Escola da Magistratura do Estado do Rio de Janeiro

Aspectos de responsabilidade civil em fraudes eletrônicas no Internet Banking

Carlos Eduardo Mendes de Azevedo

Rio de Janeiro
2012

CARLOS EDUARDO MENDES DE AZEVEDO

Aspectos de responsabilidade civil em fraudes eletrônicas no Internet Banking

Artigo Científico apresentado como exigência de conclusão de Curso de Pós-Graduação Lato Sensu da Escola de Magistratura do Estado do Rio de Janeiro.
Professores Orientadores:
Mônica Areal
Néli Luiza C. Fetzner
Nelson C. Tavares Junior

Rio de Janeiro
2012

ASPECTOS DE RESPONSABILIDADE CIVIL EM FRAUDES ELETRÔNICAS NO INTERNET BANKING

Carlos Eduardo Mendes de Azevedo

Graduado pela Faculdade de Direito da Universidade Federal do Estado do Rio de Janeiro (UNIRIO). Advogado. Pós-Graduado em Direito do Consumidor pela Universidade Estácio de Sá.

Resumo: O artigo procura discutir, sob o contexto da responsabilidade civil, o problema da ocorrência de fraudes eletrônicas no ambiente de *Internet Banking*. São descritas as principais técnicas e métodos utilizados pelos fraudadores. É tratado o papel e responsabilidade dos principais agentes envolvidos no *Internet Banking*, a relação existente de consumo entre elas, o destaque das instituições financeiras e sua relevante importância como o agente mais forte, poderoso e capacitado para aplicar mecanismos eficientes contra as fraudes eletrônicas.

Palavras-chave: Internet - Responsabilidade Civil – Direito do Consumidor - Comércio Eletrônico – Relações de consumo

INTRODUÇÃO

O desenvolvimento em geral do comércio está intimamente relacionado com as leis e julgados adotados em respeito a certos temas. No comercio eletrônico, isso não é diferente. O aumento dos negócios no ciberespaço depende de como os conflitos que surgem são resolvidos no dia a dia.

Um exemplo de decisão judicial que certamente tem impacto nos negócios na rede mundial é aquela relacionada com a responsabilidade civil por ataques de fraudes eletrônicas. Dependendo de como os tribunais se posicionem, responsabilizando (ou não) as instituições financeiras pela reparação de seus clientes vítimas desse tipo de fraude tecnológica, pode haver alteração no modelo de negócios hoje estabelecido e disseminado. Por exemplo, pode ocorrer uma diminuição da utilização dos serviços bancários *online* se os clientes perderem a certeza quanto a uma reparação completa de danos financeiros causados por um ataque. Por outro lado, os bancos certamente realizarão modificações no modelo de relacionamento via Internet se o judiciário se inclinar a responsabilizá-los de forma objetiva por esses danos.

Assim, o maior desafio nessa área de prestação *online* de serviços bancários é superar os problemas de segurança e definir responsabilidades pelas conseqüências de ataques e invasões de sistemas informáticos. Esta definição ajuda a impulsionar o desenvolvimento desse mercado, já que elimina as incertezas quanto a quem deve e em quais circunstâncias arcar com os prejuízos de práticas tecnológicas fraudulentas.

Para que o serviço de *Internet Banking* aconteça, vários atores entram em cena concorrentemente: provedores Internet, fabricante do software de navegação, a instituição bancária, e o próprio cliente do banco, como internauta. Estabelecer esquemas de atribuição de responsabilidade civil nesse contexto não é fácil, dada a intricada cadeia de papéis e funções que esses atores da comunicação informática assumem.

As fraudes eletrônicas aqui tratadas são aquelas que compreendem o elemento da burla, do ato ou efeito de enganar o usuário para que forneça seus dados pessoais e de autenticação que permita o acesso indevido à sua conta bancária. Isso ocorre tanto quando um indivíduo preenche um formulário em um sítio falso, estruturado com a aparência do sítio legítimo, ou quando abre um arquivo que contém vírus, o qual é ativado e, apropriando-se da máquina da vítima, repassa os dados contidos no computador para o fraudador. Em ambas as situações, o indivíduo geralmente recebe previamente uma mensagem enganosa via correio eletrônico, induzindo-o a abrir o arquivo anexo contendo vírus ou clicar em um *link* que descarrega o vírus ou o leva para um sítio falso.

Nesse contexto, uma questão importante é saber se essas fraudes ocorrem por culpa exclusiva do usuário, que, por desconhecimento ou negligência, acaba entregando facilmente sua conta e senha ao fraudador, sem nenhuma participação do banco nessa entrega. Ou então se elas ocorrem por vícios no serviço bancário disponibilizado, que, por não requerer uma autenticação mais rigorosa, permite que o usuário seja facilmente logrado.

Essa é a temática que o presente artigo pretende abordar.

1. TIPOS DE FRAUDES ELETRÔNICAS

O cliente bancário é o objetivo primário das fraudes eletrônicas. Nelas o computador é infectado por um artefato malicioso ou então a própria vítima é induzida, por uma mensagem fraudulenta, a repassar as informações para o fraudador. Desta forma, o próprio sistema informático do banco não é diretamente invadido ou atacado, nem tampouco o dos provedores Internet. Ou seja, a origem do procedimento criminoso está no elemento do logro ao usuário ou adulteração maliciosa do seu computador, permitindo ao fraudador ingressar no sistema do banco como se fosse o legítimo usuário, pois aquele acaba se apropriando previamente das

informações pessoais e sigilosas desse último, inclusive as de autenticação. A peculiaridade então é que o acesso indevido do fraudador ocorre pelos meios permitidos pelo próprio sistema, através da digitação da senha e informações do usuário, o que torna bastante difícil a sua prevenção.

1.1 MECANISMOS UTILIZADOS PELOS FRAUDADORES

No Brasil, as principais tentativas de fraude realizadas sobre clientes do sistema financeiro, usuários do ambiente Internet, estão baseadas em ataques conhecidos como *phishing scam* e *pharming*. No primeiro tipo, o principal vetor de propagação da ameaça é realizado através do envio de mensagens eletrônicas de conteúdo falso, que são recebidas pelas vítimas, sem sua solicitação ou consentimento. No segundo tipo, *pharming*, outros ambientes e protocolos de comunicação podem ser utilizados para o comprometimento do usuário no ambiente Internet, sendo este um golpe bem disseminado em vários países.

