

A RESPONSABILIDADE DOS BANCOS PELOS PREJUÍZOS RESULTANTES DO PHISHING

Demócrito Reinaldo Filho

Juiz de Direito (32^a. Vara Cível do Recife)

Sumário: 1- Introdução. 2- Definições; 2.1 – Definição de *phishing*; 2.2- Definição de *pharming*; 2.3- Definição de *DNS poisoning*; 3- Inviabilidade de se responsabilizar o provedor de acesso à Internet ou de hospedagem; 4- Inviabilidade de se responsabilizar os provedores de serviços de e-mail; 5- Insuficiência das leis que criminalizam a conduta do ofensor direto (*phisher*); 6. Teoria da responsabilidade dos bancos prestadores de serviços de *Internetbanking*; a) argumento de ordem econômica; b) incentivo ao desenvolvimento de ferramentas tecnológicas; c) argumento da possibilidade técnica de evitar a fraude; 6.1. Adequação do novo padrão de responsabilidade à legislação existente; 6.1.1 Responsabilidade contratual regida pelo CDC. 7. Soluções tecnológicas empregadas pelos bancos para evitar fraudes eletrônicas . a) *Firewall*. b) Criptografia de dados (SSL); c) Teclado Virtual; d) Certificado Digital. 8. Proporção entre adoção de práticas seguras pelos bancos e a diminuição do grau de responsabilização. 9. Conclusões

1- Introdução

O desenvolvimento do comércio eletrônico está intimamente relacionado com as medidas que os legisladores e juizes adotam em respeito a certos temas que assomam no ciberespaço. O incremento dos negócios e a evolução da própria rede dependem de como os legisladores e as cortes judiciais se posicionam em relação a conflitos que surgem a cada dia. Um exemplo de decisão judicial que certamente tem impacto no mundo dos negócios na rede mundial é aquela relacionada com a responsabilidade civil dos bancos por ataques de *phishing*¹. Dependendo de como os tribunais e juizes passem a decidir essa questão, responsabilizando (ou não) os bancos pela reparação dos seus clientes, vítimas desse tipo de fraude tecnológica, pode haver alteração no modelo de negócios hoje estabelecido e disseminado na rede. Não é difícil, por exemplo, prever uma diminuição da utilização dos serviços bancários *on line*, se os clientes de banco

¹ O Departamento de Justiça dos EUA define *phishing* como “criação e uso criminosos de e-mails e websites, desenhados para parecer como renomadas e legítimas empresas, instituições financeiras e agências governamentais, de modo a enganar usuários de Internet para que revelem suas informações bancárias e financeiras ou outro dado pessoal como nome de usuário e senhas” (em DEPARTMENT OF JUSTICE, SPECIAL REPORT ON “PHISHING” (2004), disponível em: <http://www.usdoj.gov/criminal/fraud/Phishing.pdf>)

perderem a certeza quanto a uma reparação completa dos danos financeiros decorrentes do *phishing*. Por outro lado, os bancos certamente procederão a modificações no modelo de relacionamento bancário na Internet, se a Justiça se inclinar a responsabilizá-los de forma objetiva por toda e qualquer fraude financeira.

Como se vê, o tema da responsabilidade dos bancos no ressarcimento dos prejuízos causados pelos ataques de *phishing* é realmente delicado, e de interesse de todo o conjunto da sociedade, em razão da disseminação dos serviços de *Internetbanking*², já tão incorporados ao nosso dia-a-dia e sem os quais não mais seria possível o atendimento bancário de forma eficiente. Sem o uso das tecnologias da informação, sobretudo a utilização da rede mundial de comunicação (Internet), na prestação dos serviços bancários, é certo dizer que seria impraticável o fornecimento desses serviços de forma massificada, conveniente e eficiente, tal qual são prestados atualmente. O maior desafio nessa área, no entanto, é superar os problemas de segurança e definir responsabilidades pelas conseqüências de ataques e invasões de sistemas informáticos. Definir, com precisão, as responsabilidades dos prestadores dos serviços bancários *on line* ajuda a impulsionar o desenvolvimento desse mercado, já que elimina as incertezas quanto a quem deve e em quais circunstâncias arcar com os prejuízos do *phishing* e outras práticas tecnológicas fraudulentas.

Acontece que estabelecer esquemas de atribuição de responsabilidade civil nesse contexto não é tão fácil, dada a intrincada cadeia de papéis e funções que cada um dos atores da comunicação informática assume. Para propiciar a comunicação na prestação do serviço de *Internetbanking*, exige-se algum tipo de envolvimento ou participação do provedor de Internet, do fabricante do programa gerenciador de e-mail, do fabricante dos softwares e soluções de segurança, do fabricante do software de navegação, da instituição bancária, da pessoa que desenvolve e dá manutenção ao sistema (de *Internetbanking*) e do próprio internauta (cliente do banco). É justamente a participação e o envolvimento desses diversos atores da comunicação informática que faz com que se torne difícil definir qual deles e em quais circunstâncias pode ser responsabilizado a reparar os prejuízos financeiros resultantes de fraudes tecnológicas como o *phishing*. Isso faz com que esse tema se torne pouco explorado e dos mais complexos.

A complexidade e a importância do tema nos instigou a incursionar na matéria, para colaborar na tarefa de definir esquemas de imputação de responsabilidade aos prestadores de serviços bancários *on line*. O aumento

² **Banco** **internético** (do inglês *internet banking*), **banco online**, *online banking*, às vezes também **banco virtual**, **banco eletrônico** ou **banco doméstico**, são termos utilizados para caracterizar transações, pagamentos etc. pela Internet por meio de uma página segura de banco. Esse sistema permite ao usuário utilizar os serviços do banco fora do horário de atendimento ou de qualquer lugar onde haja acesso à Internet. Na maioria dos casos, um programa navegador (como o Internet Explorer ou o Mozilla Firefox) e qualquer conexão à Internet são suficientes, não sendo necessário nenhum software ou hardware adicional.

gradativo dos ataques de *phishing* nos últimos anos³, e a apreensão que isso tem causado ao comércio eletrônico, também nos estimulou a escolher esse tema como foco de nossa investigação científica. A falta de trabalhos doutrinários sobre a matéria da mesma forma funcionou como fator decisivo na escolha da definição do campo de pesquisa. Pelo menos até onde sabemos, não há registro na doutrina brasileira de qualquer trabalho sobre a questão da responsabilidade civil dos bancos pelas conseqüências dos ataques de *phishing*. Mesmo na doutrina alienígena (de acordo com pesquisa que fizemos na Internet)⁴, não encontramos referência a qualquer artigo ou ensaio científico sobre esse assunto. Alguns autores estrangeiros escreveram sobre a possibilidade da responsabilização dos intermediários da comunicação eletrônica (como os provedores de acesso à Internet)⁵, mas não especificamente sobre a responsabilidade civil dos bancos diante desse tipo de fraude financeira.

No nosso trabalho, procuraremos identificar o esquema de imputação de responsabilidade - se baseado na culpa, fundado no dever objetivo de reparar o dano (responsabilidade objetiva) ou apoiado na noção de *vício* (do serviço) - que melhor se enquadra aos bancos, em face dessas situações (ataques fraudulentos). Em outro trecho, mostraremos a inviabilidade de se responsabilizar o provedor de acesso à Internet pelos prejuízos decorrentes do *phishing*.

É importante esclarecer que só iremos tratar da responsabilização do banco pelos tipos primitivos (e mais conhecido) de *phishing*, aqueles que pressupõem sempre o logro ao destinatário de uma mensagem eletrônica (e-mail), que o faz repassar suas informações pessoais (bancárias) ao criminoso (fraudador), seja clicando num *link* (que descarrega o vírus), abrindo arquivo anexo (que contém o vírus) ou inserindo manualmente informações em um *site* falso. Em ambas essas situações, o indivíduo recebe previamente a mensagem de e-mail enganosa, induzindo-o a abrir o arquivo anexo contendo vírus ou a clicar em um *link* que descarrega o vírus ou o leva para um *site* falso.

Esses são os casos mais comuns de “identity theft” (furto de identidade, traduzido para o português) cometidos com uso de comunicações eletrônicas, em que o primeiro estágio da fraude consiste no logro do usuário do serviço de *Internetbanking*, levando-o a pensar que está fornecendo suas informações pessoais à instituição confiável, com quem mantém relação contratual, quando na verdade está repassando seus dados bancários ao *phisher* (agente do crime de *phishing*). O destinatário da mensagem também é enganado quando é induzido a

³ Os incidentes de *phishing* têm crescido dramaticamente desde 2003. Sobre as taxas de crescimento desse tipo de fraude, recomendamos a leitura do ANTI-PHISHING WORKING GROUP, PHISHING ACTIVITY TRENDS REPORT (de junho de 2006), disponível em: http://www.antiphishing.org/reports/apwg_report_june_2006.pdf

⁴ Inclusive no Google Acadêmico (*Google Scholar*) - <http://scholar.google.com/>

⁵ A exemplo do trabalho de Camille Calman, sob o título: “ BIGGER PHISH TO FRY: CALIFORNIA’S ANTI-PHISHING STATUTE AND ITS POTENTIAL IMPOSITION OF SECONDARY LIABILITY ON INTERNET SERVICE PROVIDERS”, publicado na *Richmond Journal of Law & Technology*, Volume XIII, Issue 1.

clicar sobre um *link* (no corpo da própria mensagem) ou abrir arquivo anexado a ela, ação que descarrega um programa malicioso (*malware*) que se apodera de seu computador e repassa as informações nele contidas ao *phisher*, ou intercepta as comunicações feitas pelo terminal infectado com os sites de bancos⁶, capturando informações como número de contas e senhas.

Esses tipos de fraudes, portanto, compreendem sempre esse elemento, da burla, do ato ou efeito de enganar a pessoa para que forneça seus dados pessoais. Isso ocorre tanto quando um indivíduo preenche um formulário em um *spoofing* site (site falso estruturado com a aparência do *site* legítimo) ou quando abre um arquivo que contém vírus, o qual é ativado e, apropriando-se de sua máquina (da vítima), funciona repassando os dados contidos no computador para o fraudador (*hacker* ou criminoso cibernético). Em ambas essas situações, o indivíduo recebe previamente a mensagem de e-mail enganosa, induzindo-o a abrir o arquivo anexo contendo vírus ou clicar em um *link* que descarrega o vírus ou o leva para um *site* falso.

Faremos uma exceção para incluir em nosso trabalho um único tipo de fraude que não pressupõe necessariamente, no seu *iter* criminoso, a remessa prévia de uma mensagem de e-mail para o sujeito vítima da trama. Trata-se da fraude conhecida como *pharming*, procedimento que redireciona os programas de navegação (*browsers*) dos internautas para *sites* falsos. Podemos explicar a razão dessa inclusão. Mesmo essa espécie pressupõe um ataque dirigido à pessoa do usuário (cliente) dos serviços bancários, para captura de informações. Mesmo aí ainda há o elemento do logro ao usuário, o qual, apesar de não ter recebido uma mensagem prévia de e-mail⁷, teve seu *browser* direcionado para um *site* falso. O engano corresponde a encarar o *site* falso como legítimo, e por conta desse engano, entrega suas informações pessoais ao criminoso, pensando estar diante do operador do *site* legítimo. O alvo primário do criminoso, mesmo nesse caso de *pharming*, é sempre o cliente bancário (ou seu computador pessoal).

Uma modalidade de *pharming* não será enquadrada dentre os tipos de fraude objeto do nosso estudo, já que nessa hipótese o provedor de acesso à Internet é o juridicamente responsável (na órbita civil) pela reparação de seus efeitos. É o chamado *DNS poisoning* (algo próximo a “envenenamento do DNS”). Nessa modalidade também ocorre, como nos demais casos, uma ação destinada a coletar informações pessoais da vítima (para depois serem utilizadas na fase seguinte do crime). Com o servidor DNS do provedor “envenenado”, e alteradas as configurações de um determinado endereço *web*, o internauta é direcionado para um *site* falso mesmo tecendo o endereço correto. Nessa situação, no entanto, o ataque inicial não foi direcionado ao computador da vítima (cliente do

⁶ Ou também sites de pagamento (como o Paypal), de comércio eletrônico, sites de leilão, etc.

⁷ No caso do *pharming*, a vítima tem seu computador infectado de outras maneiras. Por exemplo, pode acontecer de a pessoa sofrer a inserção de vírus em seu computador simplesmente navegando por páginas da Internet. Esse vírus altera a configuração do programa de navegação da vítima (*browser*), fazendo com que, quando esta tenta acessar um *site* de um banco, por exemplo, o navegador infectado a redireciona para o *site* falso.

banco), mas sim ao sistema informático do seu provedor de Internet, que pode, por essa razão, ser tido como responsável pelas conseqüências do ataque, por falha de segurança do sistema⁸.

Em suma, o nosso trabalho abrange a investigação sobre responsabilização dos bancos em todos aqueles casos em que a fraude tem como alvo primário o cliente bancário. É o seu computador que é infectado por um vírus ou é a própria vítima que, induzida por uma mensagem fraudulenta, repassa as informações para o fraudador. Não se trata de invasão ou ataque direto ao próprio sistema informático do banco, nem tampouco ao do provedor de Internet ou exploração de alguma falha no software de navegação (ou qualquer outro). Todas as modalidades de *phishing* a serem estudadas como pressuposto para a responsabilização do banco (fornecedor do serviço de *Internetbanking*), têm no elemento do logro ao usuário ou infecção do seu computador a origem do procedimento criminoso. São casos em que o alvo primário da fraude é o cliente do banco, de quem (ou de seu computador) são capturadas as informações pessoais para a consecução das etapas seguintes do esquema criminoso. O sistema informático do banco não sofre propriamente um ataque em que são exploradas suas vulnerabilidades ou falhas de segurança, pois o criminoso nele ingressa como se fosse o legítimo usuário (já que se apropria previamente das informações pessoais e sigilosas deste). O acesso se dá pelos meios permitidos pelo próprio sistema, através da digitação da senha e informações do usuário.

É em face desse tipo de fraude ou ação criminosa que examinaremos a responsabilidade do banco, pelos prejuízos econômicos ao patrimônio das vítimas (clientes). Nesse esforço, investigamos se o fundamento da responsabilidade deve ser o do *risco* de sua atividade (responsabilidade objetiva), se deve responder com base no aspecto subjetivo de sua conduta (*culpa*) ou se lhe deve ser reconhecida uma responsabilidade especial (fundada na noção de *vício* do serviço). Uma vez definida a noção de *vício* como fundamento da responsabilização, procuramos apontar quais situações específicas podem denotar a imprestabilidade do serviço *on line* (*vício de inadequação*) capaz de justificar o dever do banco de reparar o dano sofrido por seus clientes.

Estamos certos de que, com esse esforço que ora apresentamos, contribuimos de forma decisiva para a evolução da teoria da responsabilidade civil em nosso país, já que, conforme antes referimos, ainda não existe na doutrina brasileira qualquer trabalho sobre a matéria objeto de nossa investigação.

2- Definições

Antes de passar a examinar propriamente as teorias da responsabilidade civil, salientamos a importância da compreensão dos fenômenos ocorrentes no

⁸ Em artigo que escrevemos anteriormente, já identificamos a responsabilidade do provedor na reparação dos prejuízos sofridos por seu usuário nas hipóteses de “envenenamento” do DNS. Ver “A INFECÇÃO DO SISTEMA DNS: nova modalidade de *phishing* e a responsabilidade do provedor”, artigo publicado no *site* Jus Navigandi - <http://jus2.uol.com.br/doutrina/texto.asp?id=6978>, em julho de 2005.

campo das comunicações informáticas, sem a qual não seria possível o desenvolvimento de raciocínio jurídico para identificar os sujeitos responsáveis pela reparação dos prejuízos econômicos. É preciso, antes de mais nada, saber diferenciar cada um dos aspectos técnicos das diversas modalidades de golpes e truques informáticos com objetivo de furto de informações pessoais, para identificar quem, entre os diversos atores da comunicação informática, pode ser responsabilizado pelos danos causados à vítima (o sujeito que tem os dados pessoais furtados).

