Fundação Educacional do Município de Assis
Instituto Municipal de Ensino Superior de Assis
Campus "José Santilli Sobrinho"

RAFAEL ELIAS DINIZ

RESPONSABILIDADE DAS INSTITUIÇÕES BANCÁRIAS PERANTE OS DANOS CAUSADOS POR ATAQUES CIBERNÉTICOS

Assis/SP
2021

Fundação Educacional do Município de Assis
Instituto Municipal de Ensino Superior de Assis
Campus "José Santilli Sobrinho"

RAFAEL ELIAS DINIZ

RESPONSABILIDADE DAS INSTITUIÇÕES BANCÁRIAS PERANTE OS DANOS CAUSADOS POR ATAQUES CIBERNÉTICOS

Projeto de pesquisa apresentado ao curso de Direito do Instituto Municipal de Ensino Superior de Assis – IMESA e a Fundação Educacional do Município de Assis – FEMA, como requisito parcial à obtenção do Certificado de Conclusão.

Orientando (a): Rafael Elias Diniz
Orientador (a): Jesualdo de Almeida Junior

Assis/SP
2021

FICHA CATALOGRÁFICA

D585c DINIZ, Rafael Elias
Responsabilidade das instituições bancárias perante os danos causados por ataques cibernéticos / Rafael Elias Diniz. – Assis, 2021.

39p.

Trabalho de conclusão do curso (Direito). – Fundação Educacional do Município de Assis-FEMA

Orientador: Dr. Jesualdo Eduardo de Almeida Júnior

1.Cyber-crimes 2.Crimes bancários 3.Crimes digitais

CDD 341.55251

RESPONSABILIDADE DAS INSTITUIÇÕES BANCÁRIAS PERANTE OS DANOS CAUSADOS POR ATAQUES CIBERNÉTICOS

RAFAEL ELIAS DINIZ

Trabalho de Conclusão de Curso apresentado ao Instituto Municipal de Ensino Superior de Assis,como requisito do Curso de Graduação de Direito, avaliado pela seguinte comissão examinadora:

Orientador: _____
Jesualdo Eduardo de Almeida Junior

Examinador: _____
Inserir aqui o nome do examinador

Assis/SP
2021

DEDICATÓRIA

Dedico este trabalho a minha família, amigos e aos amantesdo assunto.

AGRADECIMENTOS

Primeiramente agradeço a Deus por ter me guiado ao longo dessa caminhada, me dando fé e forças para continuar, ainda mais nesses dois últimos anos totalmente atípicos.

Aos professores e funcionários da FEMA – Fundação Educacional do Município de Assis, por todos os anos de muitas lições e aprendizados, no qual foi um imenso prazer ser aluno da Instituição.

Ao meu orientador mestre e professor de Direito Dr. Jesualdo, um exímio profissional e conhecedor de todas as áreas do direito. Imensamente agradecido por toda dedicação, conselhos e paciência para que pudesse concluir este trabalho monográfico.

Finalmente, gostaria de agradecer minha namorada, meus amigos e familiares, especialmente meus pais, os quais lutaram e me apoiaram imensamente para que pudesse continuar nesse curso, dando seguimento neste sonho.

Obrigado a todos por fazerem parte deste momento ímpar em minha vida.

RESUMO

O presente estudo e trabalho monográfico trata-se de atos e responsabilidades das Instituições Bancárias após sofrerem ataques cibernéticos, mostrando a evolução do cyber-crime e abordando o atual tratamento do judiciário e seus âmbitos. Destacando também, as responsabilidades perante o Novo Código Civil e por meio do Código de Defesa do Consumidor ao observar a crescente evolução dos crimes digitais que, recentemente, está atacando de forma assídua clientes e instituições bancárias.

Palavras-chave: Código Civil; Código de Defesa do Consumidor; crimes digitais; cyber-crime; crime bancário.

ABSTRACT

The present study and monographic work is about with the acts and responsibilities of Banking Institutions after suffering from cyber attacks, showing the evolution of cybercrime and addressing the current treatment of the judiciary and its areas. Also highlighting the responsibilities under the New Civil Code and through the Consumer Defense Code by observing the growing evolution of digital crimes that, recently, is assiduously attacking clients and banking institutions.

Keywords: Civil Code; Consumer Protection Code; digital crimes; cyber-crime; banking.

LISTA DE ABREVIATURAS E SIGLAS

CC	CÓDIGO CIVIL
CP	CÓDIGO PENAL
STJ	SUPERIOR TRIBUNAL DE JUSTIÇA
CDC	CÓDIGO DE DEFESA DO CONSUMIDOR
ART.	ARTIGO
PG.	PÁGINA
WWW	WORLD WIDE WEB

SUMÁRIO

1. INTRODUÇÃO

O presente trabalho monográfico tem como finalidade abordar sobre os crimes cibernéticos através da internet, cometido contra instituições bancárias e seus clientes, baseando-se nas lógicas das doutrinas e de como a legislação irá tratar tais crimes que estão em crescente no Brasil.

É evidente que estamos na era digital e da tecnologia, e com todo esse avanço, a sociedade deve se adequar a essas mudanças que causam enormes impactos, resultando em uma grande revolução.

Por conseguinte, o advento da internet proporcionou facilidade na vida de quem a usa, fazendo parte do cotidiano das pessoas e diminuindo frontes, devido a sua facilidade de acesso e correspondendo a diversas demandas. Nesse sentido, atividades corriqueiras e econômicas, ou seja, transações por intermédio bancário através de aplicativos de serviços e pagamentos e o próprio *internet banking* se tornaram frequentes, e assim, mantiveram as relações de compras e vendas.

A respeito do direito, há uma busca constante em se adequar a essas situações, tendo em vista que as relações jurídicas criadas na internet se tornaram muito comuns e seria de extrema necessidade acompanhar esse desenvolvimento sem deixas e lacunas jurídicas, tanto nas esferas penais, cíveis, e correspondente ao direito do consumidor.

No primeiro capítulo, estudaremos o impacto das inovações tecnológicas na prática dos crimes, abordando o conceito e história dos crimes cibernéticos e quando ganhou reais evidências no judiciário brasileiro, além de alguns métodos que ajudaram na popularização e prática dos *cyber-crimes* e sua evolução.

Já no segundo capítulo, trataremos da ligação entre os bancos e clientes junto à tecnologia, abordando a fraude bancária na internet (artigo 171), onde serão discutidos alguns métodos e mecanismos que os criminosos usam para praticar os golpes, clonagem de cartões e whatsapp e alguns métodos de segurança que clientes e bancos devem utilizar para não caírem em tais golpes.

Por fim, no terceiro capítulo, serão analisadas quais leis e responsabilidades no âmbito jurídico que cuidam desses crimes, quem será punido e quem será indenizado. Sendo assim, o foco e a base estarão no código do consumidor e no código civil, uma vez que tratam das responsabilidades de bancos e clientes, e sobre a atualização das legislações brasileiras perante os crimes cibernéticos.