1.1.1 PHISHING SCAM

O *phishing scam*, ou simplesmente *phishing*[1], é um tipo de ataque, onde mensagens eletrônicas falsas são enviadas aos usuários de caixas postais, convidando-os a acessar páginas fraudulentas na Internet. Têm a intenção de capturar informações pessoais e confidenciais, tais como números de cartões de crédito, contas e senhas de acesso bancário.

Essas páginas fraudulentas são criadas por pessoas que usam seus conhecimentos técnicos em informática, imitando as páginas legítimas de grandes companhias, como bancos e instituições financeiras, porém adicionando código malicioso para capturar conta e senha dos clientes que acessarem estas as páginas.

[1] PHISHING. Disponível em: <http://pt.wikipedia.org/wiki/Phishing>. Acesso em: 12 out. 2011.

Em geral, são classificadas como *phishing* as mensagens eletrônicas que apresentam as seguintes características:

a) O conteúdo da mensagem contém uma marca comercial forjada;

b) Contém endereços de e-mail e *links* forjados;

c) Apresenta uma mensagem que aguça a curiosidade da vítima;

A fraude busca atingir a vítima, coletando informações digitadas em formulários existentes em um e-mail ou página Web, resultante do *link* forjado na mensagem eletrônica. O processo de captura se apresenta através do serviço Web, induzindo a vítima a colaborar voluntariamente com o fornecimento de informações sensíveis.

O usuário é instigado a clicar no falso *link*, acreditando que irá obter uma informação importante. Os fraudadores são bem criativos e dotados de boa percepção psicológica, usando temas como restituição do imposto de renda, inscrição indevida no cadastro de proteção ao crédito, cobrança de dívidas, intimações policiais, fotos de acidentes ou de intimidades com pessoas famosas, entre outros.

O processo de captura de credenciais pode ser imperceptível à vitima, ou se apresentar na forma de uma tela sobreposta sobre os aplicativos do computador, induzindo-a a entrar voluntariamente com seus dados pessoais, sendo capturados em seguida.

Em geral, os dados pessoais obtidos são enviados ao fraudador por meio de protocolos de transferência de arquivos ou de envio de mensagens.

1.1.2 PHARMING

O *pharming*[2] é um conceito relativamente recente, porém vem crescendo como um meio utilizado para a efetivação da fraude sobre o ambiente *Internet Banking*.

[2] PHARMING. Disponível em: <http://pt.wikipedia.org/wiki/Pharming>. Acesso em: 12 out. 2011.

O mecanismo utilizado por este ataque promove o redirecionamento da vítima a páginas falsas de instituições financeiras, tal como descrito pelo *phishing*, porém esta variação de ataque não utiliza uma mensagem eletrônica como vetor de propagação. O atacante busca fragilizar serviços de resolução de nomes na Internet, conhecidos como DNS[3] (*Domain Name System*), que resultam no acesso errôneo do usuário à página replicada pelo fraudador, similar a página da instituição financeira, mesmo que o usuário efetive a inserção do endereço da página do banco através da digitação da URL no navegador utilizado.

Pelas modificações introduzidas no sistema de resolução de nomes (DNS), o *pharming* também é conhecido como "*DNS hijack*" ou "*DNS poisoning*", pelo fato de alterar, ou "envenenar" o DNS.

2. A SEGURANÇA BÁSICA DO *INTERNET BANKING*

É muito comum os bancos informarem aos seus clientes que seus sítios e o serviço de *Internet Banking* são seguros. Porém, geralmente isso quer dizer que o banco está utilizando basicamente dois tipos de proteções: *firewalls*[4] e criptografia de dados.

Os *firewalls* são usados no local onde residem as máquinas servidoras do sítio do banco. Sua função consiste em regular o tráfego de dados entre redes distintas e impedir a transmissão e/ou recepção de acessos maliciosos ou não autorizados de uma rede para outra. O termo *firewall* é usado como uma analogia com as paredes corta-fogo, que evitam o alastramento de incêndios, pois estes dispositivos procuram evitar o alastramento de acessos maliciosos e não autorizados dentro de uma rede de computadores. Assim, esse tipo de proteção impede que acessos não autorizados ocorram na máquina servidora, garantindo que

[3] DOMAIN NAME SYSTEM. Disponível em: <http://pt.wikipedia.org/wiki/Domain_Name_System>. Acesso em: 12 out. 2011.
[4] FIREWALL. Disponível em:<http://pt.wikipedia.org/wiki/Firewall>. Acesso em: 12 out. 2011.

os dados lá armazenados estarão sempre íntegros e confidenciais, sendo acessíveis apenas através da identificação e senha do respectivo cliente bancário.

Outra proteção utilizada pelos bancos é a criptografia de dados entre o computador do usuário e o sítio do banco, através do protocolo SSL[5] (*Secure Socket Layer*), tecnologia considerada padrão de segurança na transmissão de dados pela Internet, de maneira que todos os dados que trafegam na rede durante o período da transação eletrônica são codificados. Isso garante que não é possível a um terceiro interceptar a comunicação, de forma a capturar e entender os dados, entre elas a conta e senha bancárias, que estão passando nesse canal interceptado.

Porém, o que os bancos não costumam divulgar é que essas proteções, apesar de necessárias, não são suficientes para uma proteção completa do serviço de *Internet Banking*. Via de regra, o computador do usuário está desguarnecido, e através de um ataque via *phising*, pode, por exemplo, ser instalado localmente um programa malicioso que monitora o teclado (*keylogger*), conseguindo capturar a conta e senha bancária, antes que sejam enviadas codificadas ao sítio do banco.

Outra possibilidade é ser o usuário induzido a clicar em um *link* contido em uma mensagem falsa recebida, que o redirecionará a um sítio falso que simula o sítio original do banco. Geralmente esse sítio falso vai pedir informações pessoais do usuário, incluindo conta e senha, que serão prontamente fornecidas, uma vez que ele crê que o sítio é o verdadeiro e, portanto, confiável.

Ou seja, a segurança oferecida pelo banco ao serviço *Internet Banking* em geral é limitada à máquina servidora do sítio e ao *link* de comunicação com o usuário, não envolvendo o seu computador pessoal. Mas para a segurança ser completa, ela precisaria ser fim-a-fim, envolvendo também o ambiente computacional do cliente, pois a segurança de

[5] SSL. Disponível em:<http://en.wikipedia.org/wiki/Secure_Socket_Layer>. Acesso em: 12 out. 2011.

dados eletrônicos é como uma corrente, podendo ser quebrada no seu elo mais fraco.