A primeira etapa do *phishing* consiste na apropriação de informações de outra pessoa (como nome, informações de conta e senha bancária), para serem utilizadas fraudulentamente nas fases seguintes da trama (transferências de numerários de contas correntes e aplicações financeiras). É um ato de “impersonificação” (numa incorporação para o português do termo inglês *impersonation*), consistente na apropriação de informações pessoais do cliente do banco com finalidades ilegais. O criminoso se apodera da informação de outra pessoa, sem o conhecimento desta, que é enganada de forma fraudulenta. Nesse sentido, o *phishing* pode ser enquadrado na rubrica do “furto de identidade” (*identity theft*), que é a expressão utilizada para denominar de forma genérica o crime de maior tendência ao crescimento nos tempos atuais⁹. O furto de informações pessoais pode ser realizado com as mais diversas finalidades, tanto para imigração ilegal, espionagem, terrorismo ou mesmo para fins aparentemente menos ilícitos, como o marketing e publicidade dirigida. As estratégias para a apropriação dos dados pessoais também podem variar, com a utilização de meios tecnológicos ou não. Os dados podem ser obtidos em *sites* e bancos de dados informáticos ou em qualquer arquivo físico ou fichário. Mas consiste sempre numa exploração dos meios de identificação de uma pessoa para finalidades ilegais. O *phishing*, como espécie de furto de identidade, apenas tem a peculiaridade de ser realizado em ambientes de redes informáticas (Internet) e objetivar o furto de informações específicas (dados bancários), para finalidades também específicas (transferência de numerário existente em contas bancárias)¹⁰. Não deixa, no entanto, de ser uma exploração ilegal de informações pessoais alheias e, como tal, forma específica do crime de “furto de identidade”.

⁹ A expressão inglesa *identity theft* foi utilizada pela primeira vez em 1996, quando a Comissão Federal para o Comércio (*Federal Trade Commission*) alertou para o crescente número de utilização fraudulenta de dados de identificação de consumidores. Depois, a expressão foi incorporada na terminologia literária americana. Em verdade, não é fisicamente possível o furto da identidade de uma pessoa; o que é possível é o furto dos seus meios de identificação.

¹⁰ O *phishing* na verdade tem uma aceção mais ampla, envolvendo qualquer tentativa de fraudulentamente se obter informação sensível como senhas e dados de cartões de crédito ou qualquer outro dado que permita a realização de transação em sistemas de pagamento *on line* (*nonbank payment systems*, como o *Pay Pal* e o *e-Gold*), sites de leilão e de comércio eletrônico em geral. Assim, o *phisher* pode ter como alvo os dados de um usuário e respectivos números da conta e senhas bancárias, para serem utilizados em *sites* de *Internet banking*, ou pode coletar dados de cartão de crédito e senhas utilizadas em *sites* de comércio eletrônico ou de leilão (como o *e-Bay*) e de sistemas de pagamento *on line*. Além disso, o *phishing* não somente pode ser executado por meio do envio de uma mensagem de *e-mail* como também através de comunicação em programas de *instant messaging* e até mesmo por telefone.

Como diversos esquemas inteligentes são empregados para burlar a vítima do *phishing* (e se apoderar de suas informações bancárias) - que pode ter seu computador invadido, ser levada a ingressar em *site* falseado através de *link* em mensagem eletrônica recebida ou ter seu programa navegador infectado (levando-a a um endereço diverso do *site* legítimo, mesmo sem receber qualquer tipo de *e-mail*) -, é imprescindível a visualização e conhecimento das diversas técnicas fraudulentas, para compreender a participação do prestador dos serviços bancários *on line* e dos demais atores da comunicação informática e, dessa forma, poder apontar em quais situações uma determinada conduta justifica a imposição de responsabilização.

Relacionando e compreendendo os mecanismos e objetos necessários à realização de cada ação ou operação fraudulenta, podemos definir responsabilidades na órbita civil, daí a importância da compreensão de conceitos fundamentais como *phishing*, *pharming* e *DNS poisoning*, que são fornecidos nos itens seguintes.

2.1 – Definição de *phishing*

A palavra *phishing*, uma corruptela do verbo inglês *fishing* (pescar, em português), é utilizada para designar alguns tipos de condutas fraudulentas que são cometidas na rede. São muito comuns as mensagens eletrônicas (*e-mails*) onde são feitas propagandas de pechinchas comerciais, são solicitadas renovações de cadastro, são feitos convites para visitação a *sites* pornográficos, são ofertadas gratuitamente soluções técnicas para vírus, entre outras. Não sabe a pessoa que recebe tais tipos de *e-mail* que as mensagens são falsas, enviadas por alguém disposto a aplicar um golpe¹¹. Geralmente, o destinatário é convidado a clicar sobre um *link* que aparece no corpo da mensagem ou abrir um arquivo anexo e, ao fazê-lo, aciona o *download* de um programa malicioso que vai penetrar no seu computador e capturar informações sensíveis. Também ocorre de, ao clicar no *link* sugerido, ser enviado a um *site* falso, com as mesmas características de apresentação gráfica de um *site* popularmente conhecido (a exemplo do *site* um grande banco ou um *site* de comércio eletrônico)¹². Ao chegar no *site* falseado, a pessoa é instada a inserir informações pessoais (número de cartão de crédito ou de conta bancária) e, uma vez de posse dessas informações, o fraudador as utiliza para fazer saques e movimentações bancárias ou outras operações (em nome da vítima).

A categoria delituosa em questão consiste exatamente nisso: em "pescar" ou "fisgar" qualquer incauto ou pessoa desavisada, não acostumada com esse tipo de fraude, servindo a mensagem de e-mail como uma isca, uma forma de

¹¹ As mensagens de *phishing scam* geralmente aparentam provenientes de uma fonte confiável. Os fraudadores manipulam o campo do cabeçalho da mensagem (campo "de:" ou "from:") com o nome do remetente, de forma a que o destinatário pense ser de fonte legítima.

¹² Esse tipo de atividade fraudulenta, em que se usam clones de *websites* com a aparência de *sites* respeitáveis, é também chamada de *spoofing*.

atrair a vítima para o *site* falso (onde será perpetrado o golpe, de furto de suas informações pessoais). O *phishing*, portanto, é uma modalidade de *spam*, em que a mensagem além de indesejada é também fraudulenta (*scam*).

2.2- Definição de *pharming*

Recentemente tem sido registrada uma nova modalidade de ataque *phishing* que não é perpetrada através do envio de mensagens de *e-mail*. Trata-se de um tipo de golpe que redireciona os programas de navegação (*browsers*) dos internautas para *sites* falsos. A essa nova categoria de crime tem sido dado o nome de *pharming*.

O *pharming* opera pelo mesmo princípio do *phishing*, ou seja, fazendo os internautas pensarem que estão acessando um *site* legítimo, quando na verdade não estão. Mas ao contrário do *phishing*, o qual uma pessoa mais atenta pode evitar simplesmente não respondendo ao e-mail fraudulento, o *pharming* é praticamente impossível de ser detectado por um usuário comum da Internet, que não tenha maiores conhecimentos técnicos. Nesse novo tipo de fraude, os agentes criminosos se valem da disseminação de softwares maliciosos que alteram o funcionamento do programa de navegação (*browser*) da vítima. Quando esta tenta acessar um *site* de um banco, por exemplo, o navegador infectado a redireciona para o *spoof site* (o *site* falso com as mesmas características gráficas do *site* verdadeiro). No site falseado, então, ocorre a coleta das informações privadas e sensíveis da vítima, tais como números de cartões de crédito, contas bancárias e senhas.

No crime de *pharming*, como se nota, a vítima não recebe um *e-mail* fraudulento como passo inicial da execução, nem precisa clicar num *link* para ser levada ao *site* "clonado". Uma vez que seu computador esteja infectado pelo vírus, mesmo teclando o endereço (URL) correto do *site* que pretende acessar, o navegador a leva diretamente para site falseado. O *pharming*, portanto, é a nova geração do ataque de *phishing*, apenas sem o uso da "isca" (o *e-mail* com a mensagem enganosa). O vírus reescreve arquivos do PC que são utilizados para converter os endereços de Internet (URL's) em números que formam os endereços IP (números decifráveis pelo computador). Assim, um computador com esses arquivos comprometidos, leva o internauta para o *site* falso, mesmo que este digite corretamente o endereço do *site* intencionado.

2.3- Definição de *DNS poisoning*

A mais preocupante forma de *pharming* é conhecida como "DNS poisoning" (traduzindo para o português, seria algo como "envenenamento do DNS"), por possibilitar um ataque em larga escala. Nessa modalidade, o ataque é dirigido a um servidor DNS¹³, e não a um computador de um internauta isoladamente.

¹³ Notícia publicada na eWeek.com (www.eweek.com), no dia 29.04.05, reporta provável ataque ao servidor da *Network Solutions Inc.*, conhecido registrador de nome de domínios, através do qual *hackers* podem ter

Como se sabe, o sistema DNS (*Domain Name System*) funciona como uma espécie de diretório de endereços da Internet. Toda navegação na Internet (no seu canal gráfico, a *World Wide Web*) tem que passar por um servidor DNS. Quando um internauta digita um determinado endereço *web* na barra de seu navegador (www.ibdi.org.br, por exemplo), o seu computador pessoal se comunica com o servidor do seu provedor local de acesso à Internet, em busca do número IP que corresponde àquele determinado endereço. Se o endereço procurado estiver armazenado no *cache* do servidor do provedor local, então ele mesmo direciona o programa de navegação para o endereço almejado ou, caso contrário, transfere a requisição para servidor de um provedor maior, e assim por diante, até encontrar aquele que reconheça o endereço procurado e faça a correspondência¹⁴.

Um *hacker* pode invadir o servidor DNS de um provedor de acesso à Internet e alterar endereços arquivados na memória *cache*. Se o servidor é "envenenado", alteradas as configurações relativas a um determinado endereço *web*, internautas podem ser direcionados para um *site* falso mesmo teclando o endereço (URL)¹⁵ correto. O ataque, assim praticado, produz resultados em muito maior escala do que a outra forma de *pharming*, em que os "pharmers" vitimam uma pessoa de cada vez, infectando os seus PC's com vírus. O ataque ao servidor DNS de um provedor de Internet pode atingir inúmeros usuários de uma única vez.

O fato é que, se de um ataque a um servidor DNS resultar prejuízo efetivo ao usuário do provedor, este responde pela reparação completa. Se o usuário tiver suas informações colhidas no *site* falso, a que foi levado em função da alteração nas configurações do servidor DNS do seu provedor de acesso à Internet, pode pedir reparação dos danos que venham a resultar do uso indevido dessas informações. Se o "phisher" fizer uso do número de sua conta bancária e senha e sacar valores depositados em sua conta, é o provedor que teve o sistema invadido que deve reparar os prejuízos. A situação aqui é diferente da modalidade simples de ataque de *phishing*, onde a segurança dos serviços do provedor não é comprometida.

alterado as informações do endereço na *Web* da empresa *Hushmail Communications Corp*, de modo a redirecionar os visitantes da URL dessa empresa – hushmail.com – para um *site* falso.

¹⁴ O sistema DNS é formado por uma rede global de servidores, compreendida de 13 servidores raiz espalhados pelo mundo. O original sistema de endereços usava apenas números, de difícil utilização portanto. A partir de 1984 foi introduzido o sistema DNS, permitindo aos usuários utilizar palavras (mais fácil de memorizar) e as organizando em forma de "nomes de domínio". Assim, todo endereço na *web* passou a ser formado por um *nome de domínio* (*domain name*), que tem que ser registrado num sistema central, de maneira a que corresponda a um número IP (*Internet Protocol*) - que é o endereço que realmente os computadores se utilizam para a troca de "pacotes" de informação entre eles. Portanto, a comunicação entre computadores ainda continua a se utilizar de números. Todo *website* tem um número de identificação único (número IP), através do qual o sistema o reconhece e direciona para ele a informação. Mas os internautas procuram endereços na *web* inserindo "nomes de domínio" na barra de seus programas navegadores. O servidor DNS faz a correspondência entre o nome de domínio e o respectivo IP, repassando a informação para o computador do internauta.

¹⁵ *Uniform Resource Locator*, sigla que designa o endereço de um *site* na *Web*.

Definimos esse tipo de ataque específico (*DNS poisoning*) apenas para diferenciá-lo do *pharming* típico, que é direcionado contra o computador pessoal da vítima, usuário de provedor de Internet e de sistema de *on line banking*. A responsabilidade pelas conseqüências e danos materiais (ao usuário) resultantes de uma investida inicial ao sistema informático do provedor de Internet, é do próprio provedor, porque aí fica caracterizada uma falha de segurança na prestação do serviço, indicadora da *culpa* como fundamento da responsabilização¹⁶. Como são fenômenos parecidos, cuja diferenciação envolve um certo grau de conhecimento técnico, entendemos conveniente a apresentação antecipada dessas definições, de forma a propiciar ao leitor melhores condições para compreender as diversas situações de investidas fraudulentas contra sistemas informáticos e, dessa maneira, poder acompanhar o raciocínio lógico-jurídico em torno da teorização da responsabilidade pela reparação dos danos¹⁷.

3- Inviabilidade de se responsabilizar o provedor de acesso à Internet ou de hospedagem

De logo, queremos afastar a responsabilidade do provedor de serviços de hospedagem ou de acesso à Internet, pelos prejuízos decorrentes de *phishing* e outras fraudes do gênero. Como os perpetradores diretos das fraudes (*phishers*) não são facilmente identificáveis, pela razão de que utilizam técnicas de “anonimização” e como regra estão situados em território não submetidos à jurisdição do país da vítima¹⁸, discute-se a possibilidade da responsabilização de outros intermediários da cadeia informática, a exemplo dos provedores de hospedagem de conteúdo na Internet (*sites* e páginas eletrônicas). Embora não sendo o executante primário e direto da fraude, poderia o provedor que hospeda o

¹⁶ Sobre os fundamentos jurídicos da responsabilidade do provedor de Internet por danos resultantes ao seu usuário de ataques de *DNS poisoning*, sugerimos a leitura de nosso artigo “A INFECÇÃO DO SISTEMA DNS: a nova modalidade de *phishing* e a responsabilidade do provedor”, publicado no site *Jus Navigandi* - <http://jus2.uol.com.br/doutrina/texto.asp?id=6978> .

¹⁷ Em notícia recente (do dia 9.8.08) publicada no site da BBC, foi divulgada a existência de falha no programa navegador que permitiria um ataque de *pharming*, já que haveria a possibilidade de, explorando essa falha, os criminosos redirecionarem os internautas para sites falsos, mesmo tecendo endereços corretos. A notícia dá conta de que a Microsoft e outras grandes empresas que desenvolvem softwares estão distribuindo *patches* para conserto do defeito de segurança nos *browsers* de seus usuários. Na mesma notícia, ainda é feita referência de que não se tem comprovação de que a falha tenha sido utilizada. É certo, no entanto, que, em tendo sido efetivamente explorada para a efetivação de algum ataque, o fabricante do programa poderia ser responsabilizado. A vulnerabilidade que permitiu a concretização do golpe, nesse caso, não seria da responsabilidade do provedor de Internet.

A notícia, sob o título “Fix found for net security flaw”, pode ser acessada em:

[http://news.bbc.co.uk:80/2/hi/technology/7496735.stm](http://news.bbc.co.uk/80/2/hi/technology/7496735.stm)

¹⁸ Naftali Bennett, especialista em segurança computacional, afirma que 70% dos *phishers* produzem ataques em vítimas de países distintos . Ele acrescenta: “É quase impossível rastrear e processar os fraudadores... *Phishers* estão se tornando mais sofisticados e mascarando suas identidades e localização. Eles estão se utilizando de PC’s “zumbis” e se escondendo de forma eficiente” (Citado por Gene S. Koprowski, *Tough State Laws Won’t Stop “Phishing” Scams, Experts Say*, TECHNEWSWORLD, Oct. 29, 2005, disponível em: <http://www.technewsworld.com/story/46889.html> .

site falso (*spoofed webpage*)¹⁹ ser responsabilizado pelos danos financeiros sofridos pela vítima (cliente do banco) do *phishing*?

