CENTRO UNIVERSITÁRIO DO ESTADO DO PARÁ
CURSO DE BACHARELADO EM DIREITO

GABRIEL ARAÚJO MELO
LUIZA NINA AVELAR CORRÊA

O AGRAVAMENTO DA VULNERABILIDADE DO CONSUMIDOR NO ÂMBITO DE INSTITUIÇÕES FINANCEIRAS DIGITAIS E O INCREMENTO DE FRAUDES BANCÁRIAS NO BRASIL

BELÉM
2023

GABRIEL ARAÚJO MELO
LUIZA NINA AVELAR CORRÊA

O AGRAVAMENTO DA VULNERABILIDADE DO CONSUMIDOR NO ÂMBITO DE INSTITUIÇÕES FINANCEIRAS DIGITAIS E O INCREMENTO DE FRAUDES BANCÁRIAS NO BRASIL

Trabalho de Conclusão de Curso apresentado como requisito parcial para obtenção de grau em Bacharel em Direito, pelo Centro Universitário do Estado do Pará.

Orientador: Prof. Me. Felipe Guimarães

BELÉM
2023

Dados Internacionais de Catalogação na Publicação (CIP)
Biblioteca do CESUPA, Belém – PA

M528a Melo, Gabriel Araújo.

O agravamento da vulnerabilidade do consumidor no âmbito de instituições financeiras digitais e o incremento de fraudes bancárias no Brasil / Gabriel Araújo Melo, Luiza Nina Avelar Corrêa. — Belém, 2023.

26 p.

Trabalho de Conclusão de Curso (Graduação) – Centro Universitário do Estado do Pará, Bacharelado em Direito, Belém, 2023.

Orientador: Prof. Me. Felipe Guimarães de Oliveira.

1. Direito do consumidor. 2. Instituições financeiras. 3. Fraudes bancárias. I. Corrêa, Luiza Nina Avelar. II. Oliveira, Felipe Guimarães (orient.). III. Título.

CDD 342.5

Regina Coeli Araújo Ribeiro CRB-2/739

GABRIEL ARAÚJO MELO
LUIZA NINA AVELAR CORRÊA

O AGRAVAMENTO DA VULNERABILIDADE DO CONSUMIDOR NO ÂMBITO DE INSTITUIÇÕES FINANCEIRAS DIGITAIS E O INCREMENTO DE FRAUDES BANCÁRIAS NO BRASIL

Trabalho de Conclusão de Curso apresentado como requisito parcial para obtenção de grau em Bacharel em Direito, pelo Centro Universitário do Estado do Pará.

Orientador: Prof. Me. Felipe Guimarães

Data de aprovação: _____/_____/_____

Conceito:

Banca Examinadora:

_____
Prof. Me. FELIPE GUIMARÃES - Orientador
Centro Universitário do Estado do Pará (CESUPA)

_____
Nome com titulação
Instituição a que pertence

_____
Nome com titulação
Instituição a que pertence

O AGRAVAMENTO DA VULNERABILIDADE DO CONSUMIDOR NO ÂMBITO DE INSTITUIÇÕES FINANCEIRAS DIGITAIS E O INCREMENTO DE FRAUDES BANCÁRIAS NO BRASIL

O AGRAVAMENTO DA VULNERABILIDADE DO CONSUMIDOR NO ÂMBITO DE INSTITUIÇÕES FINANCEIRAS DIGITAIS E O INCREMENTO DE FRAUDES BANCÁRIAS NO BRASIL

Gabriel Araújo Melo[1]
Luiza Nina Avelar Corrêa[1]
Felipe Guimarães[1]

RESUMO

O objetivo geral deste estudo é analisar o sistema bancário no que tange as relações dos clientes com o atendimento remoto (autoatendimento) e o processo de inovação que os bancos estão sendo obrigados a realizar para inibir as fraudes eletrônicas, de forma a diminuir as perdas financeiras. Ademais, pretende-se estabelecer o nexo entre a vulnerabilidade do consumidor frente a instituições financeiras digitais, bem como sua hipossuficiência nessa economia de mercado. A metodologia adotada para este estudo é a revisão bibliográfica, exploratória/qualitativa. Ao finalizar este estudo pode-se observar que, com a inclusão das novas tecnologias da comunicação, especialmente nos serviços consolidados no campo da Internet, as relações comerciais passaram a adotar novas configurações visando atender as demandas especificas, como no caso do contexto mercadológico que abrange as instituições bancárias e seu relacionamento com seus clientes. Diante da diversidade de transações oferecidas por meio do canal virtual e os consequentes investimentos realizados em segurança, as fraudes bancárias têm feito com que as instituições bancárias repensem seus procedimentos em termos de inovação, buscando ferramentas tecnológicas que devolvam ao usuário a segurança de utilizar estes serviços pela internet.

Palavras-chave: Sistema Bancário; Inovações Tecnológicas; Vulnerabilidade. Consumidor; Fraude Bancária.

ABSTRACT

The general objective of this study is to analyze the banking system in terms of customer relationships with remote service (self-service) and the innovation process that banks are being forced to carry out to inhibit electronic fraud, in order to reduce financial losses. In addition, it is intended to establish the link between consumer vulnerability to digital financial institutions, as well as their hyposufficiency in this market economy. The methodology adopted for this study is a bibliographical, exploratory/qualitative review. At the end of this study, it can be observed that, with the inclusion of new communication technologies, especially in consolidated services in the field of the Internet, commercial relations began to adopt new configurations in order to meet specific demands, as in the case of the marketing context that encompasses banking institutions and their relationship with their customers. Faced with the diversity of transactions offered through the virtual channel and the consequent investments made in security, bank fraud has made banking institutions rethink their procedures in terms of innovation, seeking technological tools that give back to the user the security of using these services through the Internet.

Key words: Banking System; Technological Innovations; Vulnerability. Consumer; Bank Fraud

[1] Aluno do curso de graduação Bacharelado em Direito, turma DI9TC, gabriel19060205@aluno.cesupa.br. Matrícula 19060205.
[2] Aluna do curso de graduação Bacharelado em Direito, turma DI9TC, luiza19060121@aluno.cesupa.br. Matrícula 19060121.
[3] Processor Orientador. Doutorando em Direito (UFPA).

1 INTRODUÇÃO

Frente as inovações nos diversos setores trazidos pela nova economia de mercado digital, um se destacou: os bancos e *fintechs* digitais. Podemos dizer que juntos, esses dois elementos do sistema bancário trouxeram diversas invocações e com essas, problemáticas já existentes se acentuaram.

Outrossim, a relação dos mesmos com o consumidor mudou, enquanto antes era pautada na presença física do consumidor na compra ou aquisição de um produto, agora, com as transações digitais, adquiriu forma prática, pendendo se dizer instantânea. Desta forma, fraudes bancárias se tornaram comum nesse meio globalizado e informacional, na qual os dados ema segurança do consumidor são postos em cheque quando não se há a presença maciça de segurança digital.

Ademais, não podemos desvincular disso, sua hipossuficiência que num mercado digital é intensificada, ainda mais quando tratamos de consumidores com pouco acesso à informação.

Nesse sentido, o presente trabalho versa sobre como o consumidor se situa nessa nova economia, e como bancos e instituições financeiras podem mudar esse retrato de vulnerabilidade do consumidor, de forma a promover um ambiente de consumo adequado e consciente.

2 SISTEMA FINANCEIRO DIGITAL: BANCOS E FINTECHS

O Sistema Financeiro Mundial sofreu diversas mudanças com o advento da internet, as movimentações financeiras se tornaram possível com apenas um "*click*", e movimentar dinheiro nunca foi tão rápido e fácil, tal qual Marco Antônio cita em o sistema bancário brasileiro:

> O sistema bancário digital revolucionou a forma como as pessoas interagem com seus serviços financeiros, oferecendo maior comodidade, agilidade e praticidade. Com a possibilidade de acessar sua conta bancária a qualquer hora e em qualquer lugar, realizar transações online e ter acesso a uma variedade de produtos financeiros, o sistema bancário digital se tornou essencial para a vida financeira moderna. (MARCOS, 2020, p.17)

Entretanto, tal evolução não adveio de modo igualitário e sistemático para toda a sociedade, e debater sobre a acessibilidade desse sistema, bem como a segurança que ele exprime para a sociedade é aspecto essencial na busca de um sistema bancário que faça valer o princípio fundamental previsto na constituição federal de 1988: Igualdade e inclusão social.