Justamente por isso, alguns bancos procuram aprimorar a segurança do sistema de *Internet Banking*, incluindo recursos como o teclado virtual, para tentar impedir que os *keyloggers* interceptem senhas digitadas, ou através do uso de mecanismos de autenticação mais fortes do que simples senhas, como forma de dificultar a simulação do sitio verdadeiro por sítios falsos.

3. AS FRAUDES NO ÂMBITO DA RESPONSABILIDADE CIVIL

A responsabilidade civil consiste na obrigação de reparar um dano sofrido, dever que pode decorrer de uma relação contratual ou extracontratual. No caso do *Internet Banking*, não há duvida que existe uma relação eminentemente contratual entre o banco e o cliente lesado por fraude.

Dessa maneira, verifica-se que esse liame contratual consiste numa prestação de serviços, cujo entendimento atual pacífico é que se trata de uma relação consumerista, entendimento esse inclusive expresso no enunciado 297 da súmula do STJ: "O Código de Defesa do Consumidor é aplicável às instituições financeiras".

De acordo com o diploma consumerista, os bancos respondem objetivamente pelos defeitos dos serviços que oferecem, incluindo *Internet Banking*, conforme se pode depreender do art. 14 da Lei 8.078/90[6], que estipula:

> Art 14 – Código de Proteção e Defesa do Consumidor
>
> O fornecedor de serviços responde, *independentemente da existência de culpa* (grifo meu), pela reparação dos danos causados aos consumidores por defeitos relativos à prestação dos serviços, bem como por informações insuficientes ou inadequadas sobre sua fruição e riscos.

[6] BRASIL. Lei n. 8.078, de 11 set. 1990. Disponível em: <http://www.planalto.gov.br/ ccivil_03/leis/ L8078compilado.htm>. Acesso em: 29 jan. 2012.

O parágrafo 3º do mesmo art. 14 define as situações que excluem essa responsabilidade objetiva dos bancos:

> § 3° O fornecedor de serviços só não será responsabilizado quando provar:
>
> I - que, tendo prestado o serviço, o defeito inexiste;
> II - a culpa exclusiva do consumidor ou de terceiro.

Ao comentar sobre acidentes de consumo, Sérgio Cavalieri Filho[7] destaca que todo aquele que se dispõe a exercer alguma atividade no campo do fornecimento de bens e serviços tem o dever de responder pelos fatos e vícios resultantes do empreendimento independentemente de culpa.

Esse dever é imanente ao dever de obediência às normas técnicas e de segurança, decorrendo a responsabilidade do simples fato de dispor-se alguém a realizar atividade de executar determinados serviços.

Em suma, os riscos do empreendimento correm por conta do fornecedor (dos produtos e serviços), e não do consumidor, salvo se presente alguma excludente de responsabilidade. Por causa disso, os bancos frequentemente alegam que a fraude não decorreu de problema na segurança em um sítio fortemente "blindado" contra invasões, pois como visto, são usadas proteções como *firewall* e criptografia de dados. É o que Demócrito Reinaldo Filho aponta:

> Os bancos redargúem apontando a não razoabilidade dessa teoria, já que não podem ser responsabilizados por falha de segurança nesses casos, uma vez que são os próprios usuários do sistema que fornecem (ainda que involuntariamente) as senhas aos infratores.
> No caso de phishing, sustentam, não há propriamente nenhuma invasão ao sistema informático dos bancos. Os phishers, mediante artifícios enganosos, se apossam previamente das senhas dos verdadeiros usuários, e de posse delas acessam livremente o sistema do banco, como se fossem legítimos usuários. (...) os bancos sustentam ainda que a solução para o combate ao phishing passa pela educação do usuário, que deve ter o cuidado de utilizar softwares atualizados (antivírus, firewalls, navegadores de última versão etc.) e não ser displicente com as senhas de acesso ao sistema[8].

---

[7] CAVALIERI FILHO, Sérgio Cavalieri. Programa de Responsabilidade Civil. São Paulo : Atlas. 2008, p.402.

[8] REINALDO FILHO, Demócrito. *A responsabilidade dos bancos pelos prejuízos resultantes do "phishing"*. *Jus Navigandi*, Teresina, ano 13, n. 1836, 11 jul. 2008. Disponível em: <http://jus.com.br/revista/texto/11481>. Acesso em: 10 mar. 2012.

Assim, os bancos procuram geralmente atribuir a causa da ocorrência da fraude à conduta "ingênua" do usuário, consistente em entregar indevidamente seus dados e senhas a terceiros. Com isso, tentam excluir a sua própria responsabilidade, dizendo que houve fato exclusivo da vítima.

4. A RESPONSABILIDADE DOS AGENTES

No serviço de *Internet Banking*, existem diferentes participantes para que o serviço se complete. Pode-se destacar a participação dos provedores Internet (sejam de acesso, serviço e/ou hospedagem) da instituição bancária, e do próprio internauta (cliente do banco). Dentre esses diversos intervenientes e fornecedores da cadeia eletrônica de comunicação, a polêmica é definir quais podem e devem ser chamados à responsabilização por atos cometidos pelos fraudadores, quando estes não puderem ser identificados ou não puderem ser responsabilizados diretamente.

4.1 Responsabilidade pelo fato exclusivo da vítima

A primeira hipótese de responsabilização recai sobre os próprios usuários dos sistemas, uma vez que são eles mesmos que fornecem (ainda que involuntariamente) as senhas aos infratores. Os fraudadores, mediante artifícios enganosos, se apossam previamente das senhas dos verdadeiros usuários, e depois acessam livremente o sistema do banco, como se fossem legítimos usuários. No caso de *phishing*, não há inclusive nenhuma invasão propriamente dita ao sistema informático dos bancos.

Sob essa ótica, o ataque não é cometido contra o sistema informático do banco, que permanece sem violação, não sendo razoável, a princípio, impor à instituição bancária a

reparação dos danos patrimoniais resultantes da fraude. A solução para o combate às fraudes eletrônicas passaria pela educação do usuário, que deveria ter o cuidado de utilizar softwares atualizados (por exemplo, antivírus e *firewalls*) e não ser displicente com as senhas de acesso ao sistema.