A resposta é negativa (embora não totalmente incontroversa²⁰). É certo que a página eletrônica utilizada na fraude (*spoofed webpage*) é hospedada com o concurso do sistema informático do provedor. Se não pratica ou executa o ilícito, nem por isso deixa de fornecer os meios materiais e físicos (tecnológicos) para a hospedagem. Embora não seja o responsável pela fraude, é no seu sistema que o conteúdo do *fake site* 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 *site* que serve de instrumento para a fraude, contudo, não é suficiente, por si só, para acarretar sua responsabilização. O princípio geral que se tem consagrado em torno da atividade dos provedores de 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 indiquem ilicitudes". Simplesmente atua provendo a infra-estrutura técnica para acesso à rede de comunicação, serviço que não acarreta uma co-obrigação 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.

Esse princípio da irresponsabilidade do provedor sustenta-se 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 o seu conteúdo. A grande 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 sobre o manancial informativo.

¹⁹ O golpe de *phishing* típico envolve dois passos iniciais. No primeiro, o *phisher* obtém espaço para hospedar uma *webpage* junto a um provedor de serviços na Internet e, uma vez contratado isso, instala o falso *website*, parecido com o de um banco ou de comércio eletrônico. Somente depois, é que o *phisher* envia para a vítima o e-mail enganoso ou contendo vírus que se apodera de seu computador e direciona o programa de navegação na Internet (*browser*) para a URL onde já se encontra o *spoofed website*.

²⁰ Alguns autores estrangeiros sustentam a possibilidade de se responsabilizar civilmente o provedor, de forma solidária, pelas lesões financeiras decorrentes do *phishing*. É o caso, por exemplo, de Camille Calman, que sugere uma responsabilidade secundária do provedor, com fundamento na Lei Anti-Phishing da Califórnia (em *Bigger Phish to Fry: California's Antiphishing Statute and its potential imposition of secondary liability on Internet Service Providers*, publicado na *Richmond Journal of Law & Technology* Volume XIII, Issue 1; disponível em <http://law.richmond.edu/jolt/v13i1/article2.pdf>)

Em relação à divulgação de conteúdo difamatório ou ofensivo em páginas na Internet, ainda existe um grau de responsabilização do provedor. De fato, considera-se que o provedor de hospedagem é responsável pelo conteúdo ilegal de *websites* hospedados em seu sistema, quando tem prévio conhecimento da ilicitude do material informacional e não toma qualquer providência no sentido de fazer cessá-la (retirando a página ou *site* que contenha esse material). Mas em relação às fraudes e ataques de *phishing*, na prática nem esse resíduo de responsabilidade (da omissão por inércia na retirada do site), pode ser atribuído ao provedor. É que em regra os *phishers* não deixam as *spoofed webpages* hospedadas por longo tempo; é somente o suficiente para aplicar o golpe em algumas vítimas, o que pode ser questão de dias ou de horas²¹. Assim, o provedor, em se tratando desse tipo de golpe, na prática nem sequer pode ser acusado de inércia na remoção do conteúdo ilícito (site), pois são os próprios criminosos quem toma a iniciativa de remover o material, logo após a execução das tentativas do golpe.

Como se vê, em relação ao *phishing* e outros tipos de fraudes, o provedor de Internet não tem o mesmo grau de controle sobre a ação dos causadores diretos do dano. O contexto em que se posiciona o provedor é largamente distinto do que ocorre em relação aos crimes cometidos simplesmente pela distribuição de conteúdo ilícito (assim genericamente considerados os casos de difamação). Nos casos mais comuns de difamação, que ocorrem através da transmissão de informações prejudiciais à imagem ou nome de um indivíduo qualquer, o provedor tem as condições técnicas para, por exemplo, remover a página eletrônica onde foram publicadas as notícias ilícitas. Daí a efetividade e plausibilidade de se construir teoria de responsabilização para eles, caso se mostrem negligentes na remoção desse material, quando tenham conhecimento de forma apropriada do ilícito e são solicitados a produzir a remoção. Se a página eletrônica está hospedada no seu sistema informático, e o provedor permanece inerte, mesmo após solicitado a retirá-la, assume comportamento capaz de ensejar sua condenação à reparação dos danos produzidos à vítima. Nessa hipótese, o provedor, que tem as condições técnicas de prevenir o ato criminoso ou ao menos fazer cessar seus efeitos, mas se mantém em inércia, pode ser responsabilizado solidariamente. Quanto aos ataques de *phishing* e outras fraudes do gênero os provedores de Internet não têm o mesmo poder de controle sobre a conduta dos internautas ou capacidade para fazer cessar os efeitos do ato ilícito. Em se tratando de ataques que exploram falhas de segurança, categoria em que podem ser incluídos os golpes de *phishing*, o grau de influência que o provedor tem sobre a ação do internauta (agente criminoso) ou aptidão para eliminar os efeitos dos seus atos é imensamente menor. Em regra, os praticantes dessa categoria de atos ilícitos são muito mais sofisticados, em termos de técnicas empregadas. Qualquer pessoa pode difamar outra na Internet, bastando que tenha conta em provedor, através do qual possa hospedar uma página eletrônica ou enviar mensagem de e-mail. Já os golpes de *phishing* envolvem um maior refinamento

²¹ Segundo Jeordan Legon, que afirma que os *phishers* além de mascarar suas identidades, abrem e fecham suas operações rapidamente (em “*Phishing*” *Scams Reel in Your Identity*, CNN.COM, Jan. 26, 2004, disponível em: <http://www.cnn.com/2003/TECH/internet/07/21/phishing.scam/index.html>)

técnico e, por isso, são praticados por agentes com maiores conhecimentos de informática, os quais se valem de meios para encobrir sua identidade e evitar a repressão sobre suas ações. Além disso, a própria natureza do ato de difamação pressupõe a continuidade do ato ilícito, através da permanência da divulgação da ofensa (conteúdo) na página eletrônica. Daí o domínio que o provedor exerce sobre o autor da difamação, podendo refrear sua conduta e conter os efeitos de sua ação através simplesmente da retirada do material ou conteúdo informacional ofensivo (retirada do *site* ou página da Internet). O provedor não tem, todavia, essa mesma aptidão ou poder para conter as investidas de *phishing*, uma vez que os *sites* falseados (quando utilizados como instrumento ou meio para execução do golpe) ficam hospedados apenas pelo intervalo de tempo suficiente (em regra muito curto) para o logro da vítima (coleta de suas informações pessoais). Nesse contexto, o provedor não exerce o mesmo papel ou poder de controle sobre a atividade do agente criminoso; situa-se em posição diferente da que assume em relação aos ilícitos realizados mediante simples disseminação de conteúdo, quando tem condições de reprimir a ação criminosa ou eliminar seus efeitos.

Essa observação da diferença de contexto quanto à prevenção de certos ilícitos e condutas é feita por Ronald J. Mann e Seth Belzley. Esses autores agrupam os casos de pornografia, difamação e pirataria sob a rubrica genérica de ilícitos realizados mediante a disseminação de conteúdo (*dissemination of content*), enquanto que os tipos e condutas ilícitas que são perpetrados mediante vírus, *spam*, *phishing* e *hacking* são classificados e incluídos na categoria de falhas de segurança (*breaches of security*). Em relação a essa última categoria de ilícitos, os provedores de Internet não têm o mesmo poder de controle sobre a conduta dos internautas. Considera-se que eles não têm como controlar e prevenir esses tipos de fraudes, pois lhes faltam condições técnicas para tanto:

“The context of security harms differs in two obvious respects from that paradigm. First, it is not all clear that any intermediary readily can control the conduct in question. Perhaps the actors who are best able to increase internet security are the software manufacturers that develop the applications that make the internet useful. (...) And it seems unlikely that ISPs serving those that introduce viruses and spam into the internet community can control the misconduct, if only because of the difficulty of identifying the transmissions that cause the problem and filtering out the malicious code²².”

É tecnologicamente difícil para os provedores de Internet filtrar o tráfego de informações para prevenir as fraudes e ataques que exploram falhas de segurança (vírus, *spam*, *phishing* e *hacking*) nos computadores dos internautas. Embora seja certo que certas modalidades de *phishing scams* requeiram o uso de um provedor para hospedar o *spoofed site*, este tem pouca duração e o provedor não tem controle sobre ele. Em sendo diferente o contexto e o modo como são praticados os ataques que exploram falhas de segurança e a posição em que se

²² “The Promise of Internet Intermediary Liability”, William & Mary L. Review, 47 (2005): 239, disponível em http://works.bepress.com/ronald_mann/24.

coloca o provedor diante desses tipos de ilícitos, o esquema de atribuição de responsabilidades não pode ser o mesmo aplicado aos ilícitos praticados mediante simples disseminação de conteúdo (ofensas contra a honra e nome das pessoas). Diferentes tipos de esquemas de responsabilização devem ser aplicados a diferentes e específicos tipos de conduta. Se o contexto dos ataques de *phishing* é diferente daquele encontrado nos ilícitos praticados por disseminação de conteúdo ofensivo, o esquema de atribuição de responsabilidades também deve ser diferente.

A aplicação da teoria da responsabilização dos intermediários somente pode ser viável para alguns tipos específicos de conduta, parecendo-nos não ser aceitável tomá-la de empréstimo para responsabilizar o provedor por fraudes (*phishing* e outras do gênero) e ataques que exploram falhas de segurança²³, cometidas por terceiros não identificáveis.

Obviamente que, na hipótese de a *spoofed webpage* não ser retirada imediatamente pelo próprio *phisher*, e o provedor toma conhecimento de que sua estrutura de hospedagem está sendo utilizada como meio para a prática do golpe, sua inércia diante do fato, sem tomar medidas para “derrubar” a página eletrônica falsa, constitui circunstância que pode levá-lo a ser responsabilizado secundariamente pelos resultados. Se, comunicado (pelo ofendido ou terceiro qualquer) da existência da página ou do envio recorrente de e-mail com mensagens fraudulentas, e tendo meios para retirá-la de circulação ou bloquear a expedição de novos e-mails da mesma fonte, o provedor assim não procede, revela que endossa a atividade ilícita ou que se mostra de certa forma conivente, assumindo o risco de ser responsabilizado²⁴.

Mas essa circunstância exemplificada, de a *spoofed webpage* permanecer hospedada e ser facilmente localizada e identificada como tal, não costuma ocorrer na maioria dos ataques de *phishing*, onde as ações se desenvolvem de maneira muito mais veloz, sem dar tempo de o provedor esboçar qualquer reação

²³ Sempre, é óbvio, quando a falha de segurança não se relacione com o próprio sistema do provedor. O alvo dos ataques de *phishing*, spam e disseminação de vírus em regra são os computadores dos usuários dos serviços de comunicação na Internet.

²⁴ Seria uma responsabilidade por ato de terceiro. Em que pese a ausência de previsão da responsabilidade dos provedores por atos de seus usuários no art. 932 do C.C., a responsabilidade dos intermediários seria mantida apoiada nos fundamentos da responsabilidade por ato alheio, sobre a base de uma culpa individual. A inexistência de norma específica em relação aos provedores e operadores de sistema informáticos poderia ser explicada na circunstância de que as relações cibernéticas são um fenômeno da modernidade, não prevista pelo legislador civilista, daí porque, em nome da evolução do Direito, seria fácil sustentar a extensão da responsabilidade secundária, de forma a incluir também aqueles (provedores) como responsáveis solidários. Uma tal conclusão não seria destituída de razoabilidade jurídica, pois o Direito não pode tolerar que ofensas fiquem sem reparação. Se “o interesse em restabelecer o equilíbrio violado pelo dano é a fonte geradora da responsabilidade civil”, nada impede que se visualize a responsabilidade dos intermediários da comunicação eletrônica, para atender a uma necessidade moral, social e jurídica de garantir a segurança da vítima violada pelo ato lesivo. Nesse sentido, os fundamentos da responsabilidade por ato alheio, calcada na falta de um dever de vigilância, podem ser invocados de modo a justificar a obrigação indenizatória de um controlador de sistema negligente.

eficaz em termos de evitar a concreção de prejuízos para as vítimas da fraude. O seu domínio em relação às fraudes de *phishing* é simplesmente inexistente, sem qualquer influência na repercussão do ilícito. Sendo limitado o seu controle, não parece correto atribuir-lhe responsabilidade.

4- Inviabilidade de se responsabilizar os provedores de serviços de e-mail

Muito dificilmente se pode invocar a responsabilidade do provedor de serviços de *e-mail*²⁵ pelos prejuízos sofridos por um usuário vítima desse tipo de golpe. Não só aqui como em outros países, a tendência tem sido a de isentar o provedor pelo conteúdo das informações que trafegam em seus sistemas, sobretudo quando postadas por terceiros com os quais não mantém vínculo contratual. Em relação aos serviços de *e-mail*, não se pode exigir que o provedor tenha uma obrigação de triagem das mensagens. Ainda que no caso de simples *spams*, o provedor não pode ser obrigado a indenizar por perdas e danos, mesmo quando as mensagens indesejadas conduzam vírus (em arquivos anexados), a menos que o contrato com o usuário contenha cláusula expressa nesse sentido, com a promessa de uso de sistemas especiais e infalíveis de filtragem (*firewalls* e outros sistemas de bloqueio)²⁶. Algumas mensagens de *phishing* sequer vêm acompanhadas de arquivos infectados (programas maliciosos ou vírus), daí que a idéia de imputação ao provedor de responsabilidade por falha de segurança fica ainda mais insustentável. Sem conter anexos, fica difícil para o provedor detectar a natureza delas (se fraudulentas ou não).

A única medida que parece razoável exigir por parte dos provedores (de serviços de e-mail), em matéria de *phishing* (e de um modo geral em relação a qualquer prática fraudulenta via *spam*), é que prestem informações aos seus usuários sobre essa prática, deixando bem claro até onde se responsabilizam e como configurar seu servidor de e-mail, indicando as medidas e a tecnologia de que se vale para (se não evitá-las) minimizar suas conseqüências. A informação do usuário sobre as características fundamentais do funcionamento do serviço é de suma importância. Ele deve ser esclarecido sobre os aspectos técnicos dos serviços, tais como suas limitações e riscos a que pode ficar sujeito, a fim de que possa formar sua convicção e melhor exercer sua opção quanto à escolha da prestadora. Deve também o usuário ser devidamente orientado sobre cuidados

²⁵ Que pode ser o seu próprio provedor de acesso à Internet, cujo servidor armazena em espaço em disco uma "caixa postal", onde ficam transitariamente as mensagens até serem baixadas para o computador do usuário, que tem seu próprio programa gerenciador de e-mails (o *Outlook Express*, por exemplo), ou um provedor de serviços de *webmail*, onde as mensagens são armazenadas exclusivamente em seu servidor – o destinatário lê as mensagens na tela do programa que usa para navegar na *Web*. O *Yahoo!*, o *Hotmail* e o *GMail* são exemplos de provedores desses serviços de *webmail*. O internauta se conecta à rede Internet através de seu provedor de acesso e adentra nesses *sites* de serviços *webmail* pelo seu programa de navegação (*browser*). As mensagens que os usuários recebem ficam armazenadas de forma definitiva nos servidores desses prestadores de serviços.

²⁶ Nesse sentido é a posição defendida pelo Min. Castro Filho, do STJ, no artigo "Da Responsabilidade do Provedor de Internet nas relações de consumo", apoiando-se na opinião de Erica Barbagalo (Aspectos da Responsabilidade civil dos provedores de serviços de Internet, in LEMOS, Ronaldo (Org.). Conflitos sobre nomes de domínio: e outras questões jurídicas da Internet. São Paulo: Revista dos Tribunais, 2003, p. 345.

imprescindíveis, visando à sua própria conduta, como as cautelas que deve ter com a utilização do serviço de e-mail.

O *Gmail*²⁷, serviço de *webmail* do *Google*²⁸, divulgou recentemente que está testando uma ferramenta desenhada para alertar seus usuários contra mensagens que aparentem ser ataques de *phishing*. Quando o usuário abre uma mensagem suspeita, a tela exibe um alerta. Trata-se de uma ferramenta que funciona com a mesma lógica dos instrumentos técnicos que operam contra o *spam*. Quando o time de técnicos do *Gmail* toma conhecimento de um determinado ataque de *phishing*, configura o sistema para que automaticamente identifique futuras mensagens semelhantes. Um tipo de filtro similar ao que automaticamente desvia as mensagens de *spam* para uma pasta específica – a mensagem não entra na "caixa de entrada" (ou "inbox"), faz com que o sistema mostre um aviso, alertando para a possibilidade de ataque *phishing*, de modo a que o usuário tome cuidados antes de clicar em um *link* e fornecer informações pessoais.