Em primeiro plano, devemos diferenciar as principais instituições que formam o sistema bancário digital atual: *Fintechs* e bancos digitais.

As *Fintechs* são denominadas como tecnologia financeira, traduzindo para língua portuguesa. É utilizada no âmbito digital, ofertando produto e serviços financeiros, em bancos eletrônicos/digitais, trazendo a facilidade para o consumidor na hora de realizar transações, sendo possível tudo de forma online.

Importante salientar que, existem vários tipos de *Fintechs*, sendo estas:

> **Fintechs de Controle Financeiro**: São constituídas por empresas tecnológicas, com o objetivo de auxiliar os consumidores com suas operações financeiras, através da tecnologia.
> **Fintechs de Crédito:** Facilidade em contratação de empréstimos bancários, passando por analise de crédito de uma forma mais "rápida".
> **Fintechs de Pagamento:** São constituídas por máquinas de cartão de crédito, com ausência de anuidade.
> **Fintechs de Crowdfunding:** Constituídas por plataformas digitais, no qual pessoas jurídicas e físicas tem a oportunidade de obter financiamento coletivo para projetos e afins.
> **Fintechs de Bitcoins:** A finalidade é intermediar a transações de vendas de criptomoedas.
> **Fintechs de Investimento:** Caracterizadas por serem fintechs que oferecem opões de investimentos no mercado financeiro, cambio, imobiliário, criptomoedas e etc.

Entretanto, *Fintechs* não são bancos eletrônicos/digitais, mas não integram bancos físicos, a sua finalidade é ofertar ao consumidor cartões de crédito sem anuidade, contas digitais gratuitas, empréstimos bancários seguros, dentre outros. E, são fiscalizadas pelo governo, bem como, regulamentadas pelo Banco Central (BACEN).

Já os Bancos Eletrônicos/Digitais são bancos apenas virtuais/online, que não possuem agencias ao público ou atendimento presencial, são Internet Banking, popularizada no país nos últimos anos.

Os bancos digitais têm as mesmas finalidades que bancos comuns, porém, todas as operações são realizadas de forma online, tendo serviços gratuitos, e sendo também regularizada pelo Banco Central.

Após a conceitualização exposta, faz-se necessário a menção de semelhanças entre as Fintechs e Bancos Eletrônicos, pois os bancos digitais utilizam fintechs para ofertar seus serviços ao consumidor final, mas uma fintech não é necessariamente um banco digital, por não estar em semelhança juntamente com as regras do BACEN, não podendo atuar como banco digital ou tradicional. A grande semelhança entre elas, são a forma de atuação online, com a finalidade de facilitar a vida do consumidor.

É inegável o aumento da tecnologia avançada nos últimos anos, não só no Brasil, como no mundo. Nesse contexto, os bancos digitais chegaram de forma inovadora, trazendo facilidade ao seu consumidor na hora de resolver problemáticas.

Podemos entrelaçar o aumento dos bancos eletrônicos com o surgimento das fintechs, que possibilitou inúmeros procedimentos atrelados a serviços gratuitos, como o cartão de crédito sem anuidade e a resolução de operações bancárias através de um aparelho de celular.

Com isso, a facilidade atraiu a curiosidade do consumidor, bem como a acessibilidade a informação de investimos de forma mais rápida e fácil.

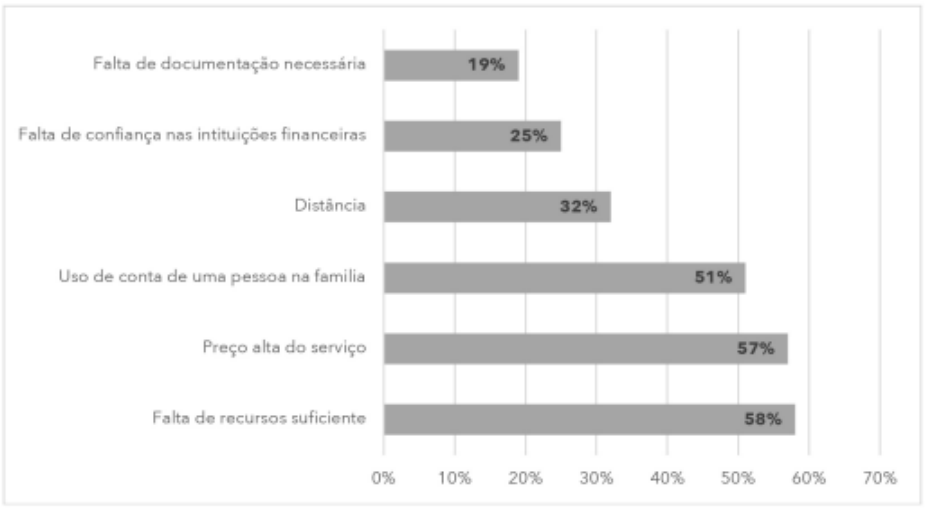
Os bancos eletrônicos/digitais já nasceram de forma totalmente online, não contendo agencias físicas, como exemplo. Já os bancos tradicionais, estão há mais tempo no mercado financeiro, atuando de forma física, contendo agência e atendimentos presencias, porém, estão cada vez mais se adaptando ao mundo digital também.

Vejamos algumas das principais diferenças entre os bancos:

> **Abertura de uma conta:** Apesar dos bancos tradicionais estarem se adaptando ao mundo digital, como mencionado acima, atualmente ainda existem diversas burocracias para abertura de um conta, como de deslocar até ao um banco tradicional com documentos de comprovação para conseguir tal ato. Já nos bancos digitais, basta o consumidor baixar o aplicativo do banco para seu celular e realizar os procedimentos solicitados, sem precisar se locomover.
> **A quantidade de serviços:** A quantidade de serviços ofertados pelos bancos tradicionais x bancos eletrônicos, são quase a mesma em valor de porcentagem. Entretanto, no banco digital o consumidor tem conhecimento mais elevado em relações as suas operações, visto que o acesso é inteiramente através do aplicativo do banco. No entanto, o atendimento presencial nesses bancos são inexistentes, bem como, o saque de dinheiro em espécie, já que não possuem agencias físicas.
> **Valor de tarifas:** Pelo fato dos bancos eletrônicos/digitais não possuírem agencias, isso possibilita a isenção ou diminuição de tarifas que um banco tradicional impõe ao seu cliente por possuir despesas maiores ao manter seus serviços de forma presencial em estruturas físicas. Mas insta salientar, que um banco digital impõe tarifas ao saque de dinheiro quando há a possibilidade.

Destarte, o crescimento desenfreado de fintech´s e bancos digitais evidenciou um ainda presente problema social de acessibilidade dessas ferramentas: A inclusão digital. Wyman (2017), define a inclusão financeira como o oferecimento e a facilitação de acesso de serviços bancários para todos os segmentos da sociedade, independendo aspectos de classe ou localidade. Frente a esse panorama, uma análise crítica do funcionamento dos bancos digitais e fintech´s se faz necessária. Ora, é incontestável que a inclusão de diversas localidades fora facilitada com o surgimento dos bancos digitais, uma vez que locais de difícil acesso ou que não possuíam agências bancárias, viram o número de correntistas crescer exponencialmente na última década, entretanto, urge expor alguns argumentos referentes ao uso e a integração que esses aplicativos proporcionam.

Outrossim, o Banco mundial realizou uma pesquisa na qual retratava os principais entraves quanto a abertura de conta bancária por brasileiros, seja ela física ou digital, e com base nessa pesquisar, podemos desenvolver problemáticas quanto a acessibilidades dessa modalidade bancária.



Fonte: Elaborado pelos autores com base no Banco Mundial, Global Findex Survey (2017 apud ABFintechs; PwC, 2018)

Percebe-se que dentre vários entraves para a abertura de conta e posterior inclusão do indivíduo no sistema bancário a questão do custo alto e de recursos suficientes se destacam como pontos principais para a segregação desse grupo. Assim, se por um lado as instituições financeiras digitais possuem taxas na maioria das vezes reduzidas em contrapartida ao sistema tradicional bancário, a falta de confiança e a ausência de documentação necessária ainda permanecem e permeiam tanto as instituições físicas quanto digitais. Para além desses aspectos, talvez o mais importante quando se discute acessibilidade dessas instituições é quanto ao conhecimento técnico mínimo para operar aplicativos bancários.