Porém, essa tentativa de se colocar exclusivamente nas mãos do próprio usuário a responsabilidade de se precaver desse típico específico de fraude não é satisfatória, quando se tem em vista as características dinâmicas do ciberespaço e o papel que as instituições bancárias desempenham no mercado de serviços *online*.

Por melhor informado que possa ser o internauta, em termos de noções básicas de navegação segura e utilização de programas de proteção, não é possível eliminar completamente a probabilidade de ser vítima de um embuste. As fraudes eletrônicas estão se sofisticando a cada dia, criando sempre maiores dificuldades para a pessoa saber quando está diante de uma tentativa de golpe. A navegação em ambiente eletrônico coloca o usuário médio em situação de fragilidade, dada a ausência de conhecimentos técnicos e a natural falta de aptidão para lidar com inovações tecnológicas, somadas às características dinâmicas da Internet.

A educação dos usuários dos serviços de *Internet Banking*, para que adotem comportamentos e práticas seguras de navegação e utilização de softwares de proteção, é um recurso válido e que pode ser utilizado na redução de fraudes e ataques informáticos, mas que, por si só, não tem o efeito de mostrar integralmente os custos e perdas financeiras deles decorrentes. Mesmo que os bancos disponibilizem em seus sítios informações sobre as fraudes eletrônicas e sobre como evitá-las, tal iniciativa não deveria ser, por si só, suficiente para excluir a responsabilidade pelos efeitos lesivos desse tipo de fraude aos usuários. Por mais que se dê informação ao cliente, esse sempre estará sujeito a riscos na operação dos serviços de *Internet Banking*, pois novas formas de golpes e ataques fraudulentos são

desenvolvidas a cada dia.

4.2 Responsabilidade do provedor Internet

Outra possibilidade é a responsabilização dos provedores Internet pelos prejuízos decorrentes de *phishing* e outras fraudes do gênero. Como os perpetradores diretos das fraudes não são facilmente identificáveis e muitas vezes estão situados em território não submetidos à jurisdição do país da vítima[9], discute-se a possibilidade da responsabilização de outros intermediários da cadeia informática, a exemplo dos provedores de hospedagem de conteúdo na Internet (sítios e páginas eletrônicas).

Desta forma, embora não sendo o executante primário e direto da fraude, poderia o provedor que hospeda o sítio falso ser responsabilizado pelos danos financeiros sofridos pela vítima (cliente do banco) da fraude?

A posição majoritária é que os provedores Internet não devem ser responsabilizados pelas fraudes eletrônicas, embora haja vozes dissonantes[10]. É certo que a página eletrônica utilizada na fraude fica hospedada no sistema informático de um provedor de hospedagem. Se não pratica ou executa o ilícito, nem por isso deixa de fornecer os meios materiais e físicos (tecnológicos) para a sua realização. Embora não seja o responsável pela fraude, é no seu sistema que o conteúdo do sítio falso é armazenado, o que, de certo modo e em certa extensão, pode relacioná-lo com ou vinculá-lo ao autor direto do ato.

Essa relação que o provedor pode ter com alguém que eventualmente contrata seus serviços para hospedar o sítio fraudulento, contudo, não é suficiente, por si só, para acarretar

---

[9] KOPROWSKI, Gene S. *Tough State Laws Won't Stop "Phishing" Scams, Experts Say*, TechnewsWorld, 29 Out 2005. Disponível em: <http://www.technewsworld.com/story/46889.html>. Acesso em: 03 mar. 2012.

[10] CALMAN, Camille. *Bigger Phish to Fry:* California's Antiphishing Statute and its potential imposition of secondary liability on Internet Service Providers. Richmond Journal of Law & Technology v. 13, Issue 1. 2006. Disponível em: <http://law.richmond.edu/jolt/v13i1/article2.pdf>. Acesso em: 10 mar. 2012.

sua responsabilização. O princípio geral que se tem consagrado em torno da atividade dos provedores Internet é o da não responsabilização por material informacional ilícito colocado por terceiro. O provedor não tem uma "obrigação geral de vigilância" sobre as informações que os usuários do sistema transmitem ou armazenam, bem como não tem uma "obrigação geral de procurar ativamente fatos ou circunstâncias que indiciem ilicitudes". Simplesmente atua provendo a infraestrutura técnica para acesso à rede de comunicação, serviço que não acarreta uma coobrigação de controle de conteúdo, de zoneamento visando à exclusão de informação ou material ilícito. Assim, prevalece um princípio geral de irresponsabilidade do provedor por material ilícito, depositado pelos usuários ou que de qualquer forma transita em seu sistema informático.

Assim, parece incontestável que o provedor Internet não é responsável pelo conteúdo dos sítios que hospeda, uma vez que sobre eles não tem qualquer ingerência. O sítio é como um cofre no qual seu proprietário guarda o que lhe for conveniente ou útil; o provedor apenas o armazena.

Como não tem acesso ao conteúdo do cofre, por ele não pode se responsabilizar. Aberto, contudo, esse cofre e verificada a ilegalidade do conteúdo, assiste ao provedor o dever de imediata interrupção do serviço, sob pena de também ser corresponsabilizado, conforme afirma Fernando Antônio Vasconcelos[11]:

> Para que o hosting fosse responsável, necessitaria que o usuário, sentindo-se prejudicado, comunicasse que, em determinado local, estaria acontecendo um fato antijurídico. Se, devidamente alertado, o hospedeiro não tomasse qualquer providência, aí sim, seria considerado responsável, pois teria se omitido na prevenção ou coibição de um fato danoso.

Esse princípio da irresponsabilidade do provedor se sustenta em uma constatação de ordem prática: de que em razão das enormes quantidades de material informacional que abriga em seu sistema, o provedor não tem como fiscalizar todo o seu conteúdo. A grande

[11] VASCONCELOS, Fernando Antônio de. *Internet:* Responsabilidade dos provedores pelos danos praticados. Curitiba: Juruá, 2007, p. 37.

massa de informações que transita no sistema informático de um provedor decorre da circunstância de que qualquer usuário da rede pode atuar como um emitente da informação, aumentando numa quantidade extraordinária o volume de mensagens circulantes e impedindo, com isso, o controle absoluto sobre o manancial informativo.