As políticas de combate à atuação de fraudadores, no sentido de criar barreiras ou algum tipo de proteção contra o *phishing*, não diferem muito das políticas que já são empregadas em relação ao *spam* em geral. E não poderia ser diferente, já que, como se disse, o *phishing* é uma modalidade mais letal de *spam*. As tecnologias disponíveis permitem um grau limitado de impedimento de chegada das mensagens fraudulentas à caixa postal dos usuários. Em geral, os prestadores de *webmail* divulgam um compromisso de combater o *spam*, através da utilização de filtros e outras ferramentas que se utilizam de inteligência artificial para apagar ou bloquear automaticamente mensagens não solicitadas²⁹. Outra técnica também bastante difundida é a de possibilitar que os próprios usuários bloqueiem certos endereços de e-mail. Ao receber múltiplas mensagens da mesma fonte, e desejando bloquear o endereço de envio, o usuário pode ativar um bloqueador para não receber e-mails daquele endereço ou domínio³⁰. Mas são sempre recursos limitados, que não garantem uma eficácia absoluta. A mesma dificuldade de natureza técnica se observa em relação ao *phishing*. As informações no *site* do *Gmail* deixam bem claro que o sistema anti-*phishing* não é infalível, tanto que possibilita ao usuário validar uma mensagem indicada como tal ou relatar uma tentativa de ataque não detectada.

Realmente, tendo em vista a natureza do serviço de *e-mail* e o atual estado da técnica referente às comunicações e transmissões eletrônicas de dados via Internet, não é razoável exigir que os provedores sejam responsabilizados pelos danos que mensagens de *phishing* (ou qualquer modalidade de *spam*) possam acarretar aos computadores dos usuários. O que é aceitável se esperar, em termos de conduta do provedor nessa matéria, é que empregue seus melhores

²⁷ <http://gmail.google.com/>

²⁸ O *Google* é uma das mais populares ferramentas de busca na Internet.

²⁹ O *Yahoo! Mail* utiliza a tecnologia patenteada como *SpamGuard*, que direciona automaticamente todas as mensagens de *spam* para uma pasta de "e-mails em massa".

³⁰ Enquanto o endereço de envio for o mesmo (assim como o domínio), o bloqueador baseado na informação do campo "De" (ou "From") é bastante efetivo.

esforços para assegurar que os serviços de *e-mail* funcionem da melhor forma e com o melhor padrão de segurança possível³¹. Colocar a responsabilidade do controle das mensagens indesejadas e fraudulentas nos ombros do provedor pode, por outro lado, provocar conseqüências socialmente prejudiciais. Tal solução levaria os provedores a regular de forma mais rígida o controle dos filtros, aumentando as probabilidades de bloqueio de uma quantidade maior de mensagens lícitas³², com o risco de liquidar ou prejudicar o valor real do e-mail como ferramenta de comunicação, comprometendo o desenvolvimento da Internet. Portanto, a política mais acertada é a da responsabilização penal e civil do *phisher* (ou *spammer*), e não do provedor³³.

5- Insuficiência das leis que criminalizam a conduta do ofensor direto (*phisher*)

Leis que estabelecem sanções criminais contra os praticantes do *phishing* estão sendo editadas em vários países, como forma de combater esse tipo de fraude. A Pensilvânia e a Flórida, bem como vários outros Estados dos EUA, estão tratando como crime o ato de enviar e-mail fraudulento ou a criação de um *website* falso. No nível federal, o Senador Patrick Leahy apresentou um projeto de lei, denominado *Anti-Phishig Act of 2005*, que pretende criminalizar as fraudes de Internet que envolvam a obtenção de informações pessoais, prevendo cinco anos de pena prisional e multa para indivíduos que cometam “furto de identidade” (*identity-theft*) falsificando *websites* ou *e-mails*³⁴.

Em nosso país, existe também iniciativa legislativa para criminalizar o *phishing*. No projeto sobre Crimes Tecnológicos em tramitação no Congresso Nacional (PLC 89-2003 no Senado, PL 84/99 na Câmara), foi incluído um tipo chamado de “falsidade informática”, por meio do acréscimo do art. 154-C ao Código Penal. Já em substitutivo que foi apresentado, posteriormente, no âmbito da Comissão de Educação do Senado, a mesma conduta recebe o nome de

³¹ O Projeto de Lei n. 6.210/2002 apresentado na Câmara dos Deputados em 05.03.02, de autoria do Dep. Ivan Paixão (PPS-SE), trazia a seguinte disposição:

"§ 3º Não será responsabilizado pelo recebimento indevido de mensagem eletrônica não solicitada o provedor de acesso ou de serviço de correio eletrônico que tenha se utilizado, de boa fé, de todos os meios a seu alcance para bloquear a transmissão ou recepção da mensagem."

O projeto, no entanto, foi arquivado em 31 de janeiro de 2003. Ver informações a respeito no site da Câmara dos Deputados.

³² As soluções técnicas, os filtros de *spam*, são soluções paliativas. Os programas de filtragem são constituídos de uma série de regras que visam a determinar a semelhança de uma mensagem analisada com um *spam*. Os programas são regulados para bloquear mensagens segundo alguns critérios pré-definidos, levando em conta, p. ex., se a mensagem é proveniente de alguns servidores listados como sendo de *spammers*, ou se é enviada para um número alto de destinatários, ou se contém certa palavra, entre outros padrões. Esses programas, contudo, são sempre limitados, e geralmente terminam filtrando mais mensagens do que o desejado.

³³ É nessa linha que se situam as leis alienígenas que regulam a atividade de envio de mensagens eletrônicas não solicitadas, a exemplo do *CAN-Spam Act*, a lei americana editada com a finalidade de combater o *spam*.

³⁴ Veja comunicado oficial, sobre a apresentação do projeto de lei no Senado Norte-Americano em: <http://leahy.senate.gov/press/200503/030105.html>. O texto completo da lei pode ser obtido em: <http://www.govtrack.us/congress/billtext.xpd?bill=h109-1099>.

"fraude eletrônica". Embora com redações diferentes, ambas as propostas pretendem tipificar as condutas de fraudes na Internet, tais como "phishing" ou "scam".

Alguém poderia discordar da necessidade desse tipo de ação legislativa, de positivar o crime de *phishing* ou *pharming*, já que, como categoria de fraude, poderia ser sancionado através da invocação do art. 171 do CPC, que prevê a figura do estelionato. O *phishing*, é certo, amolda-se perfeitamente ao descritor normativo desse dispositivo, já que o ato do criminoso corresponde a “obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo alguém em erro, mediante artifício, ardil ou qualquer outro meio fraudulento”. Todos os elementos componentes da descrição do crime de estelionato, portanto, estão presentes na ação delituosa do *phisher*. Com efeito, nesse tipo específico de delito, o agente obtém, para ele ou outrem, vantagem ilícita (numerário subtraído de conta bancária), em prejuízo de alguém (a vítima, cliente de banco) mediante o emprego do artifício da construção de uma página eletrônica falsa ou envio de mensagem eletrônica (e-mail) de conteúdo fraudulento. Não haveria, como se disse, qualquer dificuldade de enquadramento do praticante do *phishing* no art. 171 do CPC, impondo-lhe as sanções previstas nesse dispositivo (reclusão, de um a cinco anos, e multa). Além do mais, quando o criminoso implementa o último estágio da execução *phishing*, que é a subtração não autorizada dos fundos existentes na conta da vítima, a jurisprudência tem entendido que aí está caracterizado o crime de furto qualificado, previsto no art. 155, § 4º., II³⁵.

Esse tipo de legislação criminal especificamente editada para descrever e, por conseguinte, reprimir os crimes de *phishing* e *pharming* tem a vantagem de facilitar o enquadramento criminal em determinadas situações, como por exemplo nas condutas que possam representar mera tentativa. Nos termos do *Anti-Phishig Act of 2005*, por exemplo, o simples envio do e-mail fraudulento ou a estruturação do falso *website* já são consideradas ações criminosas, mesmo que nenhum usuário ou cliente venha a ser fraudado como decorrência desses atos iniciais. Ou seja: mesmo que as informações pessoais do indivíduo alvo da fraude não sejam coletadas ou não lhe sobrevenha qualquer outro tipo de dano, ainda assim os agentes serão responsabilizados criminalmente. Diante apenas das normas existentes no vigente Código Penal, talvez se tornasse mais difícil inserir essas condutas dentro da moldura de crime tentado (art. 14, II, CP) de estelionato ou furto. Daí a validade, nesse aspecto, da legislação que trata especificamente do crime de *phishing*. A previsão de ilicitude específica para a conduta do *phisher* supre eventuais brechas da legislação penal e evita insegurança jurídica.

³⁵ “Configura crime de furto qualificado a subtração de valores de conta corrente, mediante transferência bancária fraudulenta, sem o consentimento do correntista” (STJ - 3ª Seção - CC 87.057-RS - Relª Minª Maria Thereza de Assis Moura - j. 13.02.2008 - DJ 22.02.2008). Nesse caso julgado, o criminoso promoveu a transferência de valores por intermédio do Internet Banking da CEF. A relatora em seu voto esclareceu que: “A fraude, de fato, foi usada para burlar o sistema de proteção e vigilância do banco sobre os valores mantidos sob sua guarda, configurando, assim, crime de furto qualificado por fraude, e não estelionato”.

Todavia, permanecem dúvidas quanto à eficácia de uma legislação criminal que somente pune o agente direto, praticante do *phishing*³⁶. Todas as leis penais mencionadas e outras que ainda estão em gestação tomando por base o modelo das precedentes, não criam qualquer tipo de previsão quanto à responsabilização solidária de outros partícipes da corrente informática. Como os *phishers* atuam sob técnicas que favorecem o anonimato na rede e em regra desferem ataques contra pessoas situadas em outros países, quase sempre não conseguem ser identificados³⁷ e, mesmo quando tal acontece, não estão submetidos à jurisdição da localidade da vítima. Portanto, na prática o que vai se verificar é que, devido às próprias características técnicas da Internet, que permitem um alto grau de ocultação de identidade e comunicação em escala global, leis que se limitam a uma previsão sancionadora exclusivamente para o arquiteto da fraude eletrônica, não oferecem resposta social satisfatória e efetiva, sobretudo quando se tem em mira a pessoa da vítima.

Esse cenário revela a necessidade do desenvolvimento de teoria de responsabilização na órbita civil, para impedir que as vítimas da fraude, que têm seu patrimônio dilapidado, não fiquem sem qualquer tipo de reparação. É preciso identificar outros meios de se oferecer resposta eficaz para a pessoa que sofre o dano, pois o Direito não pode tolerar que ofensas fiquem sem reparação. Se “o interesse em restabelecer o equilíbrio violado pelo dano é a fonte geradora da responsabilidade civil”³⁸, nada impede que se visualize a responsabilidade de outro intermediário da comunicação eletrônica, para atender a uma necessidade moral, social e jurídica de garantir a restauração do patrimônio da vítima violado pelo ato lesivo.

É com esse sentir que voltamos nossa atenção para os bancos, prestadores do serviço de *Internetbanking*, cujos fundamentos da responsabilidade civil (por ato lesivo causado pelos fraudadores aos seus usuários) examinaremos no tópico seguinte.

6. Teoria da responsabilidade dos bancos prestadores de serviços de *Internetbanking*

³⁶ Ver, a propósito, Jim Harper, Diretor de Estudos de Política de Informação do *Cato Institute*, que afirma: “Politicians who claim to protect consumers in this environment either don't know that they are lying, or are deeply cynical” (citado por Gene S. Koprowski, em *Tough State Laws Won't Stop “Phishing” Scams, Experts Say*, publicado em TECHNEWSWORLD, Oct. 29, 2005, acessível em: <http://www.technewsworld.com/story/46889.html>)

³⁷ Naftali Bennett, especialista em segurança computacional, afirma que 70% dos *phishers* produzem ataques em vítimas de países diferentes. Ele acrescenta: “É quase impossível rastrear e processar os fraudadores... *Phishers* estão se tornando mais sofisticados e mascarando suas identidades e localização. Eles estão se utilizando de PC's “zumbis” e se escondendo de forma eficiente” (Citado por Gene S. Koprowski, *Tough State Laws Won't Stop “Phishing” Scams, Experts Say*, TECHNEWSWORLD, Oct. 29, 2005, disponível em: <http://www.technewsworld.com/story/46889.html>)

³⁸ Nas palavras de Maria Helena Diniz, Curso de Direito Civil Brasileiro, Editora Saraiva, 11ª ed., 7º. vol., p. 5.

A responsabilização tem por finalidade impor ao infrator a contrapartida legal pelos prejuízos e custos sociais decorrentes de sua conduta. Aquele que pratica ato que cause prejuízo a outrem, quer seja por dolo ou culpa, está obrigado a reparar o prejuízo. Esse é um princípio geral da responsabilidade: o homem apenas é responsável pelos prejuízos causados diretamente por ele e por seu fato pessoal.

Nem sempre, no entanto, é possível a imposição eficaz de penalidades ao autor direto de um gesto ou conduta, quer porque razões de ordem prática impedem seja alcançado, quer porque pode não dispor de solvabilidade. Essas circunstâncias servem como justificadoras para imposição de responsabilidade a outra pessoa, que não é o autor direto do gesto ou ato danoso, mas que mantém com este ou com a vítima algum tipo de relação, que, de certa forma, o liga ao resultado nocivo. A ineficácia ou falta de efetividade na atribuição de responsabilidade ao praticante direto do ato é que justifica voltar-se contra terceiro, que guarda alguma relação com aquele ou que está de alguma forma posicionado de modo a interferir em sua conduta (do ofensor primário). Essa situação é particularmente ilustrada no âmbito da Internet, onde o elevado grau de anonimato, permitido pela arquitetura da rede, impede ou ao menos dificulta a detecção do infrator primário, ou, quando isso é possível (ou seja, quando o transgressor é identificado), pode ocorrer de ser ele uma criança ou pessoa não responsável civil ou criminalmente por seus atos, ou pode se tratar de um indivíduo que não disponha de meios patrimoniais suficientes para reparar os prejuízos causados, ou ainda pode ser residente em território não submetido à jurisdição do país da vítima. Como resultado dessas possibilidades, tem-se como justificável a imposição de responsabilidade a terceiros, outros participantes da comunicação informática, por atos praticados pelos infratores primários. A limitação da responsabilidade aos infratores primários poderia comprometer o nível da segurança jurídica das relações que se estabelecem em meios eletrônicos. A dificuldade de imposição de responsabilidade aos agentes funciona como causa justificadora de sanção aos intermediários. Por atos cometidos por outrem, estes podem responder.

E quais, dentre os diversos intervenientes e fornecedores da cadeia eletrônica de comunicação podem e devem ser chamados à responsabilização por atos cometidos pelos *phishers*, quando estes não puderem ser identificados ou de qualquer maneira não puderem ser responsabilizados diretamente?

Já vimos nos itens anteriores,³⁹ que é inviável tentar responsabilizar o provedor de acesso à Internet ou de hospedagem e também o provedor de serviços de e-mail, uma vez que não têm poder de controle sobre a conduta dos criminosos ou capacidade para fazer cessar os efeitos do ato ilícito. Dentre os demais partícipes da cadeia de comunicação telemática, é o banco (prestador dos serviços de *Internetbanking*) quem está mais visivelmente posicionado de forma a interferir e impedir os efeitos da ação do *phisher*. Por ser a parte que controla

³⁹ Ver itens 3 e 4, onde apontamos a inviabilidade de se pretender a responsabilização dos provedores de serviços na Internet.

tecnicamente o acesso ao serviço de *Internetbanking*, pode prevenir os ataques de forma mais eficaz do que qualquer outro agente intermediário da cadeia eletrônica de comunicação. É justamente por isso, por ser o agente intermediário que tem o maior controle tecnológico para evitar a consecução da fraude, que pode ser chamado à responsabilização, para reparar os efeitos patrimoniais do ilícito. Além disso, nenhum outro intermediário da cadeia de comunicação informática está tão ligado à vítima de *phishing* do que o seu próprio banco, com quem mantém uma relação contratual para prestação de serviços de *Internetbanking*.