A Fintech UX COLLECTIV, responsável pelo desenvolvimento do primeiro banco digital para idosos, realizou uma pesquisa quantitativa quanto ao auxilio no uso de plataformas de pagamento por pessoas idosas, o que segue:

Assim sendo, podemos concluir que o acesso a tecnologia por parte segmentada da população ainda é feito de forma desigual, e certos segmentos da população ainda possuem dificuldade maior quando ao acesso e distribuição dessas tecnologias, revelando uma problemática que afeta o completo acesso a esse sistema bancário digital. Ademais, essa falta de acessibilidade também se reflete na solução de demandas. Ora, se a contratação é feita por via digital, podemos concluir que quaisquer dúvidas oriundas da utilização desses serviços bancários deve ser resolvida majoritariamente pela via digital, ou seja, se o consumidor deseja realizar o cancelamento da conta, a título de exemplo, deve faze-la pelo aplicativo de banco ou pelo site, sendo em pouquíssimos casos permitido que o mesmo seja feita por contato telefone ou presencialmente, tornando o consumidor escravo do uso dessas tecnologias, bem como segregado se desconhece o uso delas, desta forma dispõe Sabattine:

> A inclusão digital é uma necessidade cada vez mais urgente em uma sociedade cada vez mais conectada e dependente de tecnologia. É importante que sejam desenvolvidas políticas e iniciativas que garantam o acesso equitativo às ferramentas e recursos digitais, para que todos possam desfrutar dos benefícios da era digital e participar plenamente da vida em sociedade."(SABBATINI, 2002, p. 45)

Outro ponto essencial que reflete a problemática acima descrita, é quanto à forma como o contrato bancário realizado pelos meios digitais é feito. Se via de regra o contrato bancário é caracterizado como de adesão, podemos concluir que o mesmo é posto à disposição do consumidor com cláusulas pré-definidas e padronizadas. Outrossim, no contrato bancário digital, o contrato para abertura de conta ou aquisição de serviços é normalmente posto à

disposição uma única vez, e possui grande extensão, dificultando a leitura breve e sua interpretação. Desta forma, acabam por passar disfarçadas cláusulas importantes da própria natureza do contrato bancário digital, que são a privacidade de dados e a segurança da informação. Patrícia Peck em seu livro direito digital, aborda essa questão, assim sintetizando:

> Assim como nos contratos bancários tradicionais, os contratos bancários digitais também podem trazer malefícios aos clientes, tais como cláusulas abusivas, falta de transparência e informações claras sobre os termos do contrato, além da dificuldade em negociar e modificar suas cláusulas. Além disso, a dependência da tecnologia pode expor os clientes a riscos de segurança e privacidade, como a possibilidade de invasões de hackers e vazamento de informações pessoais e financeiras. (PINHEIRO, 2019, p.88)

Assim, podemos estabelecer um nexo entre a efetiva aplicabilidade dos contratos bancários e a transparência que eles exprimem ao consumidor. Ora, se questões importantes como o tratamento dos dados são abordadas de forma ínfima, ou se mesmo o consumidor não é convidado a se informar sobre a política de tratamento da empresa, conclui-se que a omissão é proposital, e fruto de uma cultura de aceitação, onde o consumidor é tido apenas como ser a aceitar as condições impostas, sem qualquer possibilidade de questionar, fato esse que é exposto na máxima presentes nos contratos digitais “Concordo e aceito os termos de uso e contratação”.

3 A ECONOMIA DIGITAL E O “NOVO” SISTEMA BANCÁRIO

De acordo com o que discutia Castells (1999) a concorrência globalizada se desenvolve a partir de fatores característicos que se articulam no âmbito de uma rede baseada em Tecnologia da Informação - TI. Desta forma, a capacidade tecnológica se constitui num dos principais processos que definem a forma e o resultado da concorrência. O autor no desenvolvimento de seus estudos sugere que a tecnologia é uma das principais ferramentas utilizadas para estabelecer o contexto de competição no cenário da nova economia.

Segundo Silva (2014) este cenário proposto por Castell determina que cada vez mais as organizações atuem em um contexto onde a rapidez e complexidade se referem sobretudo, às mudanças no campo das tecnologias da comunicação. Presentemente aproximadamente três bilhões de pessoas estão conectadas à Internet utilizando distintos dispositivos. São indivíduos que destinam uma parcela significativa de seu tempo online, desenvolvendo atividades de compras, comunicação, de trabalho e entretenimento por meio do acesso à internet.

Assim, as novas tecnologias de informação e comunicação quando se analisa os

conceitos, técnicas, políticas e estratégias relacionados determinam alterações importantes na estrutura competitiva local e mundial, além de transformar as formas como se financiam as atividades da economia, o funcionamento dos mercados financeiros e criar novas configurações para as organizações (SILVA, 2014).

Para Damiano (2013) em face deste novo cenário de evolução, no setor bancário, pode-se observar uma elevação dos riscos, especialmente aqueles relacionados com as fraudes nos canais tecnológicos, surgindo um contexto de ameaças e tentativas de invasão tanto da organização bancaria quanto do próprio cliente. Complementa Adachi (2004) destacando que os riscos aos quais estão expostos os bancos no mundo físico se repetem no ambiente virtual, estabelecendo um cenário de fraudes e crimes financeiros. Diante disso, a necessidade de protegeros ativos (informações) é de extremamente relevante e importante para o sucesso financeiro e sobrevivência das organizações onde qualquer falha na proteção de seus sistemas de informática podem acarretar perdas e impactos negativos para a gestão dos negócios e para a imagem da mesma perante a sociedade, causando prejuízos financeiros.

De acordo com o estudo desenvolvido por Damiano (2013) a partir daobservação desse cenário e do processo evolutivo no que tange as transações financeiras efetuadas por meio do canal eletrônico, aparece a necessidade de estruturação de meios e mecanismos de segurança com o objetivo de combater estas ameaças que podem atingir o cliente e o próprio banco. Na concepção do autor:

> A economia de escala e modelo ágil de distribuição e realizações de serviços financeiros envolvendo principalmente pagamentos e transferências que a Internet e seus usuários conectados constituem serve também para a prática de atos ilícitos (DAMIANO, 2013, p. 13).

Considera Silva (2014) que o aumento significativo dos ataques e ameaças que se espalham pela internet pode ser atrelado às suscetibilidades e falhas dos sistemas de informática ou dos próprios usuários no momento em que concretizam transações financeiras utilizando a internet. Desta forma, pode-se estabelecer a relação direta destes problemas com o gerenciamento de investimentos, contas bancárias, pagamentos de cartões de crédito ou transações realizadas por meio de comercio eletrônico, além de estar associado também ao processo contínuo de desenvolvimento de inovações tecnológicas e com a obrigação peremptória de se manter em concordância com regulamentações de múltiplos mercados. O autor destaca aqui a importância de se compreender que estes fatores emergem como elementos fundamentais para a adoção de mecanismos de segurança dainformação que promovam a correta identificação do usuário, o gerenciamento do acesso, entre outros, como indispensáveis para a efetivação de atividades em ambiente virtual.

Conforme discutem Mello; Queiroz (2006), o contexto do setor bancário, em especial, tem sido berço de amplas transformações ao redor do mundo, determinadas pelas necessidades estabelecidas pelo processo de globalização e pela redução das barreiras de regulamentação entre os mercados financeiros. Segundo os autores, pode-se associar a esses fatores as alterações provenientes dos padrões de comportamento do consumidor, o estabelecimento de um padrão de concorrência acirrado e o movimento de fusões e aquisições, que conferem novas características à competição entre os bancos.

Os autores acima citados destacam a utilização de uma linha de estratégia pelos bancos que se refere a incorporação de novas tecnologias da informação aos seus procedimentos operacionais. Segundo eles a automação bancária que teve início no interior das agências, de maneira muito rápida transpassou esse limite físico para disponibilizar serviços aos clientes utilizando uma grande rede de caixas eletrônicos, ao colocar à disposição dos mesmos equipamentos implantados em lugares de grande afluência de público, como por exemplo, centros de lazer, shoppings centers, entre outros. Desta forma, não levou muito tempo para que os serviços bancários alcançassem os níveis industriais, organizacionais e as residências de seus clientes, por meio de redes públicas de comunicação, como a *Internet*.

Assim, diante disso passa-se a discorrer sobre a utilização da internet nas transações eletrônicas e as possibilidades de fraudes no ambiente bancário.