No entanto, considera-se que o provedor é responsável pelo conteúdo indevido de sítios hospedados em seu sistema quando tem prévio conhecimento da ilicitude do material informacional e não toma qualquer providência no sentido de fazer cessá-la (por exemplo, retirando a página ou sítio que contenha esse material). A mesma lógica pode ser aplicada às fraudes eletrônicas, embora o provedor, em se tratando desse tipo de golpe, na prática nem sequer pode ser acusado de inércia na remoção do conteúdo ilícito, pois em geral as páginas são removidas logo após a execução do golpe.

4.3 Responsabilidade de terceiros

Em casos bastante peculiares, a falha pode estar no meio da comunicação entre os usuários e o banco provedor do serviço de *Internet Banking*, ou em equipamentos necessários a essa comunicação.

Por exemplo, recentemente foram descobertas vulnerabilidades em *modems* de tecnologia ADSL (*Asymmetric Digital Subscriber Line)*, permitindo redirecionamentos que permitiriam o roubo de senhas dos usuários, sem a instalação de qualquer tipo de vírus em seus computadores[12]. Essas vulnerabilidades não se restrigiam a um modelo específico, mas no próprio conjunto de *chips* eletrônicos usados nos equipamentos, o que ampliava a vulnerabilidade a uma vasta gama de fabricantes e modelos de *modems* que se utilizavam desse *chipset*.

[12] SEGURANÇA EM MODEM ADSL. Disponível em <http://g1.globo.com/platb/seguranca-digital/2012/03/20/fabricantes-de-modem-anunciam-correcao-de-falha-que-permite-fraudes>.Acesso em: 04 abr. 2012.

Nessas situações, fica evidente que não há culpa exclusiva da vítima, visto que não teria havido da sua parte nenhuma atitude ou omissão que levasse à referida falha de segurança. Seria uma clara situação de culpa exclusiva de terceiros, devendo ser esses considerados responsáveis por danos que tenham como causa um erro na prestação do serviço.

No caso citado dos *modems* com vulnerabilidades, se esses vierem a apresentar qualquer problema que cause um prejuízo ao consumidor, a empresa que o cedeu ou fabricou seria responsável e deveria ressarcir o cliente pelos danos. Essa responsabilidade, por força do CDC, seria solidária e valeria tanto para os fabricantes e fornecedores quanto para a operadora de telefonia, quando essa cedesse o equipamento de comunicação para o usuário, prática comercial essa bastante comum nos dias atuais.

Porém, a grande dificuldade está na obtenção de provas que foi essa a causa que permitiu a fraude eletrônica. Em uma situação real, seria muito difícil ao usuário, ou ao banco, provar que a fraude eletrônica foi proveniente de uma falha de equipamentos de terceiro, sendo, via de regra, necessária uma análise técnica mais detalhada do caso concreto, para se chegar a tal conclusão.

Essa identificação poderia ser mais facilmente obtida se tal vulnerabilidade fosse conhecida no mercado, mas geralmente muitas delas não o são.

4.4 Responsabilidade dos bancos

Dentre os partícipes da cadeia de comunicação bancária, é o banco, como prestador dos serviços de *Internet Banking*, que está mais visivelmente posicionado de forma a interferir e impedir os efeitos da ação dos fraudadores. Por ser a parte que controla tecnicamente o acesso ao referido serviço, pode prevenir os ataques de forma mais eficaz do que qualquer outro agente intermediário da cadeia eletrônica de comunicação. E é justamente por isso que

pode ser chamado à responsabilização, para reparar os efeitos patrimoniais do ilícito. Além do mais, nenhum outro intermediário da cadeia de comunicação informática está tão ligado à vítima de fraude eletrônica do que o seu próprio banco, com quem mantém uma relação contratual de prestação de serviços *online*.

A visão de que as fraudes eletrônicas são ataques que se executam de forma completamente externa ao sistema do banco, também não é apropriada. Na verdade, os computadores pessoais dos clientes são uma extensão do sistema de *Internet Banking*. Os bancos poderiam fornecer computadores dotados de programas atualizados de proteção contra golpes cibernéticos, mas, por questões práticas e financeiras, optaram em utilizar os próprios computadores pessoais dos clientes como um recurso disponível. Essa deliberada opção tem o condão de vinculá-los a um mais elevado grau de riscos e perdas.

As perdas decorrentes das fraudes financeiras devem integrar os custos do sistema escolhido. Já que os bancos escolheram permitir aos usuários se valerem dos seus computadores pessoais para, por meio da rede mundial, fazer conexão com o *Internet Banking*, toda a rede, nesse caso, se considera como uma extensão do sistema. Encarada a questão por esse ângulo, a fraude dirigida ou cometida contra o computador pessoal do cliente do banco pode ser comparada à fraude que é cometida contra o cliente no interior de uma agência bancária ou caixa eletrônico. Assim, pode-se justificar a responsabilização do banco pela não adoção de dispositivos eficientes de proteção contra o *phishing*[13], ficando caracterizada uma falha desse serviço.

Reforçando essa hipótese, existe ainda o argumento de que a responsabilidade deve ser imposta a quem é capaz de detectar a ação criminosa e preveni-la. Os bancos têm a capacidade tecnológica para prevenir as transações fraudulentas, já que são os únicos com acesso a todos os dados e com habilidade para evoluir seus sistemas. Além do mais, os custos

[13] REINALDO FILHO, op. cit., p. 1.

econômicos para o desenvolvimento de ferramentas tecnológicas de combates a fraudes tecnológicas são razoáveis, em relação aos prejuízos que buscam prevenir. Assim, deve ser reconhecido o papel de interesse público que as instituições bancárias devem ter na atribuição de segurança a essas transações.

4.4.1 O caráter objetivo da responsabilidade dos bancos

Nos serviços de *Internet Banking*, a responsabilidade do banco é uma responsabilidade de origem contratual e o vínculo que o prende ao seu cliente forma uma relação de consumo, a ser regida pelas normas do Código de Defesa do Consumidor (CDC)[14]. De fato, o cliente bancário se enquadra no conceito de consumidor definido no art. 2º do CDC, já que adquire e utiliza o serviço de *Internet Banking* na condição de "destinatário final". Por sua vez, a instituição bancária é considerada fornecedora, para fins de aplicação das normas do Código, na medida em que desenvolve atividade de prestação de serviços (art. 3º).

