratizados. O perigo sempre existirá, o que se pode fazer, com razoável eficácia, é a redução à exposição aos riscos. Voltaremos em 2022 com os aspectos penais. Ainda dá tempo de tomar medidas preventivas em 2021. Vamos lá?

Date Created
31/12/2021