Os bancos redarguem 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. Sob essa ótica, o ataque não é cometido contra o sistema informático do banco, que permanece invulnerável em termos de segurança, não sendo razoável impor à instituição bancária a reparação dos danos patrimoniais resultantes da fraude. 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 sistema⁴⁰.

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 os bancos desempenham no mercado de serviços *on line*. Por mais bem informado que possa ser o internauta, em termos de noções básicas de navegação segura e utilização de programas de proteção, não se tem como eliminar completamente a probabilidade de ser vítima da fraude. As técnicas de *phishing* estão se sofisticando a cada dia, criando sempre maiores dificuldades para a pessoa saber quando está diante de uma tentativa de golpe⁴¹. Portanto, o

⁴⁰ Para os bancos, é da alçada de responsabilidade do usuário a proteção do seu computador, devendo ter cuidados na utilização do correio eletrônico e do programa navegador. Indicam que o cliente deve dispor de antivírus atualizado e se manter atento ao *phishing*. Em seus *websites*, em geral informam que nunca enviam mensagens de correio eletrônico com *links* e que se o cliente receber mensagem desse tipo fica alertado que provavelmente se trata de uma fraude. Informam ainda os clientes para nunca clicar em *links* de mensagens provenientes de fontes não fidedignas e não abrir arquivos anexados, bem como manter os dados de acesso reservados, nunca divulgando-os a outra pessoa, mesmo sendo de confiança. Essas medidas, no entanto, não são suficientes para impedir a responsabilização dos bancos, como veremos adiante.

⁴¹ As mensagens de *phishing* primitivas eram mais facilmente detectáveis, pelo menos pelos usuários da Internet mais experientes. Muitas continham inclusive erros gramaticais e os endereços nos *links* eram exclusivamente numéricos, deixando revelar que a página eletrônica para a qual enviava não era a do site legítimo. Além disso, as mensagens eram enviadas de forma indiscriminada, alcançando usuários que não tinham relações com o banco ou *website* respectivo. Atualmente, as mensagens de *phishing* tendem a ser gramaticalmente corretas e quando contêm algum erro no título geralmente é posto de forma intencional, para

senso comum que as pessoas têm nos ambientes físicos, quando se protegem de ardis e esquemas fraudulentos, não é aplicável ao ambiente do ciberespaço. Uma coisa é a pessoa ser abordada em casa, no meio da rua ou mesmo no interior de uma agência bancária por um estelionatário, o qual, se passando por um funcionário do banco, solicita e obtém a senha e cartão do banco. Os clientes de banco ou usuário de caixa eletrônico sabem que não devem fornecer suas senhas a qualquer outra pessoa. Outra situação completamente diferente é a da navegação em ambiente eletrônico, onde a ausência de conhecimentos técnicos e a natural falta de aptidão para lidar com inovações tecnológicas, somadas às características dinâmicas da Internet, que permitem o aparecimento de variadas formas e a sofisticação das fraudes eletrônicas, colocam o usuário em situação de ainda maior fragilidade. Essa diferenciação de situações impede que se tome de empréstimo de forma absoluta os padrões de conduta dos ambientes físicos para construção de analogias com o ciberespaço, quando se trata de alocar os riscos financeiros da utilização de sistemas de pagamento e transações *on line*. Os riscos devem ser alocados às partes mais capazes de lidar com eles e que, no caso em questão, são justamente os bancos.

A visão de que o *phishing* é um ataque que se executa 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 *Internetbanking*. Os bancos poderiam fornecer computadores dotados de programas atualizados de proteção contra golpes cibernéticos, mas 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, através da rede mundial, fazer conexão com o *Internetbanking*, toda a rede nesse caso se considera como uma extensão do sistema⁴². 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. Essa é a analogia mais perfeita e que pode justificar a responsabilização do banco pela não adoção de dispositivos eficientes de proteção contra o *phishing*.

evitar filtros que detectam *spams*. Muitos *phishers* só enviam mensagens para clientes da instituição cuja marca ou *site* eles tentam fraudar, numa técnica conhecida como *spear-phishing*. Além disso, os fraudadores desenvolveram técnicas para mascarar a URL do site falso, fazendo com que o correspondente ao site legítimo apareça no local da barra de endereços do programa de navegação.

⁴² Pode-se usar a analogia de que a rede seria a estrada por meio da qual é feito o acesso à “casa” (site do banco). Essa analogia entre a rede de comunicação (para acesso ao sistema do banco) com uma estrada foi construída por Demi Getschko, Diretor-presidente do NIC.br. Diz ele, sobre a necessidade de se garantir a segurança do internauta contra fraudes de *phishing*: “A maioria dos bancos já têm sistemas muito seguros. Queremos resolver um problema de segurança das estradas, não das casas: garantir a segurança do usuário até que ele chegue ao site”, afirma Getschko (em entrevista à Folha Online, <http://www1.folha.uol.com.br/fofha/informatica/ult124u395485.shtml>)

Portanto, a educação dos usuários dos serviços de *Internetbanking*, 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 externalizar integralmente os custos e perdas financeiras deles decorrentes. Mesmo que os bancos disponham em seus *websites* informações sobre o *phishing* e sobre como evitá-lo, tal iniciativa não é, por si só, suficiente para excluir a responsabilidade pelos efeitos lesivos desse tipo de fraude aos usuários. O esforço de educação deve ser visto como uma iniciativa dos bancos imbuída da boa-fé, objetivando diminuir as fraudes. Prover dicas e informações ao usuário, sobre como se proteger de fraudes eletrônicas, auxilia certamente na defesa deles e da própria instituição bancária, uma vez que reduz os custos do crime. No entanto, por mais que se dê informação ao cliente, este sempre estará sujeito a riscos na operação dos serviços de *on line banking*, pois novas formas de golpes e ataques fraudulentos são desenvolvidos a cada dia⁴³. A educação do cliente, através de um contínuo processo de fornecimento de informações sobre como proteger seu micro de pragas eletrônicas é certamente um recurso que reduz o nível das fraudes, mas não as elimina por completo.

A responsabilização dos bancos na reparação dos efeitos financeiros resultantes do *phishing*, ainda pode ser justificada levando-se em consideração os seguintes argumentos adicionais:

a) argumento de ordem econômica.

Trata-se de argumento não propriamente jurídico, mas que nem por isso deixa de influenciar na definição da responsabilidade. Essa teoria é explorada por Assaf Hamdani, em relação à possibilidade da escolha de uma pessoa (intermediário) para responder pelos atos ilícitos praticados por um terceiro na rede, quando este não for passível de sanção de modo efetivo e que traga resultados práticos e úteis. Nesse caso, deve ser a parte para quem a atividade de fiscalização e monitoração represente custos mais baixos⁴⁴.

Ao analisar a responsabilidade dos bancos pelos prejuízos resultantes de *phishing* e outras fraudes semelhantes não se pode desconsiderar o argumento econômico de que são eles quem menos sofrem com a imposição dos custos da reparação. O fornecedor dos serviços bancários na Internet, pela sua supremacia econômica, é o que se chama na doutrina anglo-americana de o "least cost avoider", ou seja, a pessoa para quem a imposição do dever da reparação econômica representa o menor peso, considerando-se sua capacidade

⁴³ A solução de anti-vírus é reconhecidamente ineficiente na detecção de novas modalidades de programas maliciosos. Um estudo conduzido pelo AusCERT em 2006 revelou que, em média, 60% das formas de vírus que coletam informações pessoais não são detectadas por programas anti-vírus, assim que são utilizados em um primeiro ataque. Portanto, os computadores dos clientes com as versões mais atualizadas de software anti-vírus são vulneráveis a ataques com novas formas de *malwares*.

⁴⁴ "Liability should be expanded only to those parties whose cost of preventing misconduct is sufficiently low" (ob. cit.).

econômica. E aqui deve ser entendido que os bancos não somente podem “internalizar” mais facilmente os custos com a reparação dos prejuízos decorrentes de *phishing*, mas que são os únicos que dispõem de capacidade econômica para investir no desenvolvimento de soluções tecnológicas para combater esse tipo de fraude. Portanto, os bancos podem, em determinadas circunstâncias, suportar o ônus pelas conseqüências danosas do *phishing*, em substituição ao praticante direto da fraude, recorrendo-se à aplicação de princípios econômicos por meios dos quais se pode atribuir responsabilidade ao “least cost avoider”. A responsabilidade pela reparação dos prejuízos financeiros pode ser expandida para a parte cujos custos de prevenção pelas fraudes são mais baixos.

Chamamos a atenção para a circunstância de que esse argumento, de ordem mais econômica do que jurídica, é utilizado com mais freqüência para justificar a *responsabilidade objetiva* de alguns atores que desenvolvem certos tipos de atividade (em geral de natureza periculosa) na sociedade, embora possa também influir na visualização e definição de outros padrões de responsabilidade. De fato, a própria jurisprudência brasileira, na aplicação da *teoria contratualista* - fusão entre a teoria do risco profissional e da culpa - às instituições financeiras, sempre considerou que a responsabilidade deve recair sobre aquele que extrai maior lucro da atividade que deu margem ao dano, nas hipóteses em que não resulta configurada culpa do correntista ou do banco⁴⁵. Mesmo quando se trata de definir responsabilidade fundada na teoria pura da culpa, o argumento econômico pode ter extrema valia. A idéia é de que aqueles que se beneficiam com a venda de serviços e obtêm lucros excessivos nesse comércio devem ser responsabilizados ao menor sinal de negligência.

b) incentivo ao desenvolvimento de ferramentas tecnológicas.

A admissão da responsabilização dos bancos (obviamente, dentro de certas circunstâncias) também produz um incentivo para que desenvolvam ferramentas tecnológicas *anti-phishing*. As fraudes causam aos bancos tanto perdas financeiras como a erosão da confiança dos clientes nos sistemas de pagamentos e transações *on line*. De fato, incentivos mercadológicos já parecem estar dirigindo os bancos a lutarem contra o *phishing* da melhor forma que podem. As fraudes praticadas contra usuários de serviços na Internet ameaçam o desenvolvimento do comércio eletrônico. Se eles perdem a confiança na segurança das transações eletrônicas, quer seja porque não estão certos da identidade do site que visitam, quer porque temem de inadvertidamente divulgar informações pessoais, a conseqüência é um possível abalo ao modelo existente de *e-commerce*. O reconhecimento, no âmbito da teoria jurídica, de que os bancos podem sofrer a responsabilização pelo ressarcimento dos prejuízos causados ao seu cliente, vítima de golpe de *phishing*, funcionaria como incentivo adicional para desenvolverem dispositivos capazes de eliminar esse tipo de praga tecnológica. Sofrendo responsabilização, e conseqüentemente sendo obrigados a reparar os

⁴⁵ TRF-5ª. Reg., AC 212207/RN, rel. Des. Federal Luiz Alberto Gurgel de Faria.

danos resultados das fraudes, os bancos (e as empresas de comércio eletrônico de uma forma geral) sentir-se-ão incentivados a adotar medidas tecnológicas de segurança mais adequadas a lidar com a nova realidade do *phishing*.

c) argumento da possibilidade técnica de evitar a fraude

Para se determinar a pessoa que deve responder pelos prejuízos produzidos por fraudes bancárias em ambientes eletrônicos é imprescindível a noção 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 transações fraudulentas, já que são os únicos com acesso a todos os dados e com habilidade para evoluir seus sistemas.

Por outro lado, os custos econômicos para o desenvolvimento de ferramentas tecnológicas de combates a fraudes tecnológicas são razoáveis, em relação os prejuízos que buscam prevenir, daí que a teoria a ser evoluída nesse campo específico da responsabilidade civil deve reconhecer o papel de interesse público que as instituições bancárias devem ter na atribuição de segurança a essas transações.

6.1. Adequação do novo padrão de responsabilidade à legislação existente

Já vimos que o banco é quem guarda a relação mais estreita com a vítima do golpe de *phishing*, a quem está vinculado por meio de uma relação contratual. É o prestador direto do serviço, cuja segurança, no caso de ataque, é que está mais suscetível a acusações de falha.

A imputação de responsabilidade aos bancos, no entanto, não pode ser feita de forma aleatória, mas deve adequar-se aos esquemas de responsabilidade civil (contratual) existentes em nosso sistema jurídico. Examinando os esquemas existentes, bem como seus fundamentos, é que identificamos aquele que pode servir de padrão à responsabilidade do prestador de serviços bancários *on line*, na reparação de danos causados à vítima (cliente) de golpe de *phishing*.

6.1.1 Responsabilidade contratual regida pelo CDC

Nenhum outro intermediário da cadeia de comunicação informática está tão ligado à vítima de *phishing* do que o seu próprio banco, com quem mantém uma relação contratual para prestação de serviços de *Internetbanking*. A responsabilidade do banco, portanto, 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 da Lei 8.078/90 (Código de Defesa do Consumidor). 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 *Internetbanking* 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 § 2º.

do art. 3º. alcança “qualquer atividade fornecida no mercado de consumo, mediante remuneração, inclusive as de natureza bancária”.

A jurisprudência inclusive já vem fazendo recurso de normas do CDC quando se trata de definir a responsabilidade dos bancos em matéria de fraudes eletrônicas. Por exemplo, a 5ª Turma Cível do Tribunal de Justiça do Distrito Federal manteve, por unanimidade, sentença do Juiz Franco Vicente Piccolo, da 1ª Vara Cível de Brasília, que condenou um banco a indenizar um correntista que teve sua conta invadida⁴⁶. Para fundamentar a condenação do banco, a sentença invocou a responsabilidade orientada pela *teoria do risco profissional*, nos termos da qual é responsável pela reparação dos danos aquele que maior lucro extrai da atividade que lhe deu origem⁴⁷. O próprio STJ vem enfrentando essas questões sob a ótica das normas do CDC, com a diferença de que tem firmado o entendimento de que o uso do cartão magnético e da senha é de responsabilidade do correntista, daí que se os entrega a terceiro incide a regra do § 3º. do art. 14, que isenta o fornecedor de responsabilidade quando a culpa é exclusiva do consumidor⁴⁸.

Esse tipo de compreensão do problema, data vênua, incorre em erro técnico-jurídico, uma vez não se deve enfrentá-lo por via da utilização do esquema de imputação de *responsabilidade objetiva*, prevista no art. 14 do CDC. Como se sabe, o CDC criou dois regimes diferentes de vícios do produto ou serviço. O primeiro, se refere aos vícios de insegurança, capazes de provocar o *fato do produto* ou *serviço*, ou seja, o defeito de insegurança que atinge o consumidor (ou terceiro) na sua integridade física ou psíquica. O *defeito de segurança* provoca danos à esfera da saúde física ou psíquica da pessoa, causando o *acidente de consumo*. A responsabilidade pelos danos causados por esse tipo de vício é de natureza extracontratual e independe de culpa. Trata-se de uma responsabilidade objetiva ou *responsabilidade não culposa*, já que os arts. 12 e 14 do CDC atribuem responsabilidade a certos fornecedores “independentemente da existência de culpa” pela reparação dos danos causados aos consumidores por defeitos do produto ou relativos à prestação dos serviços⁴⁹. Já o regime dos *vícios de inadequação* ou de funcionalidade (tratados no art. 18 e ss.)⁵⁰ não caracteriza uma

⁴⁶ Segundo os autos, foram feitas transferências de valores da conta poupança da cliente sem a sua autorização, tendo ela informado o banco sobre a fraude praticada pela Internet. O banco tentou eximir-se de responsabilidade, atribuindo culpa à cliente, já que as transações foram feitas com o uso de sua senha pessoal (Proc. n. 20040110053359, em notícia do site Consultor Jurídico, de 01.06.06).

⁴⁷ Em trecho de sua sentença, o Juiz Franco Vicente Piccolo assentou o seguinte:

“Sabe-se que a prestação de serviços por meios eletrônicos tende a fomentar a atividade bancária, reduzir os custos operacionais e aumentar os lucros da instituição financeira. (...) Cabe destacar que, em casos tais, a doutrina e a jurisprudência assinalam que a imputação da responsabilidade civil orienta-se pela chamada teoria do risco profissional, nos termos da qual é responsável pela reparação dos danos aquele que maior lucro extrai da atividade que lhe deu origem” (grifo nosso).