4 A INTERNET E AS FRAUDES BANCÁRIAS

O desenvolvimento e utilização cada vez maior da Internet teve influências expressivas na mudança de uma velha economia porá o estabelecimento de uma nova ordem econômica, pautada no poder do consumidor que no seu papel de comprador passam a apresentar um poder nunca sentido anteriormente pelo mercado no que se refere a evitar produtos e serviços que não desejam, admirá-losa partir de seu gosto e comprar apenas o que lhe oferecer melhor custo-benefício conforme preconizam em seu estudo Rezabakhsh et al. (2006). Estes autores asseveram que, ainda que o consumidor atual goze de poder suplementar no desenvolvimento das relações de consumo com a utilização da Internet, devem ser ativados mecanismos governamentais, legais e corporativos visando a coibição de práticas prejudiciais nas transações concretizadas.

De acordo com o que expõe Machado (2011, p. 23) complementado oprocesso exposto.

> O mercado emergente da comunicação via Internet tem sido associado a crescentes números em função de alguns fatores: riqueza acentuada de

> informações nas transações e relações; menor custo na procura por informações dos consumidores; troca de informação assimétrica entre vendedores e compradores; proximidade espacial eletrônica entre vendedores e consumidores; tempo de compra e posse do bem adquirido nas compras digitais.

Ainda em complementação ao tema discutido, Naím (2006) acredita que as práticas fraudulentas efetivadas no contexto do comércio realizado pela Internet estão inseridos na pirataria global que assola o mercado, onde marcas são clonadas,produtos são falsificados e o processo de lavagem de dinheiro se desenvolve em escala mundial.

Segundo Fletcher (2007) somente no ano de 2004 os recursos financeiros que foram perdidos em fraudes financeiras pela Internet no país foram similares às perdas devidas a roubos de bancos. Por exemplo, na Inglaterra foram roubados aproximadamente 400 milhões de libras em 2005 do banco japonês Sumitomoutilizando a Internet e, também em 2005, um hacker extraiu informações de 40 milhões de cartões de crédito igualmente por meio da Internet.

As crescentes fraudes na Internet além de trazer muitos problemas aos usuários, têm originado uma crise de confiança nos sistemas comerciais que tem suas operações apoiadas no comércio eletrônico, o que alcança igualmente o sistema bancário. Por isso, diante da expressividade das fraudes bancárias, o referido setor se viu impelido a investir e desenvolver sistemas de segurança para seus procedimentos eletrônicos.

Para Sarma; Singh (2010), no caso específico dos serviços bancários, o Internet banking refere-se a sistemas que permitem aos clientes acessarem suas contas e obter informações gerais sobre produtos e serviços bancários através de um computador pessoal (PC) ou outros dispositivos inteligentes. Entre estes produtos bancários via Internet pode-se incluir serviços que incluem produtos por atacado para clientes corporativos, bem como produtos de varejo e fiduciários para consumidores. Em última análise, os produtos e serviços obtidos através de Internet banking podem espelhar produtos e serviços oferecidos através de outros canais de distribuição bancária. Alguns exemplos de produtos por atacado e serviços incluema gestão de dinheiro, transferência bancária, transações, contas de apresentação e de pagamento, entre outros. O exemplo de varejo são os produtos e serviçosfiduciários que incluem consulta de saldo, transferência de fundos, informaçõessobre a transação, pagamento de contas, pedidos de empréstimo, atividade de investimento e outros serviços de valor acrescentado.

5 A INTERNET E AS POSSIBLIDADES DE INVASÃO DO AMBIENTE BANCÁRIO

De acordo com o que expõe Sydow (2015) a informática é o emprego do tratamento automático das informações. Isto posto, é de se entender que é necessária uma linguagem uniforme para que o uso, a transformação e a transmissão de informações sejam amplos e difundidos de maneira global e universal. Essa ferramenta foi intensamente utilizada para o desenvolvimento dos computadores e da internet e todas as suas características e possíveis riscos.

Conforme estas ferramentas evoluem mais a tecnologia informática acaba ocupando espaço na vida da sociedade. Esta inserção se faz a partir da possiblidade de criação e armazenamento de documentos, como por exemplo, as informações bancárias são transformadas em bits e ficam disponível para consulta e utilização.

A partir disso, o desenvolvimento levou o ser humano a elaborar tecnologias e, simultaneamente, a ser capaz de detectar os riscos provenientes de tais avanços, tornando-se capaz de assumir posturas visando evitar os riscos desnecessários e decontenção de atitudes que possam interferir na elevação da quantidade mínima de riscos aceitáveis para esta evolução.

Com os avanços tecnológicos se desenvolvendo a taxas vertiginosas, como apontado por Avelino (2011), torna-se cada vez mais difícil obter-se compreensão que abranja as diversas possibilidades que o mercado apresenta aos consumidores, e por isso, acompanhar de maneira criteriosa as ameaças e vulnerabilidades que cercam o ambiente cibernético se constitui numa tarefa indispensável no contexto deevolução das inovações tecnológicas no ambiente bancário.

Estas inovações tecnológicas vêm se desenvolvendo no ambiente bancário ao longo dos anos. Segundo abordam Silva; Oliveira (2001) a inserção de tecnologiano ambiente bancário a partir do uso de computadores ocorreu na década de 1950.

Os computadores, então, eram empregados no processamento da movimentação diária das contas correntes especificamente, e no período noturno de maneira centralizada. As listagens eram disponibilizadas para as agências no período da manhã para serem usadas pelos caixas ao longo do expediente bancário, sendo queo processamento *online* em tempo real, ainda nem era cogitado.

Para Chorafas (1987) apenas na metade dos anos 1960 surge a primeira geração de computadores *online*, que significava estar conectado diretamente a um sistema. Esta fase se estendeu por aproximadamente dez anos, de 1965 a 1975, sendo que ao logo deste período, o processamento ainda era centralizado e com foco principal na movimentação de investimentos

e contas correntes.

De acordo com Oliveira (2001) destacam que a segunda geração conectada *online* também se desenvolveu por uma década, de 1975 a 1985, apresentando, contudo, diferenças básicas em relação a antecedente. Enquanto a primeira compreendia serviços de comércio exterior e transações realizadas no mercado de ações eprocessamento distribuído que se constituía numa maneira descentralizada de processamento de dados desenvolvida em computadores menores distribuídos por uma determinada região; na segunda destaca-se a importância deste período por causa da sua relação com a invenção do cartão de débito e igualmente pelo iníciode autorizações *online* em transações efetuadas no comércio.

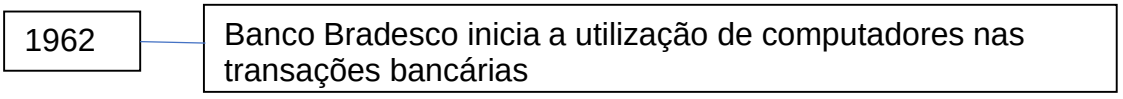
Os autores acima citados destacam que a terceira geração online se desenvolveu no período de 1985 a 1995, apresentando algumas mudanças derelevância significativa:

> **Inteligência local:** a partir do que os bancários passam a poder processar informações a partir de suas próprias mesas de trabalho, deixando para traz a necessidade de acessar um *mainframe* remotamente, que era bastante problemático;
> **Desenvolvimento e implementação de terminais online:** a partir dos quais o cliente pode se conectar efetivamente em tempo real com o banco e suprir suas necessidades bancárias;
> **Arquiteturas de rede fazendo a integração da utilização dos sistemas:** que foi desenvolvido a partir de investimentos maciços em computadores e telecomunicações.

Muitas inovações foram desenvolvidas ao longo dos anos com aplicabilidade ao contexto bancário. Em linhas gerais, esse processo evolutivo resumido pode ser visualizado na figura 1.

Segundo demonstra Nunes (2014) a Internet assumiu além das prerrogativas de ser um novo meio de comunicação, o papel de ferramenta que pode ser utilizada como instrumento de entretenimento e prestação de serviços, que trouxe consigo características capazes de atuar na redução de custos e no aumento da velocidade das operações. Diante disso, aquelas empresas que se mantiveram inseridas no mercado competitivo ao longo do processo de desenvolvimento da internet, precisaram fazer adaptações para se adequar a inserção na nova concepção de espaço, o espaço virtual, e disponibilizaram suas atividades também através da internet.