Além disso, ao definir serviço, o art. 3º, § 2º alcança "qualquer atividade fornecida no mercado de consumo, mediante remuneração, inclusive as de natureza bancária". Tal entendimento já se encontra inclusive consolidado, através do enunciado 297 da súmula do Superior Tribunal de Justiça.

As fraudes eletrônicas têm como principal consequência o surgimento de prejuízos de ordem material ao consumidor, eventualmente podendo até ocorrer danos morais. Em função disso, há uma discussão se elas podem ser caracterizadas como vício ou defeito do serviço. Entre os doutrinadores que sustentam a posição de que as fraudes eletrônicas são vícios do serviço, dado que a vítima não é afetada pela fraude em sua integridade física ou

[14] BRASIL. Lei n. 8.078, de 11 set. 1990. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L8078compilado.htm>. Acesso em: 28 fev. 2012.

psíquica, está Demócrito Reinaldo Filho[15]. Assim, segundo ele, não se configura o instituto do fato do serviço e não se poderia invocar a aplicação do art. 14 do CDC como fundamento da responsabilidade do banco (fornecedor). A situação pode ser representativa apenas de um típico vício por inadequação do serviço (de *Internet Banking*), enquadrando-se no descritor normativo do art. 20, para efeito de justificar a responsabilização do prestador do serviço falho ou inadequado.

Porém, em visão discordante, Sérgio Cavalieri Filho[16], no seu livro Programa de Direito do Consumidor, tende a caracterizar a situação como fato do serviço, ou acidente de consumo, conforme se pode verificar nesse trecho transcrito:

> A palavra-chave neste ponto é defeito. Ambos decorrem de um defeito do produto, só que no fato do produto ou do serviço o defeito é tão grave que provoca um acidente que atinge o consumidor, causando-lhe dano material ou moral. O defeito compromete a segurança do produto ou serviço. Vício, por sua vez, é defeito menos grave, circunscrito ao produto ou serviço em si; um defeito que lhe é inerente ou intrínseco, que apenas causa o seu mau funcionamento ou não-funcionamento.

Para ele e boa parte da doutrina, o vício do serviço se caracteriza como uma imperfeição na sua prestação, ligada à expectativa do consumidor, ao passo que o serviço é defeituoso quando ele é mais perigoso para o consumidor ou usuário do que legitimamente se podia esperar. E esse perigo não precisa necessariamente envolver um risco à integridade física ou psíquica do consumidor. Basta envolver qualquer dano a ele, inclusive de ordem patrimonial, como no caso das fraudes eletrônicas. Tal entendimento parece ser mais acertado, por ser mais protetivo ao consumidor.

Concretamente, o CDC impõe aos fornecedores a obrigação de liberar no mercado somente produtos e serviços isentos de defeitos. Trata-se de uma obrigação de resultado, não importa perquirir a culpa de algum dos fornecedores da cadeia. O importante é o defeito, que será reclamado, normalmente, perante o comerciante direto, último elemento na cadeia de

[15] REINALDO FILHO, op. cit., p. 1.
[16] CAVALIERI FILHO, Sérgio Cavalieri. *Programa de Direito do Consumidor.* São Paulo: Atlas. 2008, p.240-241.

fornecimento.

Cláudia Lima Marques[17] é quem melhor explica que o CDC criou uma responsabilidade especial, um sistema específico para disciplinar a relação do fornecedor de produtos e serviços com o consumidor.

De acordo com ela, o fundamento desta responsabilidade tem origem na teoria da qualidade, segundo a qual os produtos e serviços prestados trariam em si uma garantia de adequação para o seu uso e uma garantia de segurança.

Nesse sentido, todo fornecedor tem um dever de qualidade, considerado um dever anexo à própria atividade produtiva no mercado de consumo. Portanto, o CDC impôs um dever legal para o fornecedor, uma garantia implícita de adequação e segurança dos seus produtos e serviços. Só há violação desse dever ou garantia se o bem introduzido no mercado apresenta um vício de qualidade ou defeito de segurança.

Assim, para se estabelecer a responsabilidade do fornecedor pela reparação de danos não se deve perquirir se agiu com a diligência necessária (noção de culpa) ou o grau de risco criado pela sua atividade (fundamento da responsabilidade objetiva), mas se faltou com o dever de qualidade, ao inserir no mercado um produto ou serviço imprestável ou inseguro, causando uma frustração da expectativa do consumidor, no caso de vício, ou algum tipo de dano, no caso de defeito.

Ao comentar o CDC, Cláudia Lima Marques[18] volta a enfatizar que o esquema peculiar criado pelo diploma consumerista confere pouco valor ao agir do prestador de serviço, na definição da responsabilidade:

> [...] isto porque concentra-se na funcionalidade, na adequação do serviço prestado e não na subjetiva existência de diligência normal ou de uma eventual negligência do prestador de serviços e de seus prepostos. A prestação de um serviço adequado passa a ser a regra, não bastando que o fornecedor tenha prestado o serviço com

[17] MARQUES, Cláudia Lima. *Comentários ao código de defesa do consumidor.* 2 ed. São Paulo: Revista dos Tribunais, 2006, p. 259.
[18] *Ibid.*, p. 359.

diligência".

Como se observa, para fins de determinação dos limites da responsabilidade do fornecedor de serviços, o jurista deve se concentrar na análise do defeito encontrado. A sua existência pressupõe o descumprimento de um dever anexo do fornecedor, um dever de qualidade, dever de adequação do serviço à finalidade a que se destina. Assentada essa teoria da qualidade, a definição da responsabilidade do banco em reparar os danos sofridos por seu cliente, passa necessariamente pela análise da funcionalidade do serviço de *Internet Banking* oferecido.

E aqui, pelas razões já expostas anteriormente, deve-se entender que um sistema de *Internet Banking* que não proteja o usuário contra as fraudes eletrônicas não pode ser encarado como isento de defeito. Somente os bancos têm condições técnicas para monitorar, detectar e prevenir transações fraudulentas, além de capacidade econômica para investir no desenvolvimento de soluções tecnológicas para combatê-las. Portanto, deve haver um reconhecimento generalizado de que se o banco não desenvolve dispositivos capazes de eliminar esse tipo de praga tecnológica, o serviço de *Internet Banking* que oferece no mercado é defeituoso, inadequado às finalidades que dele se espera, inclusive gerando riscos patrimoniais ao usuário bancário.