⁴⁸ STJ-4ª. Turma, REsp 601805/SP, rel. Min. Jorge Scartezini, j. 20.10.05, DJ 13.11.05.

⁴⁹ O art. 12 do CDC disciplina a responsabilidade do fornecedor por *fato do produto*, enquanto que o art. 14 trata do *fato do serviço*.

⁵⁰ Os vícios por inadequação do produto são subdivididos em três tipos: vícios de impropriedade, vícios de diminuição do valor e vícios de disparidade informativa. Estes últimos também são denominados de vícios de qualidade por falha na informação ou simplesmente vícios de informação.

responsabilidade objetiva. Ao contrário dos arts. 12 e 14 (que tratam do *fato do produto ou serviço*), os arts. 18 e 20 (que regulamentam a responsabilidade por *vício do produto ou serviço*) não se utilizam da mesma expressão, ou seja, não indicam que o fornecedor responde pela reparação “independentemente da existência de culpa”. Em assim sendo, pode-se dizer que o regime dos *vícios de inadequação*, de natureza contratual, tem amparo numa “responsabilidade especial”⁵¹.

Os prejuízos decorrentes de *phishing* são de ordem exclusivamente patrimonial. Ou seja, a vítima da fraude sofre apenas danos materiais, não sendo atingida em sua integridade física ou psíquica, daí que não se configura o instituto do *fato do serviço* (ou *acidente de consumo*) e não se pode 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 *Internetbanking*), enquadrando-se no descritor normativo do art. 20, para efeito de justificar a responsabilização do prestador do serviço falho ou inadequado⁵².

Por outro lado, o que é relevante não é o aspecto subjetivo (da conduta do banco). Na definição do dever de reparação do fornecedor de serviços (bancários), o importante é um dado objetivo: se o serviço (de *Internetbanking*) é falho, no sentido de que não protege o usuário contra golpes de *phishing*. Mesmo não se tratando de uma responsabilidade puramente objetiva - a que é delineada no art. 20 do CDC - não exige culpa ou prova da culpa, mas apenas constatação do “vício”. Trata-se de uma *responsabilidade especial*, dependente de parâmetros impostos nas previsões legais específicas (art. 20 e seu § 2º.). De fato, ao estabelecer que “o fornecedor de serviços responde pelos vícios de qualidade que os tornem impróprios ao consumo”, o legislador criou um padrão de responsabilidade peculiar, que impõe a obrigação de liberar no mercado de consumo somente serviços isentos de vícios, não importando perquirir a culpa pelos danos causados em função do serviço viciado.

Cláudia Lima Marques 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 ela⁵³, o

⁵¹ Cláudia Lima Marques, explicando os critérios de responsabilidade por vícios dispostos no art. 18 do CDC, assevera: “Assim, no sistema do CDC, da tradicional responsabilidade assente na culpa passa-se à presunção geral desta e conclui-se com a imposição de uma *responsabilidade legal*” (Comentários ao Código de Defesa do Consumidor, Editora Revista dos Tribunais, 2ª. edição).

⁵² Segundo o art. 20 do CDC, “O fornecedor de serviços responde pelos vícios de qualidade que os tornem impróprios ao consumo....”.

⁵³ Comentários ao Código de Defesa do Consumidor, Editora Revista dos Tribunais, 2ª. edição, p. 259. A doutrinadora explica também que o legislador brasileiro, ao criar esse sistema especial de responsabilização, sofreu a influência do sistema da *common law*, de garantia implícita (*implied warranty*) de adequação e segurança do produto ou serviço, mas também inspirou-se no sistema da Diretiva Européia (Diretiva 35/374/CEE, de 25.07.85), que parte da idéia de defeito do produto introduzido no mercado como fundamento da responsabilidade do fornecedor. Desta fusão resultou o sistema do CDC.

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, por causa desse vício ou defeito, algum tipo de dano ao consumidor.

Ao tratar diretamente dos *vícios de inadequação*, a citada doutrinadora explicita a pouca importância do aspecto subjetivo da conduta do fornecedor na definição de sua responsabilidade:

“Concretamente, o CDC impõe aos fornecedores a obrigação de liberar no mercado somente produtos isentos de vícios. Trata-se de uma obrigação de resultado, não importa perquirir a culpa de algum dos fornecedores da cadeia. O importante é o vício, que será reclamado, normalmente, perante o comerciante direto, último na cadeia”⁵⁴ (grifos nossos).

Mais adiante, o comentar o art. 20 do CDC, Cláudia Lima Marques 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 diligência”⁵⁵.

E continua:

“Enquanto o direito tradicional se concentra na ação do fornecedor do serviço, no seu *fazer*, exigindo somente diligência e cuidados ordinários, o sistema do CDC, baseado na teoria da função social do contrato, concentra-se no *efeito do contrato*. O efeito do contrato é a prestação de uma obrigação de fazer, de meio ou de resultado. Este *efeito*, este serviço prestado, é que deve ser *adequado* para os fins que “razoavelmente dele se esperam”; é o serviço prestado, por exemplo, o transporte de passageiros, a pintura da parede da casa, a intervenção cirúrgica ou a

⁵⁴ Nos seus comentários ao art. 18 do CDC, ob. cit., p. 341.

⁵⁵ Ob. cit., p. 359.

guarda do automóvel na garagem, que deve possuir a adequação e a *prestabilidade* normal. Está claro que o fazer e o resultado são inseparáveis, conexos de qualquer maneira, mas o CDC como que presume que o fazer foi falho, viciado, se o serviço dele resultante não é adequado ou não possui a prestabilidade regular.

Se efetivamente o fornecedor agiu ou não com a diligência, o cuidado e a vigilância normal, quando da prestação de sua obrigação, importa apenas para a alegação de um eventual inadimplemento contratual. O recurso usado pelo CDC de instituir uma noção de vício do serviço facilitará a satisfação das expectativas legítimas dos consumidores também nos contratos de serviços, pois objetiva os critérios jurídicos para determinar se há ou não falha na prestação do fornecedor⁵⁶.

Como se observa, para fins de determinação dos limites da responsabilidade do fornecedor de serviços, o jurista deve se concentrar na análise do vício. O regime de vícios 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 *Internetbanking*.

E aqui, pelas razões já expostas anteriormente, deve-se entender que um sistema de *Internetbanking* que não proteja o usuário contra golpes de *phishing* não pode ser encarado como isento de vício. 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 combater o *phishing*. 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 *Internetbanking* que oferece no mercado é viciado, dotado de *vício de inadequação* às finalidades que dele se espera. O cliente desse serviço tem uma *legítima expectativa* de proteção contra fraudes eletrônicas e, se não atende a essa expectativa, não se mostra adequado para realizar a finalidade que razoavelmente dele se espera. O sistema de *Internetbanking* que não tenha evoluído para proteger o cliente contra golpes de *phishing* é “impróprio ao consumo”, por conter vício de qualidade, já que se mostra inadequado aos fins que dele razoavelmente se espera (§ 2º. do art. 20 do CDC)⁵⁷.

7. Soluções tecnológicas empregadas pelos bancos para evitar fraudes eletrônicas

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

⁵⁶ Ob. cit., p. 359 e 360.

⁵⁷ Nos termos do § 2º. do art. 20 do CDC, “são impróprios os serviços que se mostrem inadequados para os fins que razoavelmente deles se esperam”.

tecnológicas que o banco emprega, em seu sistema informático, para proteger o usuário desse tipo de cilada eletrônica. Se verificado que a tecnologia empregada é capaz de eliminar completamente os efeitos do golpe de *phishing*, impedindo que o fraudador acesse os dados pessoais do cliente e realize (em nome deste) transferências de valores, o serviço de *Internetbanking* deve ser considerado como isento de vício, não gerando a responsabilidade do banco prestador do serviço. Se, ao contrário, ficar constatado que o sistema bancário é ineficiente, contendo furos que permitam o *phisher*, por qualquer meio, coletar as informações pessoais suficientes à concretização do golpe, o serviço deve ser encarado como “impróprio ao consumo”, portador de *vício de qualidade*, apto a desencadear a responsabilidade do banco (de acordo com o art. 20 do CDC).

Em assim sendo, é imprescindível um estudo dos variados tipos de mecanismos de segurança tecnológica que os bancos empregam em seus sistemas para transações e pagamentos *on line*. Ao longo dos anos, as instituições bancárias e sites de pagamentos têm implementado rigorosas medidas de proteção e tecnologias para garantir um nível superior de segurança, na tentativa de evitar a apropriação ilícita de dados dos seus clientes. A maioria delas não é capaz de garantir que a pessoa que acessa o banco virtual é mesmo o cliente, como veremos abaixo:

a) Firewall

É o nome dado ao dispositivo de uma rede de computadores que tem por objetivo aplicar uma política de segurança a um determinado ponto de controle da rede. Sua função consiste em regular o tráfego de dados entre redes distintas e impedir a transmissão e/ou recepção de acessos nocivos ou não autorizados de uma rede para outra⁵⁸. O termo inglês *firewall* faz alusão comparativa da função que este desempenha para evitar o alastramento de acessos nocivos dentro de uma rede de computadores à parede corta-fogo (*firewall*), que evita o alastramento de incêndios pelos cômodos de uma edificação⁵⁹.

Os bancos possuem uma complexa estrutura de segurança composta por sistemas de *firewalls* que filtram o acesso externo, protegendo assim os aplicativos e os dados internos. Por isso, apenas a identificação e senha possibilitam uma transação financeira na conta do cliente. Mas a utilização de dispositivo de *firewall* não elimina os efeitos do *phishing*, já que pressupõe que o cliente mantenha sigilo absoluto sobre sua identificação e senha, sem nunca cedê-la a outros. O *firewall* tem a função de impedir acessos nocivos ou não autorizados, mas o *phisher*, que se apossa previamente das senhas e dados bancário, acessa o sistema bancário virtual como se fosse o cliente legítimo.

⁵⁸ Conceito encontrado na *Wikipedia*.

⁵⁹ Existe na forma de software e hardware, ou na combinação de ambos (neste caso, normalmente é chamado de "appliance"). A complexidade de instalação depende do tamanho da rede, da política de segurança, da quantidade de regras que autorizam o fluxo de entrada e saída de informações e do grau de segurança desejado.

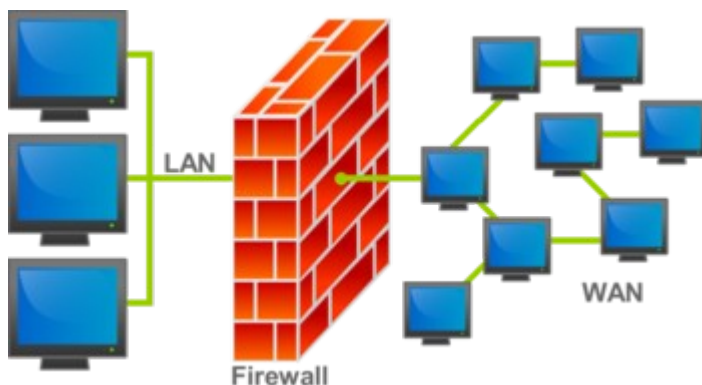


Figura representativa de Firewall separando redes LAN e WAN.

b) Criptografia de dados (SSL)

Os sites dos bancos adotam protocolo de segurança SSL (do inglês *Secure Sockets 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 criptografados (embaralhados), possibilitando que tais informações sejam acessadas somente pelo cliente e pelo banco⁶⁰.

Esse tipo de dispositivo ou protocolo de encriptação é capaz de combater um programa malicioso específico, chamado de *sniffer* (na tradução para o inglês, seria algo como “farejador”), que é utilizado para capturar e armazenar dados trafegando em uma rede de computadores. O *sniffer* é usado por um invasor para capturar informações sensíveis (como senhas de usuários), em casos onde estejam sendo utilizadas conexões inseguras, ou seja, sem criptografia.

Se é certo que o protocolo SSL pode fornecer confidencialidade na comunicação entre um cliente e um servidor, através do uso da criptografia, não se conforma em medida capaz de suprimir o *phishing*, pela simples razão de que o *phisher* não é uma terceira pessoa estranha à transação (comunicação com o banco), mas é admitido pelo sistema como se fosse o próprio cliente, já que dispõe das senhas de acesso deste, adquiridas em fase anterior da execução da fraude. O tráfego de toda a informação - incluindo a senha - é encriptado, tornando quase impossível uma terceira pessoa obter ou modificar a informação depois de enviada. Entretanto, a criptografia por si só não elimina a possibilidade de *hackers* conseguirem previamente acesso ao computador doméstico vulnerável do cliente e interceptarem suas senhas.

⁶⁰ Geralmente esse protocolo de segurança é indicado pela existência da figura de um cadeado fechado, localizada no lado direito da barra inferior – chamada de barra de status – do seu navegador (a figura do cadeado aparece a partir da tela de acesso onde é solicitada a senha). A figura do cadeado mostra que a página é segura.

c) Teclado Virtual

Os bancos disponibilizaram ainda um teclado virtual para aumentar a segurança no tratamento de senhas no navegador, dificultando o armazenamento em disco ou memória e também impedindo que programas ilícitos (*trojans* ou *spywares*) visualizem a digitação (das senhas). Portanto, o *Teclado Virtual* é uma fórmula implementada para aumentar a segurança no tratamento de senhas no programa navegador, dificultando que programas maliciosos possam “capturar” a senha do usuário, por meio do registro de teclas acionadas ou do posicionamento do mouse.

Alguns tipos de vírus (*keyloggers*) são capazes de gravar tudo o que é digitado pelo teclado convencional, inclusive senhas. Estes vírus entram no computador do cliente através de arquivos anexados em e-mails ou quando navega em um site suspeito. Uma vez instalados no computador do cliente, são capazes de capturar e armazenar (transferindo depois para o *hacker*) as teclas digitadas no teclado. A utilização do teclado virtual impede que esse tipo de vírus capte as informações, pois o registro das teclas acionadas não é armazenado no computador do cliente. Contudo, o teclado virtual não tem a capacidade de evitar que uma outra modalidade de vírus (*screenlogger*) permita que o fraudador capture as senhas da conta do cliente. O *screenlogger* é uma forma avançada capaz de armazenar a posição do cursor e a tela apresentada no monitor, nos momentos em que o mouse é clicado, ou armazenar a região que circunda a posição onde o mouse é clicado (ver figura abaixo).

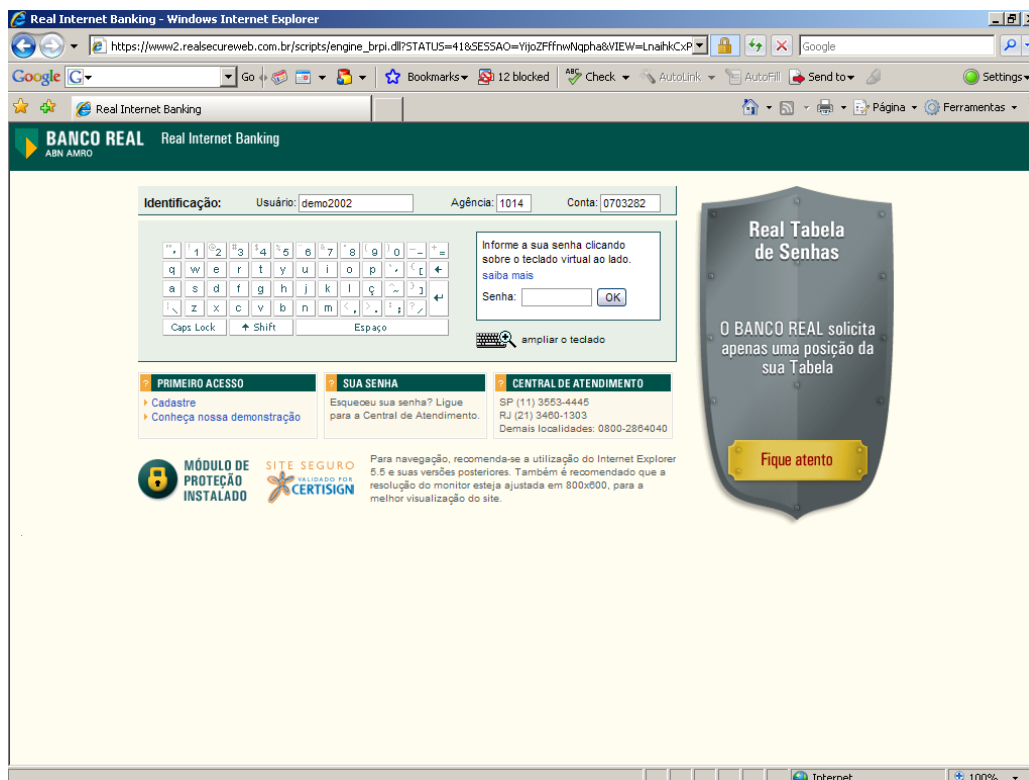


Foto 1. Representação em tela de programa navegador de um teclado virtual.



