Consumidor não tem culpa por transação em home banking

A jurisprudência brasileira cível ainda é vacilante quando trata da retirada indevida de dinheiro através de *home banking*. A maior parte dos julgados reconhece a responsabilidade objetiva do banco fazendo a relação de que basta haver o dano e o nexo causal sem a necessidade de existência de culpa por parte do banco. Entende-se que se o sistema permite a manipulação indevida das contas ele seria, por concepção, inseguro. No entanto, a questão não é tão simples assim.

Outros julgados eximem o banco da responsabilidade ao entender que houve culpa exclusiva do correntista. Em geral alega-se que o sistema é totalmente seguro e que a invasão da conta deu-se por negligência do correntista. O Código de Defesa do Consumidor, quando explica a questão da responsabilidade objetiva aplicada aos serviços assim diz no parágrafo 3º, inciso III do artigo 12:

§3 – O fabricante, o construtor, o produtor ou importador só não será responsabilizado quando provar:

…

III – a culpa exclusiva do consumidor ou de terceiro.

Um dos leading cases sobre a culpa exclusiva do usuário de Internet por negligência é a APC. 70.011.140.902, do TJ-RS. Assim diz a ementa:

APELAÇÃO. DECLARATÓRIA DE INEXISTÊNCIA DE DÉBITO. TELEFONIA. SERVIÇO NÃO PRESTADO. COBRANÇA. INSCRIÇÃO NO SERASA. Internet. conexão a provedor internacional. vírus. A ligação telefônica internacional para a Ilha Salomão, que ocasionou o alto valor cobrado na fatura emitida pela ré, decorreu de discagem internacional provocada por vírus instalado na máquina do autor. Quem navega na rede internacional (WEB) deve, necessariamente, utilizar um programa 'anti-vírus' para evitar tais acontecimentos. Negligência do autor. Inexistência de ato ilícito atribuível à Embratel. AÇÃO IMPROCEDENTE. APELAÇÃO IMPROVIDA.

No entanto para a caracterização dessa culpa exclusiva deve haver o cumprimento do dever de informar da instituição bancária. O banco deve sempre informar acerca dos riscos de utilização do serviço. Este dever de segurança é um direito básico do consumidor assim explicitado no artigo 6°, inciso III:

Art. 6º – São direitos básicos do consumidor:

…

III – a informação adequada e clara sobre os diferentes produtos e serviços, com especificação correta de quantidade, características, composição, qualidade e preço, bem como sobre os riscos que apresentem;

Vemos também a menção no artigo 9º do CDC:

Art. 9º – O fornecedor de produtos e serviços potencialmente nocivos ou perigosos à saúde ou segurança deverá informar, de maneira ostensiva e adequada, a respeito da sua nocividade ou periculosidade, sem prejuízo da adoção de outras medidas cabíveis em cada caso concreto

2023 - www.conjur.com.br - Todos os direitos reservados.

.

A norma mais esclarecedora talvez seja a do artigo 31 do CDC:

Art. 31 – A oferta e apresentação de produtos ou serviços devem assegurar informações corretas, claras, precisas, ostensivas e em língua portuguesa sobre suas características, qualidades, quantidade, composição, preço, garantia, prazos de validade e origem, entre outros dados, bem como sobre os riscos que apresentam à saúde e segurança dos consumidores.

É sabido que na internet é bastante comum a propagação de vírus (ou códigos maliciosos) que realizam as mais variadas funções. Alguns destes têm a função específica de conseguir capturar os caracteres digitados no teclado do computador, passando-os para o criminoso. Os tribunais entendem que caso o banco realize campanhas ostensivas de segurança, ele cumpriria com o dever de informação eximindo-se assim de qualquer responsabilidade em caso de invasão dos computadores dos seus clientes. A pergunta que deve ser feita é a seguinte: Será que um sistema inseguro, pode ter sua insegurança compensada pelo cumprimento do dever de informar? Na nossa opinião, a resposta é negativa.

O dever de informação deve ser satisfeito de maneira que cumpra sua função, nos termos dos artigos acima citados. A informação passada acerca do serviço deve ser eficiente para cientificar completamente o cliente do banco acerca de suas responsabilidades específicas, caso haja. O cliente necessita ter, com a informação prestada, condições de escolha sobre o uso do serviço.

O professor Christoph Fabian (O Dever de Informar no Direito Civil. São Paulo:RT, 2002) ao tratar do dever de informar, assim preceitua:

A instrução deve ser clara, ostensiva, e facilmente compreensível para o consumidor. Tais instruções não devem ficar escondidas entre elogios do produto ou alguma propaganda. p. 147

…

Uma informação é ostensiva quando se exterioriza de forma tão manifesta e translúcida que uma pessoa, de mediana inteligência, não tem como alegar ignorância ou desinformação. p. 150

Nota-se que as campanhas promovidas pelos bancos mais parecem propagandas do que reais advertências sobre o uso do sistema. Com as campanhas atuais, muitas vezes escondidas, não há como garantir a ostensividade da informação exigida pelo CDC. Quem pode, por exemplo, negar a ostensividade das advertências dispostas nas carteiras de cigarro? O autor ainda diz (p. 151) que a expressão “Beba com moderação” disposta nas bebidas, não é bastante ostensiva.