2. CAPÍTULO 1: IMPACTO DAS INOVAÇÕES TECNOLÓGICAS NA PRÁTICA DO CRIME

As inovações tecnológicas da última década revolucionaram a forma como interagimos com o mundo, e com elas, as práticas criminosas também avançaram no tempo, causando grandes imprevistos, assim como chamados crimes digitais ou *cyber-crimes*. Nesse ínterim, pessoas de todas as classes possuem a acesso a internet, e esse acesso, combinado ao conhecimento de alguns ‘’gênios do mal’’, somam diversos crimes na modalidade digital, os quais se tornaram ainda mais comuns em vários tipos e formas.

Parte-se do pressuposto histórico de invasões feitas por falhas de sistema nos anos 80 e 90 com o início da internet, se arrastando até a atualidade, onde o crime tornou-se um dos mais praticados, devido ao criminoso estar fazendo isso de sua própria casa ou com computadores interligados, caso aja conjuntamente a uma organização.

Sendo assim, os crimes ainda são encarados como algo muito novo para o judiciário no Brasil, portanto, as leis para estas infrações começaram a ser criadas e evidenciadas somente nos últimos anos, salientado-se o artigo 154-A e a Lei 12.737/2012, que são de grande importância no que se refere ao combate de crimes pelainternet. No entanto, não são os únicos artigos paras os crimes cibernéticos em geral.

2.1 CONCEITO E HISTÓRIA DO CRIME CIBERNÉTICO

Ao falar sobre crimes digitais, é de grande importância salientar onde ele selocaliza na legalidade formal no Código Penal Brasileiro (CP BRASIL, 1940). Assim, destaca-se o artigo 154 - A Invasão de dispositivo informático:

> Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita”. Possuindo pena detenção, de 3 (três) meses a 1 (um) ano, e multa podendo ser aumentada de um sexto a um terço caso resulte em prejuízos financeiros.
>
> Caso a invasão tenha resultado em obtenção impropria de conteúdo de comunicação privada e informações sigilosas a pena pode ser de reclusão de 6 (seis) meses a 2 (dois) anos e multa, podendo ser aumentada de um a dois terços se possuir venda ou divulgação a terceiro.
>
> Também podendo ser aumentada de um terço até metade se o crime for praticado contra entes do governo.

Tal lei foi impulsionada devido a grande evidência criada após os vazamentos de

fotos da atriz Carolina Dieckmann, após seu computador ter sido invadido por um criminoso. Nesse sentido, a criação da Lei 12.737/2012 representa uma atenção e um melhor tratamento nas questões de crimes cibernéticos no Brasil.

Enquanto a elaboração deste trabalho monográfico, a lei atualizou-se para 14.155/2021 no dia 27 de maio, visando coibir os crimes pelos meios eletrônicos, onde o legislador resolveu punir de maneira mais severa o crime de invasão de dispositivo móvel pertencente ao artigo 154 – A, a pena foi aumentada de um ano para quatro anos e a competência julgadora era Jecrim e agora passando a ser julgada pelo Tribunal deJustiça.

Mediante o crime de estelionato, o artigo 171 do Código Penal Brasileiro (CP BRASIL, 1940) notou mudanças em sua forma de punir:

> § 2º-A. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo.
>
> § 2º-B. A pena prevista no § 2º-A deste artigo, considerada a relevância do resultado gravoso, aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional.

Houve também a mudança na competência, visto que a consumação passa a ser onde a vítima mora ou estava, logo, o domicílio da vítima.

Deve-se levar em conta que os crimes cibernéticos foram reconhecidos e englobados pelo artigo 154 A do CP. Porém, existindo outros fundamentos legais para crimes que também são possíveis na modalidade cibernética como, por exemplo: aliciamento de crianças (241 D do ECA), ameaça (artigo 147 CP), *cyberbullyng* (138, 139 e 140 do CP), fraude bancária (171 do CP), entre outros crimes a frente citados.

Sobre Crimes Cibernéticos, Emerson Went e Higor Vinicius Nogueira Jorge, autores do livro “Crimes Cibernéticos” (2013) destacam:

> Define-se crimes cibernéticos aqueles cometidos por intermédio de computador ou rede de internet, dividindo-se entre crimes cibernéticos abertos e crimes exclusivamente cibernéticos.
> Os crimes cibernéticos abertos são aqueles que podem ser praticados de forma tradicional ou por intermédio de computadores, que significa que os computadores são apenas um meio para a prática do crime, no qual também poderia ser cometido sem o uso dele.
> Já os crimes exclusivamente cibernéticos são aqueles que podem ser utilizados por intermédio de computadores e também outros recursos tecnológicos quepossuem acesso à internet.

O critério usado para conceituar crimes cibernéticos muda conforme a situação e o autor. Sendo assim, para Damásio (2003), eles são divididos em crimes cibernéticos puros e impuros:

> Crimes eletrônicos puros ou próprios são aqueles que sejam praticados por computador e se realizem ou se consumem também em meio eletrônico. Neles, a informática (segurança dos sistemas, titularidade das informações e integridade de dados, da máquina e periféricos) é o objeto jurídico tutelado.
> [...] Já os crimes eletrônicos impuros ou impróprios são aqueles em que o agente se vale do computador como meio para produzir resultado naturalístico, que ofenda o mundo físico ou o espaço real, ameaçando ou lesando outros bens não computacionais ou diversos da informática.

Quanto ao resultado e consumação, Gabriel Cesar Zaccaria de Inellas (2009) descreve que “os crimes devem ser considerados crimes formais (no qual a intenção do agente é presumida de seu próprio ato que considera-se consumado independentemente do resultado).”

Já para Maria Helena Junqueira Reis (1997), “crimes cibernéticos são crimes materiais, que nada mais são do que crimes naturalísticos, sendo necessário ocorrer um resultado para então ter sua consumação.”

No aspecto de execução do crime, Tulio Lima Vianna (2001), ressalva que “esses criminosos desenvolvem aplicativos e vírus *malware,* que são nada mais que códigos de cunho malicioso com intuito de causar danos, alterações e roubo de dados, sendo apenas um começo para o declínio.”

Acerca de seu aspecto histórico, o termo *Cyber-crime,* vindo do dicionário inglês, “é o uso ilegal de computadores e internet”. Outra definição de *cyber-crime* é: crime cometido por meio de computadores ou a internet, criado em meados dos anos 90, junto a uma reunião do SUB8 que contava com os países mais ricos do mundo, juntamente coma Rússia, devida a sua imponência política e militar na época. Neste evento foramdiscutidas as maneiras de combater e conter as práticas ilegais na internet e como parar *Crackers*, invasores de sistema, estelionatários virtuais da então data. No entanto, os crimes virtuais acabaram crescendo de maneira astronômica e também evoluíram em suas formas e práticas.