Foto 2. Mostra como o *screenlogger* captura a posição do cursor e tela do monitor do usuário.

d) Certificado Digital

Um *certificado digital* é um arquivo de computador que contém um conjunto de informações referentes à entidade para o qual o certificado foi emitido (seja uma empresa, pessoa física ou computador). A geração, distribuição e gerenciamento dos certificados digitais é feito por meio de entidades conhecidas como *autoridades certificadoras* (AC's). São essas autoridades certificadoras que vão garantir, por exemplo, que um certificado digital pertence realmente a uma determinada empresa ou pessoa. São elas que formam a cadeia de confiança que dá segurança ao sistema. Fazem o papel desempenhado pelos notários no sistema de certificação tradicional⁶¹.

Nas relações em um *website* é possível a garantia de autenticidade por meio desse sistema. O internauta que acessa um *site* pode se assegurar que ele pertence realmente a uma determinada empresa através do certificado digital exibido. Esse certificado contém os dados de identificação da pessoa responsável pelo *site* (ver figura abaixo). Na prática, o gerenciamento da relação de confiança funciona através de aplicativo de *software* incorporado ao computador do usuário. Normalmente, o software que faz a verificação de um certificado digital tem algum

⁶¹ Da mesma forma que os cartórios tradicionais, são organizadas segundo critérios legais e obedecem, na prestação dos seus serviços de certificação, a toda uma política de procedimentos, padrões e formatos técnicos estabelecidos em regimes normativos. Obedecem, portanto, a um modelo técnico de certificação e estrutura normativa, que define quem pode emitir certificado para quem e em quais condições. O conjunto ou modelo formado de autoridades certificadoras, políticas de certificação e protocolos técnicos compõe o que se convencionou chamar de "Infra-Estrutura de Chaves Públicas" ou simplesmente ICP.

mecanismo ou função para confiar em AC's. Por exemplo, o programa utilizado para navegar na Internet (conhecido como *browser*) contém uma lista das AC's em que confia. Quando o usuário visita um determinado *site* (por exemplo, de um *shopping on line* ou de um banco) e é apresentado ao navegador um Certificado Digital, ele verifica a AC que emitiu o certificado. Se a AC estiver na lista de autoridades confiáveis, o navegador aceita a identidade do *site* e exibe a página da *Web*. Em não sendo o caso, o navegador exibe uma mensagem de aviso, perguntando ao usuário se deseja confiar na nova AC. Geralmente o programa navegador dá opções para confiar permanente ou temporariamente na AC ou não confiar em absoluto. O usuário, portanto, tem controle sobre quais AC(s) deseja confiar, porém o gerenciamento da confiança é feito pelo aplicativo de *software* (neste exemplo, pelo navegador).

Esse tipo de tecnologia empregada em sites bancários não elimina o *phishing*. O cliente pode não ter a educação necessária para evitar transações em sites com certificados emitidos por AC's não confiáveis ou o seu programa de navegação pode não ser de uma versão atualizada, falhando na apresentação de páginas ou na indicação de sites confiáveis. Além disso, nem sempre a coleta de informações (senhas bancárias) é realizada por meio do preenchimento de formulários em sites falsos. O *phisher* pode conseguir acesso aos dados pessoais do cliente bancário através da infecção de seu computador com um vírus que lhe transmita os arquivos contendo as informações.

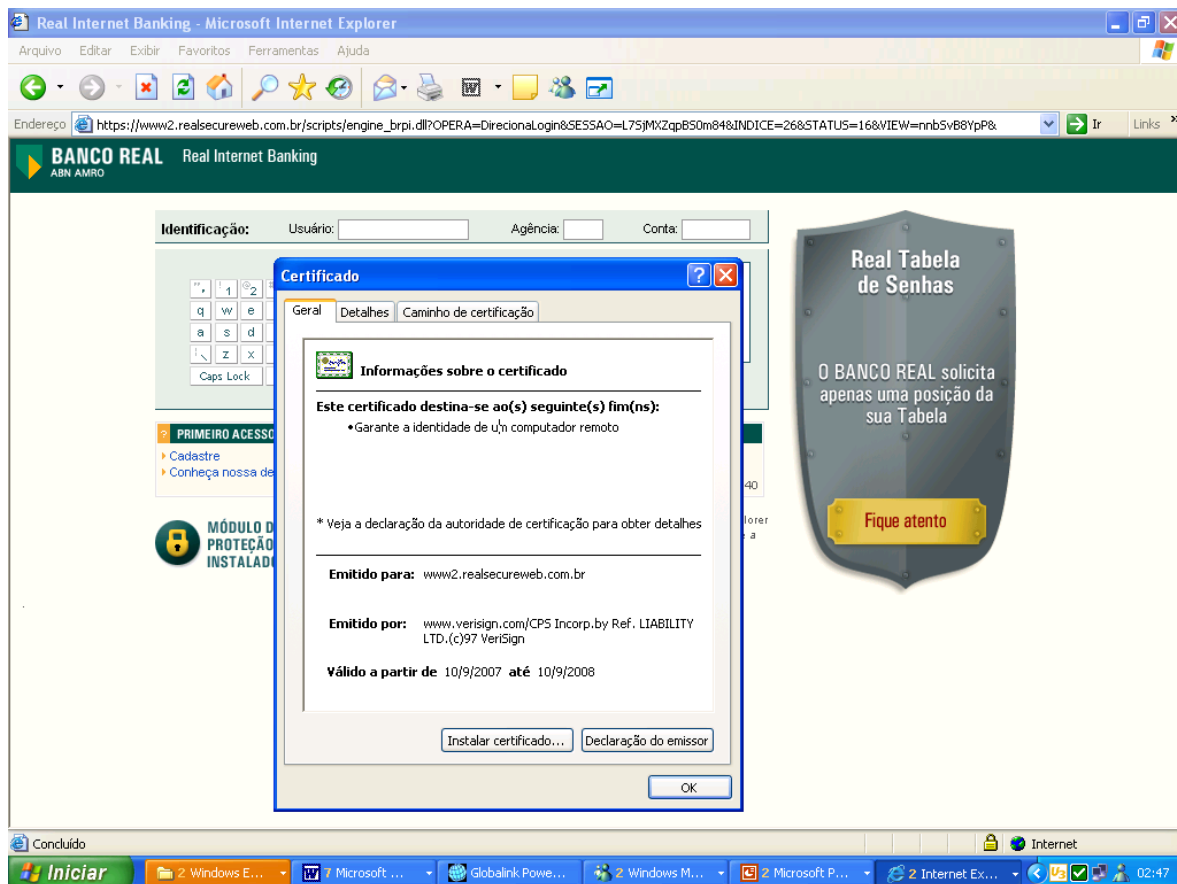


Figura mostrando ao meio o certificado digital do site de um banco.

e) Duplo fator de identificação ou sistema de senhas múltiplas

Uma falha de segurança que se tornou óbvia, diante dos diversos ataques de *phishing*, é o uso de uma senha única para acesso ao sistema de pagamento e transações *on line*. Nos sites de *Internetbanking* que funcionam mediante senha única, os fraudadores (*phishers*) necessitam de um único pedaço de informação para quebrar o sistema de segurança do banco. Requerer um pedaço adicional de informação (duplo fator de identificação) constitui uma inteligente forma de dificultar a ação dos criminosos. Além do código de utilizador (nome do usuário) e da *password* (senha) de acesso, pode-se exigir uma segunda *password* (de negociação), que constitui o código de segurança de 2º. nível. Ainda mais seguro é implantar um sistema em que a segunda senha seja aleatória, utilizável uma única vez. Assim, mesmo que o *phisher* consiga coletar ambas as senhas, não terá como acessar o sistema do banco posteriormente, pois a segunda senha só valeu para aquela transação já realizada pelo próprio usuário. A segunda senha é sempre variável, valendo apenas uma única vez.

Vários bancos brasileiros já se utilizam de sistemas de dupla autenticação, com a segunda senha variável. Um dos métodos utilizados para se viabilizar a segunda identificação de forma aleatória é o da “Tabela de Senhas” (ver figura abaixo). Consiste em um cartão com uma lista de 50 ou 70 códigos numéricos exclusivos que o cliente digita ao fazer transações de pagamento (DOC, TED, transferências, resgates etc.)⁶². Cada código é formado por quatro dígitos (senha) e quando o usuário faz uma transação de pagamento, visualiza, na tela do site, um número que terá uma senha correspondente na “Tabela de Senhas”, bastando digitá-la e dar seqüência à operação. Outra ferramenta utilizada como mais um nível de segurança, nos sistemas de *Internetbanking*, é o “token” ou cartão com display que emite senhas (ver figura abaixo). Esses dispositivos possuem um display embutido para emissão de senhas numéricas dinâmicas. Para reforçar a segurança nas transações de pagamento, o usuário tem que pressionar uma determinada área do “token” ou “displaycard”, para receber uma combinação numérica que será utilizada uma única vez.

⁶² O simples acesso para consultar saldos, extratos e realizar outras consultas não necessita da senha de 2º. nível, valendo apenas a senha de acesso.



Fig. 1. Representação de uma “Tabela de Senhas” emite senhas.

Chave de Segurança Bradesco Eletrônica

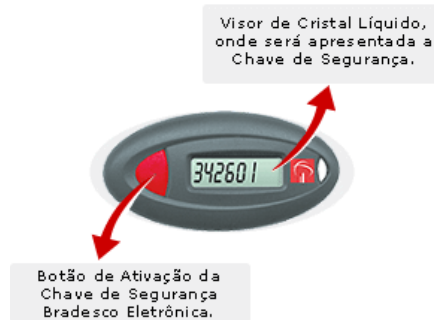


Fig. 2. Token com display que emite senhas.

Os especialistas são concordes em afirmar que esse sistema da dupla autenticação (com segunda senha aleatória) é capaz de eliminar a atual ameaça do *phishing*⁶³. O sistema “two-factor” de autenticação, que já tem sido implementado por alguns bancos, é suficiente para estancar os ataques de *phishing* atualmente conhecidos.

O sistema de dupla autenticação, todavia, não é bastante para as formas de *phishing* que combinem alguma forma de “engenharia social” (*social engineering*)⁶⁴. De fato, os *phishers* já começam a usar, além das mensagens de e-mail, outras táticas para iludir o usuário a fornecer os seus dados. Já há registros de novas versões para este tipo de ataque onde é utilizado contato telefônico. O ataque é similar só que a maneira primária do ataque não é o envio do e-mail mas sim o contato direto por telefone⁶⁵. O fraudador liga para o cliente, fazendo-se passar por algum funcionário do banco, e, alegando que está havendo algum defeito no sistema bancário, pede a senha para corrigi-lo. Caso o cliente entregue a senha, o suposto técnico pode realizar uma infinidade de atividades maliciosas, utilizando a sua conta de acesso à Internet e, portanto, relacionando tais atividades ao seu nome. Esses casos mostram ataques típicos de *engenharia social*, pois o discurso apresentado no exemplo procura induzir o usuário a realizar

⁶³ No relatório FDIC consta o depoimento de perito, nos seguintes termos: “[A]most all *phishing* scams in use today could be thwarted by the use of two-factor authentication.”). Two-factor identification combines factor one, a password, with factor two, either biometric information (such as fingerprints, eye scans, or a voice read) or a token (such as a USB device that plugs into the user’s computer’s USB port, or a smart card inserted into a reader). Systems protected by two-factor identification are far less vulnerable to phishers” (*supra* note 38, at 26).

⁶⁴ O termo *Engenharia Social* é utilizado para descrever um método de ataque onde alguém faz uso da persuasão, muitas vezes abusando da ingenuidade ou confiança do usuário, para obter informações que podem ser utilizadas para ter acesso não autorizado a computadores ou informações. *Engenharia Social* é uma modalidade de estelionato prevista no artigo 171 do Código Penal brasileiro.

⁶⁵ Também pode ocorrer a combinação dessas duas formas de contato. Alguns exemplos apresentam casos onde foram utilizadas mensagens de e-mail e contato telefônico. O cliente recebe uma mensagem de e-mail onde o remetente se passa pelo gerente ou o departamento de suporte do banco. No corpo da mensagem de e-mail é fornecido um número de telefone do suporte do banco, para o cliente mesmo fazer a ligação.

uma tarefa e o sucesso do ataque depende única e exclusivamente da decisão do usuário em fornecer informações sensíveis⁶⁶. A “Tabela de Senhas” ou o dispositivo eletrônico de emissão de senhas (*token* ou *displaycard*) pode não ser suficiente para deter essa nova forma de fraude, pois o fraudador pode solicitar à vítima (cliente) que forneça a senha (de 2º. nível), no momento em que está (do outro lado da linha) acessando o sistema.

8. Proporção entre adoção de práticas seguras pelos bancos e a diminuição do grau de responsabilização

Se os bancos, forçados por incentivos mercadológicos e por uma incerteza diante da definição de responsabilidade pela reparação dos prejuízos causados pelo *phishing*, adotaram medidas eficientemente fortes, a tendência é diminuição do seu grau de responsabilização. Se, ao contrário, as medidas não se mostrarem suficientemente vigorosas, a possibilidade de suportarem o ônus da reparação dos prejuízos aumenta. Em outras palavras, há uma verdadeira proporção entre as medidas de segurança adotadas pelos bancos e o seu grau de responsabilidade na indenização dos prejuízos decorrentes do *phishing*. Na medida em que os bancos adotam novas ferramentas tecnológicas de segurança, o *phishing* se torna menos eficiente, com a correspondente diminuição do risco de responsabilização. Se há uma compreensão de que os bancos tomaram iniciativas vigorosas, no desenvolvimento e implantação de medidas de segurança, voltadas à eliminação desse tipo de fraude tecnológica (*phishing*), então a probabilidade de sofrerem responsabilização diminui sensivelmente.

Como ficou evidenciado que a responsabilidade do fornecedor (banco) tem que ser examinada sob o aspecto objetivo da introdução (ou não) de um serviço com *vício*, e se esse *vício* foi determinante para causar dano ao seu consumidor (cliente)⁶⁷, a questão crítica, em cada caso concreto, é saber quando o sistema bancário está respondendo apropriadamente aos riscos impostos pelo *phishing*, ou seja, se evoluiu apropriadamente em resposta a essa ameaça tecnológica. A premissa deve ser a de que o banco que não tenha instalado método de autenticação com mais de um nível de segurança (sendo um deles através de senha aleatória) deve ser responsabilizado pelos prejuízos patrimoniais causados pelo fraudador (*phisher*) ao seu cliente. As soluções tecnológicas de segurança inicialmente implantadas pelos bancos, tais como *firewall*, criptografia de dados, teclado virtual e certificado digital, não são aptas a eliminar os efeitos do *phishing*, pela simples razão de que o fraudador acessa o sistema do banco como se fosse o legítimo usuário, já que se apossa previamente das senhas deste⁶⁸. Essas medidas de segurança, portanto, são ineficientes diante do *phishing*, e o banco que somente dispor delas deve ser inevitavelmente condenado a reparar os prejuízos sofridos pelo seu cliente. Nessa situação, o sistema de *Internebanking* deve ser encarado como um serviço que contém *vício de funcionalidade* (falha na

⁶⁶ Essa variedade do ataque de *phishing* que pressupõe a intervenção do agente humano, que atua no convencimento do cliente a entregar seus dados, é também chamada de “man in the middle”.