Figura 1 – Linha do tempo da automação bancária



1989	Surgimento dos terminais de saque
1990	Surgimento dos padrões gráficos nos terminais de saque
1994	Banco Bradesco inicia a disponibilização de conteúdo on line
1995	Banco do Brasil investe nas plataformas de autoatendimento
1998	Banco do Brasil adota tecnologia pioneira que permite realizar transações em tempo real. Banco do Brasil passa a pagar o acesso a internet para algunsclientes com o objetivo de fomentar os acessos aos seus serviços online. Banco Itaú implanta o uso do *homebanking*.
2000	Banco Itaú passa a disponibilizar diversos serviços via internet
2001	Banco do Brasil inicia os investimentos na tecnologia paraatendimento via celular
2003	Banco do Brasil adota um modelo de *outsorcing* nas redes de telecomunicações, multiplicando a capacidade de processamento e transmissão
2004	CEF lança projeto visando centralizar todo o sistema de lotéricasno território nacional
2005	Sistema de Informação da CEF já fazia todo o processamentodas informações geradas nas lotéricas
2006 em diante	Introdução de Internet banking e gradativa adoção da computação móvel (*mobile)* a partir da difusão dos *smartphones* e também dos *tablets* pelos bancos.

Neste contexto, as instituições bancárias também se viram obrigadas a se inserir no ambiente virtual, investindo em *sites* na Internet, adotando ferramentas como o Internet Banking para estabelecer relações com seus clientes utilizando redemundial de computadores e, desta forma, puderam reduzir custos, diminuir a superlotação de suas agencias e possibilitando mais conforto e praticidade aos seus clientes. Contudo, este cenário acabou se tornando vulnerável atraindo um grande número de indivíduos mal intencionados, que se aproveitando da ausência de informação de alguns clientes para perpetrar fraudes eletrônicas (NUNES, 2014).

De acordo com Nunes (2014) qualquer fraude implica na utilização de algumengodo visando burlar a atenção da vítima, sendo que aquele que pratica a fraude esconde informações ou as disponibiliza de maneira errada visando conduzir a possível vitima a equívoco para tirar proveito da situação que se estabelece. As origens das fraudes podem ser:

> **Interna**: Quando são perpetradas por indivíduos que apresentem algum vínculo ou estejam inseridos no interior do local que foi fraudado;
> **Externa:** Quando não existe relação entre o agente fraudador e o local que onde aconteceu a fraude. Contudo, existe a possibilidade do autor ter tido relação com a vítima anteriormente.

Para o autor supracitado, não se discute que a Internet propicia um ambiente que predispõe o cometimento de fraudes, acima de tudo porque é muito difícil a identificação do autor do delito e, em alguns casos pela falta de preparo da polícia investigativa. Além disso, os usuários que não apresentem um bom nível de conhecimento em informática ou que não tenham sido apropriadamente cientificadossobre algum procedimento na Internet, acabam sendo vítimas fáceis para os agentes fraudadores.

De acordo com Lau (2006) pode-se definir a fraude eletrônica como sendo a aplicação de qualquer golpe com a utilização dos serviços disponibilizados pela Internet, em seus mais diversos ambientes, como por exemplo, salas de bate papo, mensagens eletrônicas e sites disponíveis. De maneira adicional, o autor alude que a fraude decorre também do aliciamento de potenciais vítimas pelo fraudador com o intuito de consolidar transações fraudulentas em benefício de um indivíduo ou grupo de indivíduos envolvidas no esquema. Pode-se concluir que a fraude se define pela relação de abuso de um sistema de lucro organizacional que não resulta necessariamente em consequências legais diretas para o fraudador.

Diante dessas afirmações expostas acima, Kovach (2011) faz uma definição de fraude eletrônica como qualquer acesso feito sem a devida autorização ou efetivação de uma transação não autorizada em uma conta corrente através da Internet. Para o autor, a fraude

igualmente pode ser vista como uma ação que resulta de um conjunto de violações de controles de segurança que, em último caso, acabou resultando na realização de uma operação financeira sem autorização.

Desta forma, complementa Machado (2011, p. 22) descrevendo que:

> Fruto desse cenário, as empresas têm inserido mecanismos de segurança em seus sites e sistemas virtuais, caso do uso de diversas senhas, fases distintas de acesso a informações de caráter restrito, mensagens de advertência, acompanhamento do histórico de transações e outros procedimentos para inibir a prática de fraudes.

De acordo com Soares (2014) as fraudes bancárias que movimentam milhões de reais todo ano no país são resultado da ação de cibercriminosos e da falta de ação dos próprios usuários que não adotam orientações de segurança como atualização de antivírus, utilizar software oficial, atualização constantes no sistema operacional, entreoutros.

Conforme coloca Avelino (2011) a fraude se caracteriza pela interação direta entre pessoas, contudo, algumas modalidades com maior grau de sofisticação atacam sistemas bancários, contábeis, judiciários, etc., onde seu alvo é o usuário. Por isso o autor destaca a importância de utilizar algumas tecnologias e metodologias para utilização de alguns tipos de tecnologias e serviços como os bancários, de forma a evitar que ocorram inúmeros tipos de fraudes, porque os serviços disponibilizados pela internet devido a sua característica de rapidez deste ambiente pode-se gerar consequências muito negativas tanto para o usuário quanto para as instituições.

Dentre estas ferramentas destaca-se, segundo CERT.br (2006), criptografia, assinatura digital, Certificado digital, Ferramentas antimalware, Firewall pessoal e Filtro antispam.Outras ferramentas atuais que tem por objetivo aumentar a garantia de segurança têm sido desenvolvidas e são disponibilizadas pelos bancos em ambientecibernético. O Quadro 1 a seguir faz uma descrição sucinta de algumas dessas ferramentas cuja utilização tem sido implementada:

Quadro 1 – Ferramentas de segurança atuais utilizadas pelos bancos no Brasil.

Ferramenta	Descrição
Certificados digitais	Os certificados digitais são usados para autenticar os usuários e o próprio sistema bancário. Este tipo de autenticação depende da existência de uma infraestrutura de Chave Pública (PKI) e uma Autoridade Certificadora (AC), que representa uma terceira parte confiável, que assina os certificados atestando a sua validade.
Dispositivos One Time Password (Token)	São dispositivos comumente usados como segundo

	fator de autenticação, que pode ser solicitados emsituações específicas ou aleatórias. Este tipo de dispositivos de processamento faz uso de senhas quepodem ser utilizadas apenas uma vez.
Cartões One Time Password	Constitui um método mais barato para gerar senhas dinâmicas, fornecendo também um segundo fator de autenticação. Porém, em alguns sistemas bancários, senhas geradas por cartões OTP são reutilizadas várias vezes antes de serem descartadas, tornando este sistema vulnerável a vários outros ataques.
Proteção do navegador	Neste modelo, o sistema é protegido no nível do navegador de Internet do cliente. Com essa proteção, o usuário e seu navegador estão protegidos contra programas maliciosos conhecidos através do monitoramento da área de memória alocada pelonavegador, a fim de detectá-Ios e impedir o roubo de credenciais e captura de informações confidenciais.
Teclados virtuais	Estes dispositivos são geralmente baseados em Java e softwares baseados em criptografia, permitindo a portabilidade entre diferentes dispositivos. Atualmenteestão sendo substituídos por outros métodos mais eficientes, que exigem menos poder de processamentoe taxas de transmissão mais rápidas.
Dispositivos registrados	Este método restringe o acesso ao sistema bancário a dispositivos previamente conhecidos e registrados pelo banco. Esse tipo de técnica, chamada de impressãodigital de hardware é usada em conjunto com a identificação do usuário por meio de credenciais secretas.
CAPTCHA	*Completely Automated Public Turing test to tell Computers and Humans Apart* é um método recentemente adotado em alguns sistemas bancários, cujo objetivo é tornar ineficazes os ataques automatizados contra sessões autenticadas pelos bancos. Este método requer que o usuário real introduza informações (solicitadas pelo site) exibidas em imagens difíceis de reconhecimento e processamento por robôs automatizados (Bots).
Short Message Service (SMS)	Este método tem sido aplicado em alguns sistemas bancários para notificar os usuários sobre as transaçõesque requerem sua autorização. Ele fornece um canal de segunda autenticação para transações que se enquadram em determinadas características, enviando para o usuário um conjunto de caracteres que devem ser informados, a fim de autorizar e processar a transação através do sistema bancário online.
Identificação positiva	É um modelo em que o usuário é obrigado a introduzir algumas informações secretas apenas conhecidas por ele, a fim de identificar-se. É aplicado como um método de autenticação secundário.
Monitoramento de Transação	Mesmo que este método não seja minuciosamente analisado no presente trabalho, é atualmente aplicado em muitos sistemas bancários online, cada um deles usando diferentes técnicas. Inteligência artificial, análise de históricos de transações e outros métodos que identificam padrões de fraudes em transações processadas anteriormente estão entre as várias abordagens para a monitoração de transações.
Palavra passe	É um modelo de segurança baseado em informaçõesdetidas pelo usuário. É normalmente utilizado como um

	método de autenticação secundário em transações queenvolvem movimento de recurso financeiro.