É interessante mencionar a Convenção de Budapeste, efetivada em 23/11/2001, na qual seu tema foi *cyber-crimes*. A discussão realizada também pelo Conselho Europeu, teve como membros vários países incluindo a União Europeia. Nessa convenção, foram

discutidos tratados em âmbitos penal e processual penal e as resoluções de crimes cibernéticos ao redor do mundo, as quais o Brasil demorou a acatar e ainda estuda essa possibilidade de se juntar aos demais países ao combate contra os *cyber*-criminosos. (MIGALHAS, 2020)

Baseando-se em dados atuais, durante o isolamento social da pandemia da Covid-19, os crimes cibernéticos cresceram cerca de 50%, sendo um dos crimes mais praticados durante a pandemia.

‘’O balanço também mostra que no primeiro semestre de 2020, no ápice do isolamento social, o número de crimes virtuais cresceu 50% na comparação com omesmo período do ano anterior” (JORNAL JURID, 2021).

2.2 POPULARIZAÇÃO: DEEP WEB

Os crimes cibernéticos deram início na *surface*, conhecida como a internet com os mecanismos de busca como *Google*, *duckduckgo*, *Bing*, sendo possível a tentativa de inúmeros golpes, mas acabou evoluindo e se popularizando na *deep web,* que em sua tradução livre significa ‘’internet profunda’’. Nesse ínterim, a grosso modo, pode ser encarada como a internet sem lei, onde nada é rastreado com facilidade, isto é, um local sem a presença de governo.

É interessante reforçar que na *Deep Weeb não existem URL* como, por exemplo ‘’globo.com’’, e sim, *links* todos bagunçados e codificados para que seja mais difícil ser encontrado o site na rede.

‘’A *Surface Web* ou Internet superficial é a parte do *World Wide Web* (WWW) indexada pelos motores de busca. A parte que não é indexada chama-se *Deep Web*. Motores de busca constroem um banco de dados através de programas chamados *Web Crawlers* ou *spiders* (aranhas) que começam com uma lista de páginas de internet conhecidas. Esse programa pega uma cópia de cada página e indexa-a, guardando informações importantes que permitirão que a página seja facilmente recuperada mais tarde. Qualquer hiperlink para novas páginas são adicionadas para a lista de páginas para serem indexadas. Eventualmente, todas as páginas acessíveis são indexadas, a menos que exceda os limites do motor de busca. O conjunto de páginas acessíveis define a *Surface Web*. Por diversas razões (como o Protocolo de Exclusão de Robôs, *links* gerados por *Javascript* e *Flash*, proteção de senhas) algumas páginas não podem ser acessadas pela Web *Crawlers*. Essas páginas compõem a *Deep Web*. Em Janeiro de

2014 as páginas indexadas eram pelo menos 15 bilhões de páginas.7” (MARCON *et. al*., 2016).

A princípio, foi desenvolvido um mecanismo de comunicação chamado de *Onion Roting,* que a partir dele foi criado um navegador chamado *Tor Onion Browser,* desenvolvido e financiado por laboratórios da marinha americana. Nesse sentido, o navegador tem o intuito de garantir o anonimato na comunicação entre duas pessoas na internet, embora seu código para entrada seja público, e assim, todos podem acessar. Logo, com anonimato garantido, o governo não consegue obter uma ordem judicial por meio da empresa de telefonia para conseguir efetuar a localização. Por isso o nome*Onion* (cebola), devido a camadas de uma cebola, visto que a cada camada que se passa, o conteúdo é criptografado e mandado para outra camada, assim o indivíduo sempre pode estar mantido em anônimo. Também vale ressaltar que o *Tor* não é o único navegador que possibilita a entrada na *deep web*, mas sim o primeiro, mais conhecido e usado do meio.

Em seu lado em que presa pela legalidade, também podemos localizar coisas positivas e dentro da legalidade, como registros financeiros de instituições, artigos científicos, muitos filmes que não são achados na surface e documentos governamentais lá colocados para que os mesmos não sejam achados com facilidade.

Mas quanto ao seu lado ruim e ilegal, podem ser encontrados desde fóruns e *chats hackers* conhecidos como *chans*, passaportes falsos, venda de cartões clonados, venda de produtos roubados e diversos dados de pessoas que são roubados e, subsequentemente, usados. Devido à pandemia, esses crimes só aumentaram, uma vez que o criminoso pode trabalhar diretamente de seu computador.

‘’No dia 3 de fevereiro, a equipe da *PSafe* detectou a oferta na *deep web* de 102.828.814 contas de celular com informações sensíveis, como o tempo de duração de ligações, número do telefone e outros dados pessoais, como CPF e endereço” (BBC NEWS, 2021).

Podendo ser ainda pior, na camada dentro da *Deep Web* chamada *Dark web*, onde se deve realmente ser cuidadoso, uma vez que são encontrados venda de drogas, assassinos de aluguel, pornografia infantil, trafico de órgãos e pessoas, canibalismo e exploração infantil. Nesse contexto, as ações supracitadas são pagas com *bitcoins*, uma moeda criptografada que pode distinguir comprador e vendedor, mantendo o sigilo na *deep web*, apesar dele ainda poder ser rastreado.

É interessante mencionar que a Policia Federal faz operações na *deep web* se

passando por pedófilos e através de chats, conseguem marcar encontros, e assim, capturar os criminosos.

Outro deslize cometido por parte dos criminosos ao receberem *bitcoins,* é que acabam sendo rastreados, visto que não ocorre um tipo de troca de carteira eletrônica e o valor cai diretamente na conta do criminoso. Sendo assim, ocorre a possibilidade de rastreamento e captura de bandidos.

3. CAPÍTULO 2: INTERNET, BANCOS E CLIENTES: A TECNOLOGIA.

Há quem ainda duvide que o mundo seja completamente digital, no entanto, estamos na era conhecida como ‘’a revolução 4.0’,’ onde quase tudo funciona e evolui conforme a tecnologia. Nesse contexto, realizar compras e vendas, se relacionar e buscar conhecimento é relativmente fácil, pois é uma área cheia de vantagens e descomplicada, porém, é também repleta de riscos e perigos. Isto posto, percebe-se o surgimento de uma nova legião de criminosos digitais, orientados a explorar as principais vulnerabilidades da internet e com um objetivo em comum: obter lucros com os roubos e a exposição de dados.

Crimes cibernéticos estão em uma crescente evolução criminalmente e juridicamente, mas dentre esses, destaca-se os delitos cometidos devido a falhas do sistema bancário, desatenção de clientes ao caírem em golpes e ao grande avanço tecnológico na modalidade criminosa.

Bancos puderam evoluir com o tempo, tentando facilitar a vida de seus clientes com a criação de sites e aplicativos para acesso a conta bancária, assim pode-se pagar boletos, fazer transferências para outras contas no método de transferência ou pix. Por conseguinte, todos esses métodos facilitam a vida de seus clientes, pois permitem que suas operações sejam realizadas diretamente de casa, sem necessidade de ir até a agência bancária.