⁶⁷ Ver item 6.1.1.

⁶⁸ Como vimos em item acima (item 7).

adequação, na prestabilidade), já que não protege adequadamente a confidencialidade dos dados pessoais do cliente (para efeito de acesso ao sistema). Sendo o serviço inadequado às finalidades que dele se espera (proteger o usuário de fraudes tecnológicas), e portanto “impróprio ao consumo”, o fornecedor (banco) responde pela reparação dos prejuízos decorrentes do vício, nos termos do art. 20 e seu § 2º. do CDC⁶⁹.

O fato é que as formas mais corriqueiras de *phishing* podiam ser completamente eliminadas se os bancos tivessem implementado certas medidas tecnológicas. Os ataques de *phishing* ainda têm eficácia atualmente, de certa forma, porque as instituições financeiras permitiram esse estado de coisas. Até que implantem procedimentos seguros, não deve haver mudança na atribuição de responsabilidades pelos danos decorrentes desses ataques.

A situação se inverte para os bancos que introduziram métodos de múltiplos níveis de autenticação, com um deles realizado através da inserção de senha aleatória fornecida por dispositivo cuja responsabilidade pela guarda é do usuário (tabela de senhas, *token* ou *displaycard*). A introdução desse método de segurança para transações de pagamento afasta a inicial constatação de ineficiência quanto ao resguardo dos dados pessoais (dos clientes). Quando ocorre de o *phisher* se apropriar da senha (*password*) de acesso, ele fica apenas com um pedaço da informação (dados do cliente), que não é suficiente para realizar uma transação de transferência de numerário. A segunda senha, por ser aleatória e informada somente no momento da efetivação da transação (pela tabela de senhas, *token* ou *displaycard*), só vale para uma única operação realizada pelo próprio usuário (que é quem controla e guarda o dispositivo eletrônico de emissão de senhas). Assim, mesmo que o criminoso colete também a senha de segundo nível, esta já perdeu sua validade, não servindo para uma segunda operação.

Portanto, serviço de *Internetbankig* que disponha de múltiplo fator de autenticação (com senha de segundo nível aleatória) não sofre de *vício de inadequação*, e se não dispõe de vício, o fornecedor (banco) não pode ser responsabilizado por eventuais prejuízos, cuja causa se entende como sendo outra qualquer (culpa exclusiva da vítima). O *vício* é que fundamenta o dever de reparação do fornecedor; sem *vício*, não pode ser condenado a reparar os danos provenientes do *phishing*, já que a origem dos prejuízos (causa), nessa hipótese, é considerada como do âmbito da conduta do próprio cliente. É de ser considerado, nessa hipótese, que a concretização dos efeitos da fraude (prejuízos patrimoniais à vítima) foi causada não por uma falha do serviço, indene de *vício*, mas por outra causa – culpa da própria vítima.

É certo, por outro lado, que o múltiplo fator de autenticação não protege totalmente de golpe de *phishing* mesclado com “engenharia social” (também

⁶⁹ O inc. II do art. 20 do CDC prevê expressamente que, além da restituição da quantia paga, o consumidor pode exigir do fornecedor a reparação de eventuais perdas e danos causados por *vício de qualidade* do serviço.

chamado de “man in the middle”). Para além dos e-mails e dos sites falsos, os *phishers* também usam o telefone para contactar os clientes, fazendo-se passar por funcionários dos bancos. Mas, nesse caso, como a fraude não é exclusivamente tecnológica, deve haver um reconhecimento da exclusão da responsabilidade dos bancos, pela admissão de que os sistemas informáticos que utilizam duplo fator de autenticação (com a segunda senha aleatória) não podem ser considerados *inadequados*. Uma pessoa pode se passar por um funcionário do banco e solicitar o *token* do cliente, além de sua senha de primeiro acesso e, com isso, realizar operações de transferências de dinheiro. O próprio correntista, por confiança, pode passar o dispositivo e a senha para uma pessoa conhecida, que realiza a transação sem seu conhecimento. Ou seja, sempre haverá a possibilidade de um fraudador burlar um sistema de segurança. Mas, nesses casos, deve ser reconhecido que o sistema do banco é eficiente contra as fraudes meramente tecnológicas e que, quanto às hipóteses de fraudes cuja execução é mesclada pela “engenharia social”, o próprio cliente é que deve assumir o prejuízo, por ter repassado negligentemente seus dados pessoais ao fraudador.

Nos golpes “puros” de *phishing*, o cliente do banco sequer sabe que outra pessoa está coletando seus dados – o criminoso se vale de vírus ou de um site falso para coletá-los; já nos golpes que envolvem “engenharia social”, é o próprio cliente quem repassa seus dados para o fraudador (ainda que tenha sido ludibriado a achar que se trata de um representante legítimo do banco). O sucesso do ataque depende única e exclusivamente da decisão do usuário em fornecer informações sensíveis.

Para os bancos que tenham implantado sistema múltiplo de autenticação (com senha de segundo nível aleatória), mostra-se apropriada a jurisprudência do STJ sobre fraudes em sistemas eletrônicos de pagamento, que atribui o dever de vigilância sobre os dados pessoais ao próprio correntista, cabendo a este “cuidar pessoalmente da guarda de seu cartão magnético e sigilo de sua senha pessoal no momento em que deles faz uso”, não podendo “ceder o cartão a quem quer que seja, muito menos fornecer sua senha a terceiros”, porquanto, “ao agir dessa forma, passa a assumir os riscos de sua conduta, que contribui, à toda evidência, para que seja vítima de fraudadores e estelionatários”⁷⁰. Essa jurisprudência

⁷⁰ STJ-4ª. Turma, REsp 601805-SP, rel. Min. Jorge Scartezini, j. 20.10.05, DJ 14.11.05. A ementa desse julgado 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.

1 - 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, 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).

2 - Fica excluída a responsabilidade da instituição financeira nos casos em que o fornecedor de serviços comprovar que o defeito inexistente ou que, apesar de existir, a culpa é exclusiva do consumidor ou de

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 e, havendo quebra desse dever, não há relação de causalidade entre a atuação do banco e o prejuízo eventualmente gerado por esse descuido⁷¹.

Realmente, de alguma forma o cliente tem que ser responsável pela confidencialidade de sua senha e dispositivos de acesso, considerando que o banco fez a parte dele em termos de segurança informática, ao desenvolver a tecnologia do duplo fator de autenticação. Se os experts consideram que a tecnologia do duplo (ou múltiplo) fator de autenticação é eficaz contra o *phishing* (na sua forma pura), o restante é o correntista quem tem que cumprir. Os bancos já fizeram a sua parte implementando um sistema de segurança eficaz. Se o cliente não toma cuidado, e entrega todas as suas senhas e dispositivos de segurança (tabela de senhas, *token* ou *displaycard*) a outra pessoa, ele é no mínimo descuidado e totalmente responsável pelos seus atos. Não existe sistema de autenticação de acesso em que se possa prescindir a participação do cliente, adotando certas precauções. Assim, a segurança dos dados e transações do cliente é também, em alguma extensão, de sua responsabilidade.

É preciso ter em mente, por outro lado, que uma jurisprudência extremamente ampla em termos de responsabilização dos bancos pode simplesmente inviabilizar o “modelo de negócios” construído na *web* via serviços de *online banking*. Se o cliente não tem qualquer temor de que pode sofrer perdas financeiras, nunca vai ser estimulado a tomar cuidado com seus equipamentos de segurança (de acesso ao sistema bancário). Ademais, entender-se que em todos os casos de fraude o banco deve ser responsável pela reparação dos prejuízos,

terceiro (art. 14, § 3º do CDC).

3 - Recurso conhecido e provido para restabelecer a r. sentença”.

A única crítica que deve ser feita a esse julgado é a invocação do art. 14, § 3º. do CDC, ao invés do seu art. 20, par. 2º. Houve, nesse caso, um erro de apreciação entre o que seja fato do serviço e simples vício do serviço.

⁷¹ Representativos dessa corrente jurisprudencial são os acórdãos abaixo ementados:

“CIVIL. CONTA-CORRENTE. SAQUE INDEVIDO. CARTÃO MAGNÉTICO. SENHA. INDENIZAÇÃO. IMPROCEDÊNCIA.

1 - O uso do cartão magnético com sua respectiva senha é exclusivo do correntista e, portanto, eventuais saques irregulares na conta somente geram responsabilidade para o Banco se provado ter agido com negligência, imperícia ou imprudência na entrega do numerário.

2 - Recurso especial conhecido e provido para julgar improcedente o pedido inicial” (STJ-4ª. Turma, REsp 602680-BA, rel. Min. Fernando Gonçalves, j. 21.10.04, DJ 16.11.04).

“CIVIL E PROCESSUAL. AÇÃO DE INDENIZAÇÃO. SAQUE EM CONTA CORRENTE MEDIANTE USO DE CARTÃO MAGNÉTICO. DANOS MORAIS E MATERIAIS. ÔNUS DA PROVA. EXTENSÃO INDEVIDA. CPC, ART. 333, I.

I. Extraída da conta corrente do cliente determinada importância por intermédio de uso de cartão magnético e senha pessoal, basta ao estabelecimento bancário provar tal fato, de modo a demonstrar que não agiu com culpa, incumbindo à autora, em contrapartida, comprovar a negligência, imperícia ou imprudência do réu na entrega do numerário.

II. Recurso especial conhecido e provido, para julgar improcedente a ação” (STJ-4ª. Turma, REsp 417835-AL, rel. Min. Aldir Passarinho Junior, j. 11.06.02, DJ 19.08.02).

tal estado de coisas alimentaria a possibilidade de um cliente simplesmente forjar um “legítimo acesso”, e depois pedir que o banco reembolsasse o dinheiro. O jurista deve ter em conta que a responsabilidade ilimitada dos bancos pode criar a indústria dos “falsos acessos”, terminando por dismantelar o “modelo” de serviços bancários *on line*. Não se pode, portanto, adotar um padrão de responsabilidade estrito e exclusivo para os bancos, no sentido de que estes estariam sempre obrigados a responder por toda e qualquer operação fraudulenta no acesso ao sistema de serviços bancários *on line*, mesmo evidenciado certo grau de negligência ou descuido por parte do usuário.

Diante dessas observações, até que as instituições financeiras tenham implementado sistemas de múltiplas senhas devem sofrer responsabilização pelas conseqüências do *phishing*. É dizer: banco *online* que não disponha desse mais avançado padrão de segurança deve responder pelos danos patrimoniais causados aos seus clientes como resultado de fraude eletrônica (*phishing*), em razão da falha (*vício*) do serviço, que não oferece proteção contra esse tipo de ataque informático. A evolução do sistema de autenticação para o de múltiplas senhas (com senha de segundo nível aleatória), para efeito de acesso ao ambiente de *Internetbanking*, leva a uma transferência da responsabilidade para os próprios clientes, pela constatação de que não há nexo de causalidade entre a atuação do banco (o sistema passa a ser considerado como isento de *vício de funcionalidade*) e o prejuízo material.

9. Conclusões:

1ª.) É inviável tentar responsabilizar o provedor de Internet pelos prejuízos decorrentes do *phishing*, 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. Nem por inércia na remoção do conteúdo ilícito, quando comunicado da presença de uma *spoofed webpage* hospedada em seu sistema, o provedor pode ser responsabilizado, pois em geral os próprios fraudadores tomam a iniciativa de remover o material, imediatamente após as tentativas de execução do golpe.

2ª.) Também não é razoável exigir que os provedores de serviços de *e-mail* sejam responsabilizados pelos danos que mensagens de *phishing scam* possam acarretar aos seus usuários. A menos que o contrato com o usuário contenha cláusula expressa nesse sentido, o provedor não tem uma obrigação de triagem das mensagens e, tendo em vista a natureza do serviço de *e-mail* e o atual estado da técnica referente às comunicações e transmissões eletrônicas de dados via Internet, as tecnologias disponíveis permitem um grau limitado de impedimento de chegada de mensagens fraudulentas à caixa postal dos usuários.

3ª.) A legislação criminal que objetiva a punição exclusiva do agente direto, praticante do *phishing*, não produz resultado satisfatório em termos de resposta à pessoa da vítima. Como os *phishers* atuam sob técnicas que favorecem o anonimato, quase sempre não conseguem ser identificados, permanecendo a

vítima sem a restauração de seu patrimônio. Daí a necessidade do desenvolvimento de teoria na órbita civil, que admita a possibilidade de responsabilização de outro intermediário da comunicação eletrônica, para suportar o ônus de reparar o dano causado à vítima da fraude.

4º.) Dentre todos os partícipes da cadeia de comunicação telemática, é o banco (prestador dos serviços de *Internetbanking*) quem está mais visivelmente posicionado de forma a interferir e impedir os efeitos da ação do *phisher*. Por ser a parte que controla tecnicamente o acesso ao serviço de *Internetbanking*, pode prevenir os ataques de forma mais eficaz do que qualquer outro agente intermediário da cadeia eletrônica de comunicação. E é justamente por isso, por ser o agente intermediário que tem o maior controle tecnológico para evitar a consecução da fraude, que pode ser chamado à responsabilização, para reparar os efeitos patrimoniais do ilícito. Além disso, nenhum outro intermediário da cadeia de comunicação informática está tão ligado à vítima de *phishing* do que o seu próprio banco, com quem mantém uma relação contratual para prestação de serviços de *Internetbanking*.

5º.) A imputação de responsabilidade aos bancos, no entanto, não pode ser feita de forma aleatória, mas deve submeter-se aos esquemas de responsabilidade civil (contratual) existentes em nosso ordenamento jurídico. Examinando a natureza do vínculo que prende o banco ao seu cliente, identificamos a presença de uma relação de consumo, a ser regida pelas normas da Lei 8.078/90 (Código de Defesa do Consumidor). No universo textual do CDC, encontramos um esquema de *responsabilidade especial* (no art. 20), atribuível aos fornecedores por *vícios de inadequação* dos serviços que disponibiliza no mercado. É com esse enquadramento legal que deve ser definida a responsabilidade dos bancos pelas conseqüências resultantes do *phishing*.

6ª.) No regime dos *vícios de inadequação* do serviço, tratado no art. 20 do 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 *Internetbanking*) é falho (viciado) ou não. E um sistema de *Internetbanking* que não proteja o usuário contra golpes de *phishing* não pode ser encarado como isento de **vício**. O cliente desse serviço tem uma *legítima expectativa* de proteção contra fraudes eletrônicas e, se não atende a essa expectativa, não se mostra adequado para realizar a finalidade que razoavelmente dele se espera. O sistema de *Internetbanking* que não tenha evoluído para proteger o cliente contra golpes de *phishing* é “impróprio ao consumo”, por conter vício de qualidade, já que se mostra inadequado aos fins que dele razoavelmente se espera (§ 2º. do art. 20 do CDC)

7ª.) Como a definição da responsabilidade passa necessariamente pela análise da adequação do serviço, ou seja, se não padece de vício que comprometa sua funcionalidade, o dever de reparação dos danos de cliente bancário sofrido em decorrência de *phishing* 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 método de autenticação com mais de um nível de segurança (sendo um deles através de senha aleatória) deve ser responsabilizado pelos prejuízos patrimoniais causados pelo fraudador (*phisher*) ao seu cliente. As soluções tecnológicas de segurança inicialmente implantadas pelos bancos, tais como *firewall*, criptografia de dados, teclado virtual e certificado digital, não são aptas a eliminar os efeitos do *phishing*. A introdução dos métodos de múltiplos níveis de autenticação, com um deles realizado através da inserção de senha aleatória fornecida por dispositivo cuja responsabilidade pela guarda é do usuário (tabela de senhas, *token* ou *displaycard*), afasta a inicial constatação de ineficiência quanto ao resguardo dos dados pessoais (dos clientes) - os *experts* consideram que essa nova tecnologia de autenticação é eficaz contra o *phishing* (na sua forma pura). Portanto, serviço de *Internetbanking* que disponha de múltiplo fator de autenticação (com senha de segundo nível aleatória) não sofre de *vício de inadequação*, e se não dispõe de vício, o fornecedor (banco) não pode ser responsabilizado por eventuais prejuízos, cuja causa se entende como sendo outra qualquer (culpa exclusiva da vítima).