Fonte: Damiano (2013, p. 41-42).

Conforme descrito por Silva (2014) a complexidade da segurança da informação tem sido elevada a partir da pesquisa por um algoritmo que afiance a inviolabilidade do sistema criptográfico associada às constantes mudanças tecnológicas. O desenvolvimento das inovações no campo da criptografia foi disseminada para quase a totalidade das tecnologias de informação e comunicação e, como consequência, a maioria dos setores da economia faz utilização da aplicação da criptografia e de outros mecanismos de segurança em seus sistemas inseridos no contexto virtual, em suas redes organizacionais complexas, na computação móvel, na computação em nuvem, no big data, entre outras tecnologias,corroborando a importância da segurança da informação no contexto econômico pela possibilidade de redução do risco de perda financeira e de reputação aos quais as organizações estão sujeitas por operarem no ambiente da internet e digital.

Conforme analisa Barros Filho (2010, p. 1):

> Há situações mais sofisticadas em que *hackers* conseguem invadir o sistema de bancos e realizar transferências bancárias. Em tais casos, embora haja a vantagem ilícita em prejuízo alheio, não se configura oestelionato. De fato, não há qualquer pessoa induzida em erro, já que a vantagem foi obtida, sem que houvesse qualquer contribuição do correntistaou de quem o representas-se. Por mais lesiva e socialmente danosa que seja a conduta, não existe estelionato em tais situações.

Os tipos de fraudes que mais assolam os internet bankings são, segundo CERT.br (2006) e Nunes (2014) a utilização de páginas falsas e o cavalo de troia, contudo existem outros códigos maliciosos que abrem caminho para as fraudes, conforme serão adiante pormenorizados.

5.1 PHISHING OU PHISHING/SCAM

Este tipo se constitui como uma fraude através da qual um criminoso tenta obter dados pessoais e financeiros de um usuário utilizando uma combinação de meios técnicos e engenharia social.

O phishing sucede por meio do envio de mensagens eletrônicas que procuram efetivar a fraude por meio de comunicação oficial de uma instituiçãoconhecida; buscam atrair a atenção do usuário por curiosidade, caridade ou pela possibilidade de auferir alguma vantagem financeira, entre outras formas.

5.2 PHARMING

Pharming é um tipo específico de phishing que cujo mecanismo de ação é o redirecionamento da navegação do usuário para sites falsos utilizando alterações no serviço de DNS (Domain Name System). Este redirecionamento forçado do navegador Web para uma página falsa pode ocorrer através de comprometimentodo servidor de DNS do provedor utilizado; devido a ação de códigos maliciosos que alteram o comportamento do serviço de DNS do computador e pela ação direta de invasores que possuam acesso às configurações do serviço de DNS do computador ou do modem de banda larga.

5.3 CÓDIGOS MALICIOSOS (MALWARE)

São programas desenvolvidos especificamente desenvolvidos para executar ações danosas e atividades maliciosas em um computador.

5.4 SPYWARE

É um tipo de programa desenvolvido para fazer o monitoramento das atividades de um sistema e remeter as informações recolhidas para terceiros. A conotação de fraude se estabelece quando é utilizado de forma maliciosa, das açõesrealizadas, do tipo de informação monitorada e da utilização que é feita pelo receptordos dados coletados.

5.5 VÍRUS

O vírus se constitui em um tipo de ameaça programada que surge recorrentemente na Internet que se define por ser um código de computador que adere a um programa ou arquivo com o intuito de se disseminar a partir dai para outros computadores. Os *worms*, da mesma maneira que os vírus, igualmente se copiam de um computador para outro com a diferença de se propagar sem dependerde outro programa, fazendo-o em uma velocidade tão rápida que obstrui as redes e interfere no funcionamento do computador (GUEDES, 2009).

Estes programas invasores agem de maneira independente, consumindo os recursos do computador e acessando todos os arquivos do mesmo, tornando viávelo acesso ilegítimo às informações pessoais da vítima.

5.6 CAVALO DE TROIA (TROJAN)

O cavalo de troia, também conhecido como trojan ou *trojan-horse* é um programa que executa as funções para as quais foi aparentemente projetado, mas também executa outras funções, geralmente maliciosas e sem a anuência do usuário.

5.7 SPAM

O *spam* trata-se do envio de mensagem eletrônica sem a solicitação do usuário, cuja procedência é de remetente desconhecido. Estas mensagens eletrônicas podem apresentar conteúdo malicioso, como por exemplo, o *site* falso de uma instituição financeira, fazendo com que o usuário possa acreditar que se trata de um *site* real e por isso dispor seus dados pessoais e sua senha bancária nos locais solicitados, sem idealizar que estas informações estão sendo gravadas e remetidas prontamente a um fraudador (GUEDES, 2009).

6 O AGRAVAMENTO DA VULNERABILIDADE DO CONSUMIDOR NA ECONOMIA DE PLATAFORMA DAS INSTITUIÇÕES FINANCEIRAS

Azevedo (2012) coloca que o cliente bancário é o alvo principal das fraudes eletrônicas que infectam o computador utilizando uma ferramenta maliciosa ou a indução da própria vítima a partir de uma mensagem fraudulenta que tem como objetivo de repassar as informações para o agente fraudador. As principais tentativas de fraude concretizadas sobre clientes do sistema financeiro e usuários do ambiente Internet no país se baseiam principalmente em ataques *pishing scam* e *pharming* já conceituados anteriormente neste estudo.

Dito isto, podemos concluir que a vulnerabilidade do consumidor nessas economias de plataforma e instituições financeiras vai além da mera exposição a fraudes bancárias. Em uma análise mais aprofundada, podemos estabelecer dois pontos importantes que permitem que essas fraudes aconteçam: A inobservância por parte do banco, da execução correta e assertiva de procedimentos de segurança e a vulnerabilidade do consumidor, seja no âmbito informacional, que o permite repassar informações privadas a terceiros, seja no âmbito tecnológico, que por falhas ou desconhecimento permitem a ação de criminosos.

No tocante a inobservância, é clara a existência de responsabilidade bancária, fato esse já consagrado pela doutrina e pela jurisprudência jurídica, tal qual exemplifica o seguinte acordão do tribunal de justiça de São Paulo:

OBJETIVA DA INSTITUIÇÃO FINANCEIRA. ATO ILÍCITO CONFIGURADO. NEGATIVAÇÃO INDEVIDA. DANOS MORAIS IN RE IPSA. APELO AO QUAL SE NEGA PROVIMENTO. SENTENÇA MANTIDA. DECISÃO UNÂNIME. 1. A instituição financeira não se desincumbiu do ônus que lhe incumbia no sentido de demonstrar ter havido relação jurídica entre o demandante e o banco requerido, não tendo sequer trazido aos autos cópia dos supostos negócios firmados entre o autor e a instituição financeira demandada. 2. Ademais, nos termos do artigo 14, § 3°, II do Código de Defesa do Consumidor, apenas a culpa exclusiva de terceiro poderia isentar a responsabilidade do banco réu pelos defeitos na prestação do serviço, considerando que nos termos da Súmula 479 do STJ o banco responde objetivamente por danos causados aos seus clientes. Precedentes desta 2ª Câmara Extraordinária Cível. 3. Sob estes fundamentos, resta patente a conduta ilícita desenvolvida pela instituição apelante, sendo medida que se impõem o estabelecimento da prestação reparatória. 4. Ressalte-se que o dano moral sofrido em virtude de indevida negativação do nome independe de comprovação, operando, portanto, in re ipsa. 5. Dano moral mantido em R$ 10.000,00.