O cliente desse serviço tem uma legítima expectativa de proteção contra fraudes eletrônicas e, se o referido serviço não atende a essa expectativa, não se mostra adequado para realizar a finalidade que razoavelmente dele se espera.

Comprovando este entendimento, pode-se verificar que muitos bancos têm aplicado, nos últimos anos, reforços significativos de segurança tecnológica nos seus sistemas de *Internet Banking*. Por exemplo, vários bancos implantaram o uso de teclado virtual, para evitar que as senhas digitadas sejam capturadas por artefatos maliciosos capturadores de teclado (conhecidos como *keyloggers*). Outros cadastram previamente os computadores dos

clientes, só permitindo o acesso aos serviços bancários a partir desses equipamentos cadastrados. O uso de *tokens* e certificados digitais também vêm sendo gradativamente ampliado, como forma de implantação de uma autenticação mais forte, não apenas baseada apenas em senhas, notadamente frágeis e sujeitas a vários tipos de fraude.

Mecanismos como esses reforçam a segurança dos sistemas de *Internet Banking*, mas não evitam o *phishing*, por exemplo. Para isto, o sistema deve pedir outras informações pessoais, constante no cadastro dos clientes que apenas o banco possua, como por exemplo, data de nascimento, endereço e nome dos pais. Assim, apenas o redirecionamento para um sítio falso e a boa fé do usuário não seriam suficientes para a fraude se consumar, pois o fraudador não teria a posse dessas informações, ficando mais simples para o cliente perceber que está sendo logrado.

4.5 A Jurisprudência brasileira e internacional

Existem poucos casos na jurisprudência brasileira e internacional que tratam das fraudes eletrônicas no *Internet Banking*, dado que se trata de uma questão tecnológica relativamente nova.

No Brasil, o STJ já realizou julgados sobre fraude em sistema eletrônico de pagamentos. Uma ementa[19] extraída desses julgados está assim expressa:

> RECURSO ESPECIAL - RESPONSABILIDADE CIVIL - AÇÃO DE INDENIZAÇÃO - DANOS MATERIAIS - SAQUES INDEVIDOS EM CONTA-CORRENTE – CULPA EXCLUSIVA DA VÍTIMA - ART. 14, § 3º DO CDC - IMPROCEDÊNCIA.
>
> Conforme precedentes desta Corte, em relação ao uso do serviço de conta-corrente fornecido pelas instituições bancárias, cabe ao correntista cuidar pessoalmente da guarda de seu cartão magnético e sigilo de sua senha pessoal no momento em que deles faz uso. Não pode ceder o cartão a quem quer que seja, muito menos fornecer sua senha a terceiros. Ao agir dessa forma, passa a assumir os riscos de sua conduta,

[19] BRASIL. Superior Tribunal de Justiça. REsp 601805-SP, rel. Min. Jorge Scartezzini, j. 20.10.05, DJ 14.11.05. Disponível em:<http://www.jusbrasil.com.br/ filedown/dev0/files/JUS2/STJ/IT/ RESP_601805_SP_20.10.2005. pdf.> Acesso em: 02 mar. 2012.

> que contribui, à toda evidência, para que seja vítima de fraudadores e estelionatários. (RESP 602680/BA, Rel. Min. FERNANDO GONÇALVES, DJU de 16.11.2004; RESP 417835/AL, Rel. Min. ALDIR PASSARINHO JÚNIOR, DJU de 19.08.2002).
> Fica excluída a responsabilidade da instituição financeira nos casos em que o fornecedor de serviços comprovar que o defeito inexiste ou que, apesar de existir, a culpa é exclusiva do consumidor ou de terceiro (art. 14, § 3º do CDC).
> Recurso conhecido e provido para restabelecer a r. sentença .

Essa decisão reconhece que a funcionalidade do serviço eletrônico do banco pressupõe a utilização de senha pessoal e dispositivos de segurança, que são exclusivos do cliente e intransferíveis, assumindo este a obrigação de zelar pela sua guarda e sigilo. Havendo quebra desse dever, entende-se que não há relação de causalidade entre a atuação do banco e o prejuízo eventualmente gerado por esse descuido.

No entanto, o julgado ainda não trata especificamente das fraudes eletrônicas, mas demonstra a necessidade de o usuário zelar por suas informações pessoais e sigilosas. No caso das fraudes, essa consequência da falta de zelo só se aplica nas situações em que o banco tenha implantado um mecanismo mais sofisticado de autenticação, pois caso contrário, as informações pessoais e sigilosas do cliente teriam sido furtadas não por negligência deste, mas por armadilhas bem montadas por fraudadores.

Deve-se observar, no entanto, que tais fraudes só puderam ser levadas adiante devido a falhas tecnológicas no serviço de *Internet Banking* oferecido.

Em decisão mais recente, o STJ publicou o seguinte julgado[20] sobre o tema, em março de 2010:

> EMENTA
>
> RESPONSABILIDADE CIVIL. DÉBITOS EFETUADOS EM CONTA CORRENTE DO AUTOR, MOVIMENTAÇÃO MEDIANTE SERVIÇO DISPONIBILIZADO PELO BANCO VIA INTERNET. FRAUDE. DEVER DO BANCO INDENIZAR. AGRAVO REGIMENTAL A QUE SE NEGA PROVIMENTO.
>
> VOTO

[20] BRASIL.Superior Tribunal de Justiça. AgRg no AGRAVO DE INSTRUMENTO Nº 940.608 - RJ (2007/0195173-7). Disponível em: < https://ww2.stj.jus.br/revistaeletronica/Abre_Documento.asp?sLink=ATC&sSeq=8337662&sReg=200701951737&sData=20100322&sTipo=91&formato=PDF>. Acesso em: 06 abr.2012.

> O SR. MINISTRO LUIS FELIPE SALOMÃO (Relator):
>
> A insurgência não comporta provimento.
> Além do acerto da decisão quando diz que "quanto ao rompimento do nexo causal, a configuração da responsabilidade, na espécie, independe da atuação ilícita de terceiro, tendo em vista que o panorama fático descrito no acórdão objurgado revela a ocorrência do chamado caso fortuito interno" merecem confirmação os fundamentos do decisório impugnado que se encontram na linha do entendimento jurisprudencial deste STJ: [...]