Há um mecanismo bastante interessante chamado *pré-logon-banner*, muito utilizado em ambientes corporativos e acadêmicos. Tal mecanismo consiste em pequenas janelas com informações, que são mostradas antes de alguém ter acesso ao sistema. Esses *pré-logon-banners* têm a função de passar informações para quem acessa o sistema. No ambiente corporativo eles têm a função de cientificar os colaboradores de que os sistemas são monitorados, que o uso deve ser apenas para fins profissionais, etc. Destaca-se que a informação é passada antes de se acessar o sistema. Caso a pessoa não concorde com

2023 - www.conjur.com.br - Todos os direitos reservados.

aquelas regras apresentadas, não consegue acessar o sistema. Vemos que um dispositivo semelhante poderia ser adaptado nos sistemas de *home banking*. Isso reforçaria o dever de informação do banco pela ostensividade do mecanismo. Não haveria como, antes do correntista acessar o sistema, não ler as recomendações de segurança.

Não percamos de vista também que os controles de Segurança da Informação são bastante complexos. É sabido que em incidentes de segurança, um dos aspectos mais explorados por criminosos é exatamente a parte humana da cadeia. E isso vale não apenas para ataques envolvendo *home banking*, mas também para outros sistemas. O processo de explorar as vulnerabilidades humanas para conseguir informações é conhecido como “engenharia social”. Aliado a isso deve ser dito que a atividade de tornar um sistema seguro não é tarefa simples.

A cada dia descobrem-se novas vulnerabilidades dos sistemas, inconsistências em sistemas operacionais além de novas formas de explorar falhas. Os especialistas em Segurança da Informação dizem inclusive que não existe um sistema 100% seguro; sempre haverá uma forma de quebrá-lo, seja por forma técnica ou mediante a exploração das vulnerabilidades humanas.

A ciência da computação, ao tratar também da segurança da informação, utiliza a seguinte premissa “Nenhuma corrente á mais forte do que seu elo mais fraco”. Ao que sabemos essa expressão foi cunhada originalmente por Arthur Conan Doyle (Nenhuma cadeia é mais forte do que seu elo mais fraco). A idéia é que todas as proteções de segurança aplicadas a um sistema tornam-se ineficazes se houver um ou mais controles ineficientes ou fracos. A segurança, então, é um processo que se não observado em todas as suas fases, torna o sistema mais ou totalmente inseguro.

Fazendo uma analogia, é como se alguém trancasse todas as portas de sua casa mas deixasse uma janela aberta. Esse “elo mais fraco” é a parte humana e diga-se de passagem, todo o especialista em segurança da informação sabe disso. O banco inclusive sabe muito bem disso. Por saber disso, os sistemas devem ser adaptados e protegidos contra essa vulnerabilidade. A construção dos sistemas deve observar sempre tal vulnerabilidade. A questão é saber se um sistema que permite a exploração desta vulnerabilidade pode ser considerado potencialmente inseguro. Entendemos que tal situação torna sim o sistema inseguro nos termos do CDC.

Tal insegurança provém, entre outras coisas, da disparidade de informações que tem o fornecedor e o consumidor. Como disto, o consumidor não tem condições técnicas de avaliar corretamente os riscos provenientes do uso do *home-banking*; não há como se exigir do consumidor o conhecimento das técnicas de engenharia social utilizadas pelos criminosos. Isso foge do conhecimento do homem comum, do homem médio. Tais relações baseiam-se na confiança que o consumidor deposita no serviço de *home banking*. Como ensina o professor Christoph Fabian, na obra já citada, a informação prestada pelo fornecedor deve atentar para os riscos do uso do produto ou serviço:

Os perigos previsíveis não são apenas aqueles que resultam do uso adequado. Eles abrangem também os perigos de utilizações erradas que podem naturalmente ou facilmente acontecer. p. 148

Por fim, entendemos que a interpretação da questão ainda deve evoluir. A doutrina e a jurisprudência devem ainda reforçar qual a extensão do dever de segurança. É urgente também que se defina se um sistema que permite a invasão através da exploração de vulnerabilidades humanas pode ser entendido

2023 - www.conjur.com.br - Todos os direitos reservados.

como seguro. Ainda, é importante que não se perca de vista a responsabilidade objetiva dos fornecedores de serviços; esquecer-se disto seria esquecer-se de aplicar o CDC às relações consumeiristas.

Date Created
17/11/2008

2023 - www.conjur.com.br - Todos os direitos reservados.