Em contrapartida, os dados dos clientes são fornecidos a agência, sendo ela responsável ou não pelos vazamentos de informações, que são devidamente protegidas pela LGPD (Lei Geral de Proteção de Dados 2019) Lei nº 13.853, de 2019:

> Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Apesar disso, criminosos agem de maneira fraudulenta ao violar tal lei e ao enviar e-mails com vírus, se passando ser funcionário da agência bancária e até mesmo o próprio funcionário bancário agindo de má fé para tirar proveito de clientes, visto que não possuem conhecimento e passam suas informações, tendo seus dados e contas

roubados.

Há também a possibilidade de falhas do sistema bancário, no qual esses criminosos se aproveitam e roubam dados de clientes para si, possibilitando a fraude bancária de maneira executada pela internet, que tem crescido de maneira astronômica.

3.1 FRAUDES BANCÁRIAS NA INTERNET

As fraudes bancárias (podem ser enquadradas como estelionato e furto eletrônico, segundo o artigo 171 (CP BRASIL),1940):

> Art. 171 - Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento:
> Pena - reclusão, de um a cinco anos, e multa, de quinhentos mil réis a dez contos de réis.
> § 1º - Se o criminoso é primário, e é de pequeno valor o prejuízo, o juiz pode aplicar a pena conforme o disposto no art. 155, § 2º.
> § 2º - Nas mesmas penas incorre quem:
> Disposição de coisa alheia como própria
> - vende, permuta, dá em pagamento, em locação ou em garantia coisa alheia como própria;
> Alienação ou oneração fraudulenta de coisa própria
> - vende, permuta, dá em pagamento ou em garantia coisa própria inalienável, gravada de ônus ou litigiosa, ou imóvel que prometeu vender a terceiro, mediante pagamento em prestações, silenciando sobre qualquer dessas circunstâncias;
> Defraudação de penhor
> - defrauda, mediante alienação não consentida pelo credor ou por outro modo, a garantia pignoratícia, quando tem a posse do objeto empenhado;
> Fraude na entrega de coisa
> - defrauda substância, qualidade ou quantidade de coisa que deve entregar a alguém;
> Fraude para recebimento de indenização ou valor de seguro
> - destrói, total ou parcialmente, ou oculta coisa própria, ou lesa o próprio corpo ou a saúde, ou agrava as conseqüências da lesão ou doença, com o intuito de haver indenização ou valor de seguro;
> Fraude no pagamento por meio de cheque
> - emite cheque, sem suficiente provisão de fundos em poder do sacado, ou lhe frustra o pagamento.
> § 3º - A pena aumenta-se de um terço, se o crime é cometido em detrimento de entidade de direito público ou de instituto de economia popular, assistência social ou beneficência.

É o modo mais usado por *cyber*-criminosos, visto que movimenta muitos roubos financeiros e de bancos de dados, em especial aquelas feitas pelo *Internet Banking,* que é uma das formas em que clientes de agências bancárias podem fazer transações e administrar sua conta diretamente pelo computador, (Marcelo Lau (2006) especialista em *cyber*-segurança).

> A Fraude Internet é definida pelo Departamento de Justiça Norte- americano (*U.S. Department of Justice*), como a aplicação de qualquer golpe relativo à fraude, utilizando os serviços disponíveis na Internet, tais como salas de bate-papo, mensagens eletrônicas e sites disponíveis na Internet. É compreendido como fraude, o aliciamento de vítimas através do fraudador e realização de transações fraudulentas beneficiando um indivíduo ou grupo de pessoas envolvidas no esquema.

Nesse meio, os golpes mais praticados são venda de serviços, promessa de oportunidade de trabalho, roubo de dados e identidades. Tudo é oferecido e prometido pelos fraudadores ao agir, a fim de enganar muitos clientes.

O crime é iniciado a partir do primeiro contato do criminoso com a vítima mediante aos meios digitais, na maior parte efetuado por e-mails ou mensagens, sendo aprofundado a partir dos seguintes mecanismos:

- *Ransomwares*: É um dos ataques mais conhecidos e utilizados pelos crackers, onde o criminoso sequestra os dados por meio de criptografia e pede o resgate em *bitcoins*.
- *Trojans*: Conhecidos por vírus *malware,* que roubam informações de uma conta, podendo ser bancária, de jogos online, lojas.
- *Phishings*: Aqueles que diariamente ‘’fisgam’’ vítimas por meios de campanhas falsas, podendo ser enviado por redes sociais, *e- mails* e caindo na caixa de *spam*, citado abaixo.
- *Spam*: Refere-se aos *e-mails* não solicitados, que geralmente são enviados para um grande número de pessoas. Quando o conteúdo é exclusivamente comercial, esse tipo de mensagem é chamada de UCE (do inglês *Unsolicited Commercial E-mail*).
- *Scam*: Pode ser destacado como situação ou ação fraudulenta que tem como finalidade enganar e obter vantagem financeira.

Como destaca Lau (2006):

> A natureza fraudulenta destas mensagens está relacionada à tentativa de convencimento do receptor mediante a alguma oferta descrita pelo responsável115 no envio desta mensagem eletrônica. Nestes casos, a oferta se constitui em um golpe, levando a vitima a perdas financeiras.

Nesse método, é interessante mencionar alguns *e-mails* que recebemos de

intermediários totalmente aleatórios, que propoem uma quantia financeira, onde a vítima é intermediária em transações milionárias, e também, na maioria das vezes, o golpe tenta atingir a vítima através de *links* forjados para a obtenção de dados por parte do criminoso.

Subsequentemente, temos o *Pharming* que segundo Lau (2006):

> O mecanismo utilizado por este ataque promove o redirecionamento da vítima a páginas falsas de instituições financeiras, entretanto esta variação de ataque não utiliza uma mensagem eletrônica como vetor de propagação. O atacante busca fragilizar serviços de resolução de nomes na Internet, conhecidos como DNS128, que resultam no acesso errôneo do usuário à página replicada pelo fraudador, similar a página da instituição financeira, mesmo que o usuário efetive a inserção do endereço da página do banco através da digitação da *URL* no *browser* utilizado na navegação Internet.

Vale ressaltar que, na atualidade e com o fator agravante da pandemia do coronavírus, a fraude bancária no meio digital é o crime que mais movimenta a internet.