PROCESSUAL CIVIL. AÇÃO DECLARATÓRIA DE INEXISTÊNCIA DE DÍVIDA DECORRENTE DE FRAUDE C/C INDENIZAÇÃO POR DANOS MORAIS. PROCEDÊNCIA. APELO. TRANSAÇÕES BANCÁRIAS NÃO FIRMADAS PELO AUTOR COM O BANCO DEMANDADO. ATUAÇÃO DE FALSÁRIOS. RESPONSABILIDADE OBJETIVA DA INSTITUIÇÃO FINANCEIRA. ATO ILÍCITO CONFIGURADO. NEGATIVAÇÃO INDEVIDA. DANOS MORAIS IN RE IPSA. APELO AO QUAL SE NEGA PROVIMENTO. SENTENÇA MANTIDA. DECISÃO UNÂNIME. 1. A instituição financeira não se desincumbiu do ônus que lhe incumbia no sentido de demonstrar ter havido relação jurídica entre o demandante e o banco requerido, não tendo sequer trazido aos autos cópia dos supostos negócios firmados entre o autor e a instituição financeira demandada. 2. Ademais, nos termos do artigo 14, § 3°, II do Código de Defesa do Consumidor, apenas a culpa exclusiva de terceiro poderia isentar a responsabilidade do banco réu pelos defeitos na prestação do serviço, considerando que nos termos da Súmula 479 do STJ o banco responde objetivamente por danos causados aos seus clientes. Precedentes desta 2ª Câmara Extraordinária Cível. 3. Sob estes fundamentos, resta patente a conduta ilícita desenvolvida pela instituição apelante, sendo medida que se impõem o estabelecimento da prestação reparatória. 4. Ressalte-se que o dano moral sofrido em virtude de indevida negativação do nome independe de comprovação, operando, portanto, in re ipsa. 5. Dano moral mantido em R$ 10.000,00. (TJ-PE – Apelação cível – Relator: Des. Jovaldo Nunes Gomes – Data da publicação: 12/02/2020)

Nesse sentido, a decisão acima citada reafirma a responsabilidade dos bancos em casos de fraudes, sendo que no caso em questão, houve a adoção de falsa identidade pelos criminosos, que visando causar dano a vítima, contrataram serviço de crédito no banco demandado. Ademais, como referenciado na súmula, já esse sentimento já é consolidado pelo STJ, em sua súmula 479, que trata da responsabilização bancária em caso de danos causados a seus clientes.

Desta forma, devemos abordar o segundo e importante ponto que permite que fraudes bancárias se tornem mais comum, que é a vulnerabilidade do consumidor no meio digital. Assim disciplina, nesse sentido, Claudia Lima marques (2017, p. 02):

> Já a vulnerabilidade jurídica ou científica é falta de conhecimentos jurídicos específicos, conhecimentos de contabilidade ou de economia. Esta vulnerabilidade, no sistema do Código de Defesa do Consumidor, é presumida para o consumidor não profissional e para o consumidor pessoa física. Quanto aos profissionais e às pessoas jurídicas vale a presunção em contrário, isto é, devem possuir conhecimentos jurídicos mínimos e sobre a economia para poderem exercer a profissão, ou devem poder consultar advogados e profissionais especializados antes de obrigar-se.

Assim, podemos estabelecer sobre a ótica da autora a carência do consumidor enquanto pessoa física, de informação. Não podemos destoar ao afirmar que sim, grande parte das fraudes bancárias em meios digitais são facilitadas pelo próprio consumidor, em especial consumidores que não possuem familiaridade com o uso da tecnologia. Entretanto, podemos estabelecer um nexo direto entre a conduta do consumidor e a responsabilidade das instituições financeiras em promover ações que visem coibir essa prática, ou mesmo dar segurança ao consumidor. Aliado a isso podemos acrescentar a carência de educação financeira por parte do consumidor brasileiro, que permitem que fraudes como essa se perpetuem.

Outrossim, não podemos descaracterizar a responsabilidade de bancos e entidades financeiras nessas questões, uma vez que as principais fraudes já apresentadas se dão por ausência de políticas públicas direcionadas ao consumidor, parte essencialmente hipossuficiente da relação de consumo. Ora, se é direito assegurado do consumidor poder usufruir de um sistema bancário eficiente, em especial quando tratamos de novas tecnologias, para que as mesmas possam servir a um proposito social, como disciplina Ferrarini (2021, p. 3):

> A inclusão financeira acontece, de fato, quando as pessoas passam a usar a instituição financeira e, consequentemente, os serviços por ela ofertados, a favor de sua qualidade de vida.

Desta forma, podemos concluir que a superação dos elementos de vulnerabilidade não perpassa apenas pela concessão de "informação" ao consumidor. Ela passa pela inclusão do mesmo no sistema bancário digital, uma vez que a "digitalização dos bancos" ainda é um fenômeno recente e pouco acessível a grande maioria dos brasileiros. Assim, podemos caracterizar como fato superador dessa vulnerabilidade a acessibilidade, que deve abranger de modo significativo os consumidores, seja por políticas públicas, seja pela atuação do setor privado.

7 CONSIDERAÇÕES FINAIS

Ao finalizar este estudo pode-se observar que a inclusão das novas tecnologias da comunicação, especialmente nos serviços consolidados no campo da Internet, as relações comerciais passaram a adotar novas configurações visando atender as demandas especificas, como no caso do contexto mercadológico que abrange as instituições bancárias e seu relacionamento com seus clientes

Desta forma, a integração das inovações em tecnologia com os diversos ambientes econômicos trouxe uma realidade que mudou o desenvolvimento destes setores. Assim, as organizações, incluindo-se aqui as instituições bancárias, visualizaram a importância de integrar as novas tecnologias e passaram a fazer uso frequente das mesmas para atender os diversos contextos de seus negócios. Por isso as instituições bancárias passaram a visualizar na Internet uma realidade que tinha potencial de incrementar seus negócios e projetar de maneira positiva sua imagem em um mercado de grande competição. Esta constatação encontrou respaldo no referencial teórico analisado e que trouxe a confirmação de que a relação desenvolvida entre os bancos e seus usuários mostra que o processo de comunicação que os bancos e seus consumidores protagonizaram foi permeado pelas inovações tecnológicas que o setor tem adotado, cujo desenvolvimento foi respaldado e paralelo ao desenvolvimento econômico brasileiro.

É indiscutível que a inovação das tecnologias da informação desenvolveu novos mecanismos que propiciaram uma maior interação entre banco e cliente, como o caso especifico do Internet Banking, que trouxe como benefícios a diminuição dos custos bancários, a redução da superlotação das agências, entre outras coisas. Contudo, a vulnerabilidade desse contexto propiciou o aumento considerável do número de fraudes bancárias, que surgiram devido a falhas do sistema eletrônico ou pela falta de informação de segurança dos clientes no que diz respeito a adoção de medidas de proteção ao utilizar a rede.

Os bancos sempre foram de encontro às necessidades de seus clientes, o que

demanda que estas instituições desenvolvam novos serviços e produtos que apresentem diferenciais competitivos aliados a elevado grau de inovações em suas operações. Por isso, acredita-se que o número de transações bancárias que édisponibiliza os clientes do Internet banking tem aumentado. Contudo, mesmo em face da diversidade de transações oferecidas por meio do canal virtual e os consequentes investimentos realizados em segurança, as fraudes bancárias têm feito com que as instituições bancárias repensem seus procedimentos em termos de inovação buscando ferramentas tecnológicas que devolvam ao usuário a segurança de utilizar estes serviços pela internet.

Outrossim, a vulnerabilidade do consumidor, por outro lado, ainda se mantém presente, uma vez que a desigualdade no acesso a informação e a dificuldade do consumidor se proteger de fraudes ainda é uma realidade, e uma vez posto o código de defesa do consumidor em debate, ainda se percebe a ausência de politicas públicas por parte de entidades governamentais para a solução do problema, enquanto que as instituições bancárias, apesar de investir massivamente em segurança digital, ainda pecam em fornecer tratamento adequado ao que dispõe a lei, uma vez que em muitos casos negligenciam a hipossuficiência do consumidor, não promovendo uma relação harmónica de consumo, como dispõe o código.

Ademais, percebe-se que é consolidada jurisprudência e doutrina no tocante a responsabilidade desses entes quanto a fraudes, sejam de carater interno quanto externo, uma vez provada a responsabilidade do banco na eventual fraude.

Por fim, percebe-se que a Internet ainda é utilizada apenas como um canal adicional de vendas. Para ampliar a sua utilização, aperfeiçoando a qualidade de seus serviços, os bancos deverão trabalhar e divulgar as iniciativas e processos inseridos visando aumentar a segurança do meio transacional e promover uma ampla inclusão, desta forma melhorando a acessibilidade e combatendo fraudes.