Como se pode verificar, esse precedente do STJ expressou o entendimento de que a situação de fraude eletrônica no *Internet Banking* é caso de fortuito interno da atividade bancária, inerente ao próprio serviço oferecido e, assim sendo, caberia ao banco assumir a responsabilidade.

Reforçando tal entendimento, aconteceu na Índia, em dezembro de 2009, um primeiro caso em que um banco absorveu a responsabilidade por um caso de *phishing*, envolvendo um prejuízo de 28.000 rúpias[21].

A Suprema Corte da Índia entendeu que um banco não teria responsabilidade em uma fraude eletrônica apenas se pudesse provar que o cliente estava ciente que a mesma estava em curso. Como tal prova não foi apresentada nos autos, a decisão foi pela responsabilização do banco.

CONCLUSÃO

A legislação que objetiva a punição exclusiva do agente direto, praticante da fraude eletrônica, não produz resultado satisfatório em termos de resposta à pessoa da vítima. Como os fraudadores utilizam técnicas que favorecem o anonimato, quase sempre não conseguem ser identificados, permanecendo a vítima sem a restauração de seu patrimônio. Daí a necessidade da responsabilização de outro intermediário da comunicação eletrônica, para

[21] Blogger Network News. Disponível em: <http://www.bloggernews.net/124283>. Acesso em: 03 mar. 2012.

suportar o ônus de reparar o dano causado à vítima da fraude.

É inviável tentar responsabilizar o provedor Internet pelos prejuízos decorrentes das fraudes financeiras, porque não tem uma "obrigação geral de vigilância" sobre o conteúdo do material que hospeda ou sobre as informações que os usuários transmitem através de seu sistema informático. Apenas por inércia na remoção do conteúdo ilícito, quando comunicado da presença de um sítio falso hospedado em seu sistema, o provedor poderia ser responsabilizado.

Dentre os participantes da cadeia de comunicação telemática, é o banco que está mais visivelmente posicionado de forma a interferir e impedir os efeitos da ação do fraudador eletrônico.

Por ser a parte que controla tecnicamente o acesso ao serviço de *Internet Banking*, pode prevenir os ataques de forma mais eficaz do que qualquer outro agente intermediário da cadeia eletrônica de comunicação. Além disso, nenhum outro intermediário da cadeia de comunicação informática está tão ligado à vítima da fraude do que o seu próprio banco, com quem mantém uma relação contratual para prestação do citado serviço.

No regime dos defeitos do serviço, tratados no CDC, o que é relevante para definir a responsabilidade não é o aspecto subjetivo da conduta do fornecedor (banco). Na definição do dever de reparação, o importante é um dado objetivo: se o serviço (*de Internet Banking*) é falho (defeituoso) ou não. E um sistema de *Internet Banking* que não proteja o usuário contra as fraudes eletrônicas não pode ser encarado como isento de defeito. O cliente desse serviço tem uma legítima expectativa de proteção e, se não atende a essa expectativa, não se mostra adequado para realizar a finalidade que razoavelmente dele se espera.

Como a definição da responsabilidade passa necessariamente pela análise da adequação do serviço, ou seja, se não padece de defeito que comprometa sua funcionalidade, o dever de reparação dos danos de cliente bancário vai exigir, em cada caso, a investigação

das ferramentas tecnológicas que o banco emprega, em seu sistema informático, para proteger o usuário desse tipo de cilada eletrônica. A premissa deve ser a de que o banco que não tenha instalado métodos de autenticação com mais de um nível de segurança deva ser responsabilizado pelos prejuízos patrimoniais causados pelo fraudador ao seu cliente. O defeito é que fundamenta o dever de reparação do fornecedor; sem ele, não pode ser condenado a reparar os danos provenientes da fraude eletrônica, já que a origem dos prejuízos, nessa hipótese, é considerada como do âmbito da conduta do próprio cliente. Portanto, um serviço de *Internet Banking* que disponha de vários níveis de autenticação não possui um defeito de inadequação, e sem esse defeito, o banco não pode ser responsabilizado por eventuais prejuízos, cuja causa, nesse caso, se entende como sendo por fato exclusivo da vítima.

REFERÊNCIAS

AUBY, Jean-Marie *apud* GRINOVER, Ada Pellegrini et al . *Código Brasileiro de Defesa do Consumidor comentado pelos autores do Anteprojeto*. 9. ed. Rio de Janeiro: Forense Universitária, 2007.

BRASIL. Lei n. 8.078, de 11 set. 1990. Disponível em: <http://www.planalto.gov.br/ ccivil_03/leis/ L8078compilado.htm>. Acesso em: 29 set 2011.

CALAIS-AULOY, Jean. *Droit de la consommation*. 6. ed. Dalloz: Paris, 2003.

CALMAN, Camille. *Bigger Phish to Fry: California's Antiphishing Statute and its potential imposition of secondary liability on Internet Service Providers.* Richmond Journal of Law & Technology v. 13, Issue 1. 2006. Disponível em: <http://law.richmond.edu/jolt/ v13i1/article2.pdf>. Acesso em: 10 set 2011.

CAVALIERI FILHO, Sérgio Cavalieri. *Programa de Direito do Consumidor*. São Paulo : Atlas. 2008.

KOPROWSKI, Gene S. *Tough State Laws Won't Stop "Phishing" Scams, Experts Say*, TechnewsWorld, 29 Out 2005. Disponível em: <http://www.technewsworld.com/story/ 46889.html>. Acesso em: 03 set 2011.

MARQUES, Cláudia Lima. *Comentários ao código de defesa do consumidor*. 2. ed. São Paulo: Revista dos Tribunais, 2006.

NERY JR, Nelson. *Código de Processo Civil Comentado e legislação processual civil extravagante em vigor*. 4. ed. São Paulo: Revista dos Tribunais, 2006.

PECK, Patrícia. *Direito digital*. São Paulo: Saraiva, 2007.

REINALDO FILHO, Demócrito. *A responsabilidade dos bancos pelos prejuízos resultantes do "phishing"*. Jus Navigandi, Teresina, ano 12, n. 1836, 11 jul. 2008. Disponível em: <http://jus2.uol.com.br/doutrina/texto.asp?id=11481>. Acesso em: 15 set 2011.

VASCONCELOS, Fernando Antônio de. *Internet: Responsabilidade dos provedores pelos danos praticados.* Curitiba: Juruá, 2007.