O ano de 2020 foi marcado por um enorme aumento das fraudes financeiras globalmente, impulsionado pela rápida adesão ao internet *banking* e ao comércio online, segundo o relatório de crimes financeiros divulgados pela Feedzai. A empresa de ciência de dados, especializada na detecção e prevenção ao risco de fraude financeira, comparou o volume de fraudes bancárias e crimes cibernéticos no quarto e no primeiro trimestre de 2020 com o último trimestre, período imediatamente anterior ao recrudescimento da pandemia. (CISO ADVISOR, 2021)

O Tribunal de Justiça julgou alguns casos e processos mediante os métodoscitados acima, mostrando evolução, embora lenta, acerca de crimes digitais/ cibernéticos no Brasil, tais como:

> APELAÇÃO CÍVEL. DIREITO DO CONSUMIDOR. AQUISIÇÃO DE APARELHO CELULAR PELA INTERNET. FRAUDE VIRTUAL (*PHISHING*). Sentença de procedência parcial, condenando o Banco apelante ao ressarcimento do valor pago pelo produto não recebido, no importe de R$ 490,00. Constatação que o boleto de pagamento do produto realizado pela parte autora ter sido falsificado porterceiros, já que não condiz com os boletos disponibilizados pela empresa ré. Banco réu ré que não responde pelos prejuízos derivados de fraude virtual denominada *phishing*. Conduta descuidada sem consultar o site da empresa varejista, a partir do seu sítio eletrônico registrado no sistema de domínio de internet. Valor da mercadoria adquirida (R$ 490,00), nitidamente incompatível comas propriedades e marca do aparelho no mercado de consumo, em torno de RR 1.189,00. Precedentes jurisprudenciais deste Tribunal de justiça. Inexistência de prova de que a emissão do boleto tenha decorrido de falha no seu sistema interno, situação que afasta a incidência da Súmula 479 do STJ e, consequentemente, a responsabilidade objetiva do Banco apelante. Sentença que se reforma para julgar improcedente os pedidos indicados na inicial. Custas,despesas e honorários advocatícios em favor da parte ré para o percentual de

> 10% sobre o valor dado à causa, pela parte autora, observando-se a condição suspensiva de exigibilidade contida no artigo 98 § 3º do CPC, diante a gratuidade concedida. Conhecimento e provimento do recurso. (TJ-RJ - APL: 01448935220188190001, Relator: Des(a). JDS RICARDO ALBERTO PEREIRA, Data de Julgamento: 25/03/2021, VIGÉSIMA CÂMARA CÍVEL, Data de Publicação: 06/04/2021)

> APELAÇÃO CÍVEL. DIREITO DO CONSUMIDOR. AÇÃO INDENIZATÓRIA. FRAUDE EM CONTA CORRENTE. DESFALQUE PERPETRADO PORTERCEIRO. PRÁTICA DE *FISHING* OU *PHARMING*. CONSUMIDOR QUE, LUDIBRIADO, FORNECE DADOS BANCÁRIOS SIGILOSOS. FALHA NO DEVER DE SEGURANÇA NÃO CONFIGURADA. FORTUITO EXTERNO. RESPONSABILIDADE DO FORNECEDOR AFASTADA. DESPROVIMENTO DO RECURSO. 1. Trata-se de ação indenizatória visando à restituição de quantia retirada por terceiro da conta corrente da autora, bem como compensação por dano moral. 2. Do próprio relato da representante legal da autora, mostram-se inequívocos não só o fato exclusivo de terceiro fraudador como o fato do consumidor, inexistindo falha na prestação do serviço. 3. O fraudador agiu mantendo contato direto, não com o Banco, mas com a representante legal da empresa autora, que seguiu o passo a passo da orientação dada pelo terceiro desconhecido. 4. Inexistência de concurso do réu para o sucesso da empreitada criminosa, já que o estelionatário se passou por preposto do Banco e, a título de configuração ou atualização do dispositivo *token*, induziu a representante legal da autora a acessar um sítio eletrônico fictício, que foi criado para ludibriar o incauto, e a lhe fornecer informações sigilosas, configurando modalidade de fraude chamada de *fishing* ou *pharming*. 5. As transferências fraudulentas não foram realizadas em razão de falha no sistema de segurança do Banco, estando configurado o fortuito externo. 6. Desprovimento do recurso. (TJ-RJ - APL: 00025988220168190026, Relator: Des(a). ELTON MARTINEZ CARVALHO LEME,
> Data de Julgamento: 22/09/2020, DÉCIMA SÉTIMA CÂMARA CÍVEL, Data de Publicação: 24/09/2020)

3.2 CLONAGENS DE CARTÕES E CELULARES (WHATSAPP)

No que se refere a evoluções em práticas de crimes bancários cibernéticos, as clonagens de cartões de créditos e celulares, para que os criminosos possam usufruir do dinheiro ou simplesmente vender e coletar dados da vítima, são as ações mais comuns.

Leva-se em conta que as clonagens por cartão de crédito podem ser feitas física e presencialmente, por meio de um estabelecimento ou funcionário fraudulento/estelionatário, e essa clonagem acontece devido a ‘’tarja magnética’’, quando esta é passada nas máquinas de cartão ou caixa eletrônico, coleta-se os dados facilmente. Porém, devido à implantação de chips, tornou-se muito difícil o processo de clonagem, mas ainda pode ser efetuado como, por exemplo, quando o garçom de uma lanchonete percebe a vítima bêbada e na hora do pagamento da conta, ao invés de colocar o valor total da compra, vai diretamente para a senha do cliente, tendo assim a senha do cartão para usar como bem entender.

No mundo virtual, através de golpes, os criminosos tentam atrair as vítimas criando

links e os ‘’jogando’’ pela web. Tais links podem conter produtos em valores extremamente abaixo do valor de mercado, algo que chama a atenção do consumidor e faz com que o mesmo adquira esse ‘’produto’’ e, através dessa transação, dados são roubados. Também acontece em outros exemplos, em que são fornecidas imagens ou os dados do cartão de crédito, os quais não devem ser passadom em hipótese alguma.

De acordo com Anne Lacerda de Brito (2014):

> A responsabilidade entre as empresas acima mencionadas é classificada pelo Código de Defesa do Consumidor como objetiva e solidária. Objetiva porque o consumidor não irá precisar provar que houve intenção do fornecedor do serviço (banco/administradora/estabelecimento) para que o ato se concretizasse, ou seja, independe de culpa. E solidária porque os três poderão responder pela totalidade da devolução de valores devida ao consumidor.

O consumidor lesado não deve arcar de forma alguma com o pagamento da compra quando o cartão for clonado.

Nos casos abaixo, o TJ julgou alguns processos como procedente, referindo-se a dano moral, falhas na prestação de serviço e negligência de estabelimentos:

> EMENTA: APELAÇÃO CÍVEL - AÇÃO DE INDENIZAÇÃO - CARTÃO DE CRÉDITO CLONADO - FALHA NA PRESTAÇÃO DO SERVIÇO - DANO MORAL CONFIGURADO - QUANTUM INDENIZATÓRIO - HONORÁRIOS ADVOCATÍCIOS.
>
> EMENTA: APELAÇÃO CÍVEL - AÇÃO DE INDENIZAÇÃO - CARTÃO DE CRÉDITO CLONADO - FALHA NA PRESTAÇÃO DO SERVIÇO - DANO MORAL CONFIGURADO - QUANTUM INDENIZATÓRIO - HONORÁRIOS ADVOCATÍCIOS.
>
> EMENTA: APELAÇÃO CÍVEL - AÇÃO DE INDENIZAÇÃO - CARTÃO DE CRÉDITO CLONADO - FALHA NA PRESTAÇÃO DO SERVIÇO - DANO MORAL CONFIGURADO - QUANTUM INDENIZATÓRIO - HONORÁRIOS ADVOCATÍCIOS.
>
> EMENTA: APELAÇÃO CÍVEL - AÇÃO DE INDENIZAÇÃO - CARTÃO DE CRÉDITO CLONADO - FALHA NA PRESTAÇÃO DO SERVIÇO - DANO MORAL CONFIGURADO - QUANTUM INDENIZATÓRIO -- HONORÁRIOS ADVOCATÍCIOS.
> Não tendo o banco procedido com a cautela necessária na disponibilização de seus serviços e, ainda, enviado aos cadastros negativos o nome do autor, em razão de dívida inexistente, quebrou dever legal de vigilância e agiu com negligência, devendo ser responsável pelos prejuízos causados ao titular do cartão de crédito. Deve-se atentar na fixação da indenização pelos danos morais, às circunstâncias dos fatos do caso concreto, evitando o enriquecimento indevido, mas proporcionando à vítima uma satisfação e ao ofensor um desestímulo à prática de condutas abusivas. Se cada parte for vencedor e vencido na demanda,é de se aplicar o artigo 21 do Código de Processo Civil, que determina a divisão proporcional das despesas e honorários advocatícios. (TJ-MG - AC: 10707100104926001 Varginha, Relator: Tiago Pinto, Data de Julgamento:15/03/2012, Câmaras Cíveis Isoladas / 15ª CÂMARA CÍVEL, Data de Publicação: 23/03/2012)

> NEGATIVAÇÃO INDEVIDA. CARTÃO DE CRÉDITO "CLONADO" FRAUDE PERPETRADA POR TERCEIRO ESTELIONATÁRIO. DANO MORAL. RESPONSABILIDADE CIVIL. QUANTUM REPARATÓRIO CORRETAMENTE ARBITRADO.
>
> NEGATIVAÇÃO INDEVIDA. CARTÃO DE CRÉDITO "CLONADO" FRAUDE PERPETRADA POR TERCEIRO ESTELIONATÁRIO. DANO MORAL. RESPONSABILIDADE CIVIL. QUANTUM REPARATÓRIO CORRETAMENTE ARBITRADO.
>
> NEGATIVAÇÃO INDEVIDA. CARTÃO DE CRÉDITO "CLONADO" FRAUDE PERPETRADA POR TERCEIRO ESTELIONATÁRIO. DANO MORAL. RESPONSABILIDADE CIVIL. QUANTUM REPARATÓRIO CORRETAMENTE ARBITRADO.
>
> NEGATIVAÇÃO INDEVIDA. CARTÃO DE CRÉDITO "CLONADO". FRAUDE PERPETRADA POR TERCEIRO ESTELIONATÁRIO. DANO MORAL. RESPONSABILIDADE CIVIL. QUANTUM REPARATÓRIO CORRETAMENTE ARBITRADO.
> O autor teve seu nome negativado pelo réu em decorrência de débitos oriundos de compras efetuadas por terceiro estelionatário utilizando-se dos dados do cartão de crédito do autor, naquilo que popularmente se convencionou chamar de "clonagem". A veracidade das alegações do autor se evidencia diante da fatura acostada aos autos, enviada a endereço situado em São Paulo, diverso do domicílio do autor, que reside em Niterói, assim como as compras impugnadas, todas realizadas em cidades paulistas. Por outro lado, não trouxe a ré qualquer fato extintivo, modificativo ou impeditivo do direito do autor e, tampouco, demonstrou que as compras ou a mudança de endereço nos seus cadastrosforam efetuados pelo autor. Neste diapasão, afigura-se a responsabilidade civil objetiva da instituição financeira, por evidente defeito na prestação de serviço, fundada no art. 14, § 1º da Lei nº 8.078/90 e na teoria do risco empresarial, considerando que quem retira proveito de uma atividade de risco, comprobabilidade de danos, obtendo vantagens, lucros, benefícios, deve arcar com os prejuízos perpetrados. No que se refere ao quantum indenizatório arbitrado a títulode dano moral, infere-se o acerto do d. Julgador ao fixar o valor de R$3.800,00, quantia que se mostra adequada e suficiente para reparar o dano extrapatrimonial sofrido, na ótica do arbitrium boni juri segundo os princípios da razoabilidade, proporcionalidade, equidade e de Justiça ancorado nas funções: a) punição - desestímulo - punitive dommage; b) compensação - pela intensidade do sofrimento, considerando no caso, falta não intencional do réu. DESPROVIMENTO DO RECURSO. (TJ-RJ - APL: 00082259120068190002 RIO DE JANEIRO NITEROI 7 VARA CIVEL, Relator: ROBERTO DE ABREU E SILVA,
> Data de Julgamento: 28/07/2009, NONA CÂMARA CÍVEL, Data de Publicação: 31/07/2009)

O correto a se fazer quando percebe-se que seu cartão foi clonado é contatar imediatamente a agência bancária, para que seu cartão seja bloqueado para uso, e para casos mais graves, é indicado ir até uma delegacia de polícia fazer o boletim de ocorrência.

Existe também a hipótese de clonagem via Whatsapp, no qual criminosos entram em contato com números aleatórios mandando algo chamativo como, por exemplo, passar-se pela operadora de telefone, com um número falso, prometendo um bônus de gigas a mais em internet móvel. Logo, a vítima se interessa, entra em contato fornecendo o código passado pelo golpista e assim tem seu whatsapp clonado.

Criminosos agem dessa forma para que possam ter uma conversa com a agenda de contatos das vítimas, se passando por ela e pedindo grandes quantidades em dinheiro por empréstimo.

Segundo Zanin, em seu blog no Jusbrasil (2019):

> Grande maioria de operadoras de telefones sugere a seus clientes a compra de novos chips, sendo um total desrespeito ao consumidor ao dar essa enorme ‘‘brecha’’ a fraudadores e golpistas, incluindo a exposição de seus clientes ao ridículo, incluindo perda de dinheiro, de contatos, histórico de conversas, e principalmente a privacidade zelada.

O TJSP (2019) julgou de maneira procedente o processo de uma vítima, caracterizando uma ação condenatória por danos morais:

> AÇÃO CONDENATÓRIA. DANOS MORAIS. MAJORAÇÃO DO VALOR DA INDENIZAÇÃO. Autora que teve seu aplicativo de mensagens clonado e utilizado por fraudador, que invadiu seu histórico de conversas e até pediu dinheiro emprestado se passando pela recorrente. Foi orientada a adquirir outra linha telefônica para dificultar nova clonagem e uma semana após a aquisição da nova linha, foi novamente clonada. Ante os elementos fáticos demonstrados nos autos, bem como se pautando nos princípios da razoabilidade e proporcionalidade, o valor da indenização por danos morais deve ser majorado para R$ 20.000,00 (vinte mil reais). Recurso parcialmente provido. (TJSP – Apelação Cível – 1105778-06.2018.8.26.0100. Relator: Desembargador Roberto Mac Cracken. Julgado 02/08/2019).