REFERÊNCIAS

ADACHI, Tomi. Gestão de segurança em internet banking: estudo de casos brasileiros. Dissertação de Mestrado em Administração de Empresas. São Paulo: Fundação Getulio Vargas, 2004.

AVELINO, Daniel Angelo. **Fraudes eletrônicas em bancos brasileiros e a proteção dos clientes através da conformidade**. Monografia de Especialização. Belo Horizonte: Belo Horizonte, 2011.

AZEVEDO, Carlos Eduardo Mendes de. **Aspectos de responsabilidade civil em fraudes eletrônicas no Internet Banking**. Artigo de Conclusão de Curso. Rio de Janeiro: Escola de agistratura do Estado do Rio de Janeiro, 2012.

BARROS FILHO, José Nabuco Galvão. Algumas observações sobre o estelionato. Aquestão da pessoa induzida em erro. **Jus Navigandi**. Teresina, n. 2644, set. 2010.

BASTOS, Paulo Sérgio Siqueira; PEREIRA, Roberto Miguel. Fraudes eletrônicas: o que há de novo? **Revista de Contabilidade do Mestrado em Ciências Contábeis da UERJ**. Rio de Janeiro, v.12, n. 2, p. 1, mai./ago. 2007.

BERNARDES, Roberto; BESSA, Vagner e KALUP, André. A economia da inovação no setor de serviços: desvendando o cenário brasileiro. **São Paulo em Perspectiva**, v. 19, n. 2, p. 115-134, abr./jun./2005.

BOCCHINI, Bruno. **Fraudes eletrônicas ocorrem principalmente pelocomportamento dos clientes**. (2012) Disponível em: http://www.ebc.com.br/2012/1 1/fraudes-eletronicas-bancarias-ocorrem-principalmente-pelo-comportamento-dos- clientes. Acesso feito em set./2014.

CAMPANARIO, Milton de Abreu. **Tecnologia, Inovação e Sociedade**. VI Módulode la Cátedra CTS I. Colombia, set./2002.

CASTELLS, Manuel. **A sociedade em rede**. A era da informação: economia,sociedade e cultura. 2. ed. São Paulo: Paz e Terra, 1999.

CERT.br - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. **Cartilha de Segurança para Internet 3.1**. Disponível em: http://cartilha.cert.br/sobre/old/cartilha_seguranca_3.1.pdf. Acesso feito em set./2014.

CHANG, Joshua J.S. An analysis of advance fee fraud on the Internet. **Journal of Financial Crime**, v. 15, n. 1, p. 71-81, 2008.

CHORAFAS, Dimitris N. Strategic Planning For Electronic Banking. London: Butterworths & Co. Ltd, 1987.

CONDE, Mariza Velloso Fernandez e JORGE, Tania Cremonini de Araujo. Modelose concepções de inovação: a transição de paradigmas, a reforma da C&T brasileira e as concepções de gestores de uma instituição pública de pesquisa emsaúde. **Ciênc. saúde**

coletiva, v. 8, n. 3, p. 727-741, 2003.

CARLOTO, Leandro. **Breve comentário histórico sobre a segurança da InternetBanking no Brasil**. Disponível em: http://leandrocarloto.jusbrasil.com.br/artigos/111 941203/breve-comentario-historico-sobre-a-seguranca-da-internet-banking-no-brasil?ref=home. Acesso em: 28 mai. 2023.

COSTA, Sergio Francisco. **Método científico**: os caminhos da investigação. SãoPaulo: Editor Harbra. 2001.

DAMIANO, Andre Luis. **As fraudes no internet banking e sua evolução para o social banking**. Dissertação de Mestrado. São Carlos: Escola de Economia da Universidade de São Paulo, 2013.

DEMO, Pedro. **Introdução à metodologia da ciência**. 2 ed. São Paulo: Atlas, 1987.

DEZA, Xavier Vence. Economía de la Innovación y del cambio tecnológico. México: Silgo Veintiuno Editores S/A, 1995.

FEBRABAN. A sociedade conectada - Setor Bancário em Números, Tendências Tecnológicas e Agenda Atual. CIAB FEBRABAN 2012

GARCIA, Eduardo Alfonso Cadavid. **Manual de sistematização e normalização de documentos técnicos.** São Paulo: Atlas, 1998.

GARTNER, Susan Moore. **Gartner Says Worldwide Information Security Spending Will Grow Almost 8 Percent in 2014 as Organizations Become More Threat-Aware**. (2014) Disponível em: http://www.gartner.com/newsroom/id/2828722.Acesso feito em set./2015.

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa.** 4. ed. São Paulo: Atlas,2002.

GONSALVES, Elisa Pereira. **Conversando sobre iniciação a pesquisa científica**.3 ed. Campinas, SP: Editora Alínea, 2003.

GUEDES, Edmárcio Cerqueira. **Fraudes no *Internet Banking*:** Conceituação eEstado Atual dos Mecanismos de Defesa. Monografia de Graduação em Informática com ênfase em Gestão de Negócios. São Paulo: Faculdade de Tecnologia da Zona Leste, São Paulo, 2009.

KOVACH, Stephan. **Detecção de fraudes em transações financeiras via internet em tempo real**. Tese de Doutorado em Engenharia Elétrica. São Paulo: Escola Politecnica da Universidade de São Paulo, 2011.

FERRARINI, LETICIA. Inclusão Financeira Em Tempos De Fintech. Percurso, [S.l.], v. 3, n. 40, p. 66 - 70, dez. 2021. ISSN 2316-7521.

LAKATOS, Eva Maria; MARCONI, Marina de Andrade. **Técnicas de pesquisa**. 5 ed. São Paulo: Atlas, 2002.

LAR, Saleem-Ullah; LIAO, Xiaofeng; REHMAN, Aqeel ur; MA, Qinglu. **Proactive Security Mechanism and Desing for Firewall**. International Journal of Information Security. 2011.

LAU, Marcelo. **Análise das fraudes aplicadas sobre a ambiente internet banking**. Dissertação de Mestrado. São Paulo: Escola Politécnica da Universidade de São Paulo, 2006.

MACHADO, Antonio Carlos. **Comunicação para prevenção de danos ao consumidor com o uso da internet**. Dissertação de Mestrado. São Caetano do Sul: Universidade Municipal de São Caetano do Sul, 2011.

MELLO, Roberto Agostinho de; STAL, Eva; QUEIROZ, Ana Carolina S. O Banco na Internet: Inovações em Tecnologia da Informação Moldam Novos Serviços Bancários.**30º Encontro da ANPAD**. Salvador, set. 2006.

RAMON, Miguel. **Fraudes eletrônicas**. (2008) Disponível em: http://slideplayer.com. br/slide/293331/#. Acesso feito em set./2014.

RAUEN, Fábio José. **Elementos de iniciação à pesquisa.** Rio do Sul: Nova Era,1999.

REZABAKHSH, Behrang; BORNEMANN, Daniel; HANSEN, Ursula; SCHRADER, Ulf. Consumer Power: A Comparison of the Old Economy and the Internet Economy. **Journal of Consumer Policy**, n. 29, p. 3-36, 2006.

SIQUEIRA, Andressa. Banco digital: qual é o melhor? Conheça os principais e saiba o que eles oferecem. **Blog Magnetis**. Disponível em: https://blog.magnetis.com.br/bancos-digitais/#:~:text=Um%20banco%20digital%20%C3%A9%20uma,resolvidas%20pelo%20computador%20ou%20aplicativos. Acesso em: 28 mai. 2023.

TORRES, Thalita. Banco digital para todos – estudo do caso de UX. **UX Collective BR**, 2019. Disponível em: https://brasil.uxdesign.cc/banco-digital-para-idosos-bbbda9dc423a. Acesso em: 28 mai. 2023.

Brasil fracassa em ranking global de educação digital em cibersegurança, 26 nov. 2020. **Associação Brasileira de Internet.** Disponível em: https://www.abranet.org.br/Noticias/Brasil-fracassa-em-ranking-global-de-educacao-digital-em-ciberseguranca-3183.html?UserActiveTemplate=site&UserActiveTemplate=mobile#.ZGaLmezMKW0

O que é fintech e por que esse termo ficou tão popular? **Redação Nubank,** 2020. Disponível em: https://blog.nubank.com.br/fintech-o-que-e/. Acesso em: 28, mai. 2023.