O ideal a se fazer nessa situação é comunicar o suporte do whatsapp para que o bloqueio do número que acabou por ser clonado, há também a possibilidade de realização de boletim de ocorrência, que pode ser feito de maneira online pelo site: ‘‘https://www.delegaciaeletronica.policiacivil.sp.gov.br/ssp-de-cidadao/home.’’

Deve-se ressaltar que ambas as práticas estão enquadradas como estelionato, presente no artigo 171 e artigo 154-A invasão de dispositivo móvel do Código Penal.

> ‘’ Um levantamento feito pelo laboratório especializado em segurança digital da Psafe mostrou que mais de 5 milhões de brasileiros foram vítimas da clonagem de WhatsApp(EXTRA, 2021)’’

3.3 FEBRABAN (FEDERAÇÃO BRASILEIRA DE BANCOS)

No capítulo em questão, será tratado a FEBRABAN, que em sua real nomenclatura significa Federação Brasileira de Bancos, que é a principal entidade representativa do setor bancário no Brasil, tomando conta de 98% de instituições financeiras e também do

setor bancário nacional, sendo uma entidade sem fins lucrativos.

Fundada no ano de 1967, na cidade de São Paulo, seu objetivo descrito em seu próprio site é:

> O objetivo da Federação é representar seus associados em todas as esferas do governo – Poderes Executivo, Legislativo e Judiciário e entidades representativas da sociedade, para o aperfeiçoamento do sistema normativo, a melhoria continuada dos serviços e a redução dos níveis de risco. Também busca concentrar esforços que favoreçam o crescente acesso da população aos produtos e serviços financeiros. (FEBRABAN, 2021)

É interessante salientar sua importância para o mercado de pagamentos, pois é uma grande instituição que rege no setor como, por exemplo, na criação da Lei do Boleto Bancário, em 2018, visando o aumento da segurança ao longo do processo de pagamento, o mesmo servindo para pagamentos via cartão de crédito. Junto ao PROCON, a entidade elaborou diretrizes de formas seguras referente ao pagamento via pix.

Basicamente, a FEBRABAN toma conta de praticamente tudo que aborda o mundo financeiro, inclusive, na atualidade, alerta sobre fraudes mediante internet, ainda mais levando em conta a atualidade e a pandemia, onde os crimes bancários via internet cresceram cerca de 80% e as tentativas de fraude, em sua maioria, são feitas através da tentativa do criminoso para que a vítima forneça sua senha e outros dados bancários via whatsapp, falsas lojas online, boletos falsos, entre outros.

> ‘’Os fraudadores usam de Engenharia Social, um conjunto de métodos e técnicas (computacionais e psicológicas) para manipular e convencer a vítima a revelar seus dados pessoais e bancários. O golpista é perspicaz e habilidoso.(FEBRABAN, 2021)’’

3.4 CYBER-SEGURANÇA E SEGURANÇA BANCÁRIA

A *cyber*-segurança é um dos braços da segurança da informação, juntamente com a segurança digital, atua na proteção das informações no ambiente físico e digital, isto é, área que cuida unicamente da segurança do universo digital.

A princípio, conceitua-se cyber-segurança como uma forma de proteção de dados da rede mundial de computadores, segura de roubos de dados, danos ao *hardware* e *software* e dados eletrônicos.

Como forma de precaução, para que se consiga se desviar desses golpes, existem

algumas recomendações a serem seguidas para estar sempre seguro, utilizando cuidados e algumas ferramentas.

A própria FEBRABAN (2021) cita em suas normas recomenda a prevenção a fraudes:

> - Manter programas antivírus atualizados instalados nos computadores utilizados para o acesso aos serviços bancários
> - Trocar a sua senha de acesso ao Internet Banking e aplicativos do setor bancário periodicamente
> - Use somente provedores confiáveis.
> - Evitar sites arriscados. Só faça transferência de arquivos para o seu computador de sites que você conheça e saiba que são confiáveis.
> - Cuidado ao receber e-mails não solicitados.

Outras recomendações que possibilitam ainda mais a segurança são: manter o software de computadores e celulares sempre atualizados, nunca usar computadores em redes públicas para fazer operações financeiras, usar apenas o site ou aplicativo oficial do banco em questão, sempre solicitar a opção de segurança a autenticação de dois fatores vinculados ao celular e a implementação de *token* cada vez que entrar na conta e efetuar uma transação bancária, utilização de *webfilters* que filtram a navegação e bloqueia sites não autorizados de acordo com a política de segurança estabelecida.

Segundo relatório da Code42(2019), aproximandente 78% dos profissionais de segurança acreditam que a maioria das ameaças à segurança de *endpoints* (dispositivos, computadores, desktop, notebooks e celulares) são relacionados à negligência entre os colaboradores por polítcas claras de segurança ou pela falta delas.

A conscientização pode ser realizada de algumas formas, mas principalmente duas são utilizadas:

- Política de segurança: Relatando as ações nas quais os colaboradores podem e devem seguir.
- Treinamento de pessoas: Onde essas pessoas irão conhecer os riscos, os ataques e como agir para garantir que as informações da empresa e clientes permaneçam em segurança.

Com essa conscientização, o objetivo sempre é que as pessoas/vítimas pensem antes de clicar. Nesse ínterim, a *cyber*-segurança é uma área da segurança que precisa ser cada vez mais conhecida e implementada na sociedade, não só por empresas, mas

também para pessoas, afim de diminuir ou evitar golpes e roubos.

4. CAPÍTULO 3: ANÁLISE DA TENDÊNCIA DO JUDICIÁRIO NA JURISPRUDÊNCIA

Ao falar em crimes cibernéticos, sempre ocorrem algumas dúvidas perante leis e medidas que o judiário nacional segue e aborda para julgar ou penalizar os crimes cibernéticos cometidos quanto às instituições bancárias e clientes, acerca dos âmbitos do direito e suas esferas.

A legislação tem acertos e erros mediante aos crimes cibernéticos que tanto crescem no país, ainda mais na modalidade financeira práticada junto a bancos e seus clientes.

4.1 RESPONSABILIDADE CIVIL

No tocante a responsabilidade civil, relaciona-se imediatamente a resolver sanções e não causar prejuízo algum ao interesse alheio.

Conforme explica a doutrina ‘’não há responsabilidade se não houver dano’’, o objetivo da responsabilidade será reparar os danos causados, sendo injusto ou não.

Consequentemente, a responsabilidade civil poderá ser conceituada como “normas a serem aplicadas as quais obriguem uma pessoa a responder e assumir o dano causado a outro semelhante.”

Conforme diz Rui Stocco (2007)

> A noção da responsabilidade pode ser haurida da própria origem da palavra, que vem do latim respondere, responder a alguma coisa, ou seja, a necessidade que existe de responsabilizar alguém pelos seus atos danosos. Essa imposição estabelecida pelo meio social regrado, através dos integrantes da sociedade humana, de impor a todos o dever de responder por seus atos, traduz a própria noção de justiça existente no grupo social estratificado. Revela-se, pois, como algo inarredável da natureza humana. (STOCO, 2007, p.114)

Como diz Sergio Cavalieri Filho (2012), responsabilidade civil deve ser tratada com dever jurídico:

> Entende-se, assim, por dever jurídico a conduta externa de uma pessoa imposta pelo Direito Positivo por exigência da convivência social. Não se trata de simples conselho, advertência ou recomendação, mas de uma ordem ou comando dirigido e à vontade dos indivíduos, de sorte que impor deveres jurídicos importa criar obrigações. (CAVALIERI FILHO, 2012, p. 2)

E também ressalva em caso de seu descumprimento:

> A violação de um dever jurídico configura o ilícito, que, quase sempre, acarreta dano para outrem, gerando um novo dever jurídico, qual seja, o de reparar o dano.Há assim, um dever jurídico originário, chamado por alguns de primário, cuja violação gera um dever jurídico sucessivo, também chamado de secundário, que é o de indenizar o prejuízo. A título de exemplo, lembramos que todos têm o dever de respeitar a integridade física do ser humano. Tem- se, aí, um dever jurídico originário, correspondente a um direito absoluto. Para aquele que descumprir esse dever surgirá um outro dever jurídico: o da reparação do dano. (CAVALIERIFILHO, 2012, p. 2).

4.1.1 Responsabilidade civil subjetiva

Antes mesmo de falar em responsabilidades, deve-se salientar a necessidade de passar pelos pressupostos, ou seja, o nexo causal, dano, ação e omissão, e subsequentemente, a conduta humana.

A ação e omissão, através da conduta humana, é a obra de causar dano alheio, e consequentemente, um ato que por si só ocasiona prejuízos, podendo ser por negligência, imperícia, dolo e imprudência.

Ressalva Pablo Stolze Gagliano e Rodolfo Pamplona Filho (2008):

> Em outras palavras, a voluntariedade, que é pedra de toque da noção de conduta humana ou ação voluntária, primeiro elemento da responsabilidade civil, não traduz necessariamente a intenção de causar o dano, mas sim, e tão-somente, a consciência daquilo que se está fazendo. E tal ocorre não apenas quando estamos diante de uma situação de responsabilidade subjetiva (calcada na noção de culpa), mas também de responsabilidade objetiva (caucada na idéia de risco), porque em ambas as hipóteses o agente causador do dano deve agir voluntariamente, ou seja, de acordo com a sua livre capacidade de autodeterminação. (2008, p.28)

Conceitua-se responsabilidade civil subjetiva ou culposa sendo aquela que dependa de comprovações de culpa ou dolo por parte de quem causou o dando. Nesse sentido, só haverá direito a indenização caso o dolo ou culpa seja comprovado por parte do agente agressor.

Logo, a teoria subjetiva, portando o elemento de culpar, constitui-se no artigo 186 do CC (Código Civil, 2002):

> ‘’ “Art. 186”. Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente’’

Embora a maioria dos casos puderam ser resolvidos pela forma subjetiva, ela não é a única aplica em regra segundo Sergio Cavalieri Filho (2009):

> Por esta concepção clássica, todavia, a vítima só obterá a reparação do dano se provar a culpa do agente, o que nem sempre é possível na sociedade moderna. O desenvolvimento industrial, proporcionado pelo advento do maquinarismo e outros inventos tecnológicos, bem como o crescimento populacional geraram novas situações que não podiam ser amparadas pelo conceito tradicional de culpa.

4.1.2 Responsabilidade civil objetiva

Por fim, conceitua-se responsabilidade objetiva como aquela que independe da comprovação de culpa ou dolo do causador do dano. Nesse contexto, existe apenas o nexo de causalidade entre a conduta aferida e o dano causado, ambas tendo relação.

Ou seja, mesmo que o agente causador não tenha agido com culpa ou dolo, deverá ser imposta a indenização a vítima zelada.

Como conceitua Carlos Roberto Gonçalves (2012):

> A classificação corrente e tradicional, pois, denomina objetiva a responsabilidade que independe de culpa. Esta pode ou não existir, mas será sempre irrelevante para o dever de indenizar.
> Indispensável será a relação de causalidade entre a ação e o dano, uma vez que, mesmo no caso de responsabilidade objetiva, não se pode acusar quem não tenha dado causa ao evento.

A responsabilidade na maneira objetiva foi disposta no artigo 927 de nosso CC (Código Civil, 2002):

> Parágrafo único: Haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, riscos para os direitos de outrem.

A responsabilidade civil objetiva, criada ao final do século XIX, foi adotada para remediar as dificuldades impostas nas comprovações de dolo e culpa perante defensores apenas de teorias subjetivas.

4.2 RESPONSABILIDADE PERANTE O CÓDIGO DE DEFESA DO CONSUMIDOR

Em seu 14º artigo, o código de defesa do consumidor abordou de forma evidente que os fornecedores de serviços devem responder possuindo culpa ou não, por reparação de danos causados a seus consumidores referentes a prestação de seu serviço disponibilizado:

> Art. 14. O fornecedor de serviços responde independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos relativos à prestação dos serviços, bem como por informações insuficientes ou inadequadas sobre sua fruição e riscos.

Desta forma, eventuais fraudes cometidas contra clientes utilizadores do serviço bancário mediante *internet banking* ou aplicativos móveis estará em plena responsabilidade da instituição bancária/financeira, tendo que restituir os valores desviados ou roubados da conta da vítima, também podendo responder por danos patrimoniais e morais.

Vale ressaltar que, nos casos de fraudes mediante internet, a instituição irá responder de forma objetiva no que tange o ressarcimento de prejuízos e danos causados ao cliente, visto que as fraudes ocorram em meio à falha da instituição como, por exemplo, com um dado vazado do cliente, ou seja, a responsabilidade será dada apenas com a ajuda do juiz ao analisar o caso na situação em questão, como demonstrado a seguir para forma de excludente de culpa da instituição.

> Art. 14. O fornecedor de serviços responde independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos relativos à prestação dos serviços, bem como por informações insuficientes ou inadequadas sobre sua fruição e riscos.
>
> § 3° O fornecedor de serviços só não será responsabilizado quando provar:
>
> I - que, tendo prestado o serviço, o defeito inexiste; II - a culpa exclusiva do consumidor ou de terceiro.

Aplica-se também o artigo 3º do CDC:

> Art. 3° Fornecedor é toda pessoa física ou jurídica, pública ou privada, nacional ou estrangeira, bem como os entes despersonalizados, que desenvolvem atividade de produção, montagem, criação, construção, transformação, importação, exportação, distribuição ou comercialização de produtos ou prestação de serviços.
>
> § 1° Produto é qualquer bem, móvel ou imóvel, material ou imaterial.
>
> § 2° Serviço é qualquer atividade fornecida no mercado de consumo, mediante

> remuneração, inclusive as de natureza bancária, financeira, de crédito e securitária, salvo as decorrentes das relações de caráter trabalhista.

4.3 QUANTO A RESPONSABILIDADE DA INSTITUIÇÃO BANCÁRIA NOS DANOS CAUSADOS PELOS CRIMINOSOS

Ao falar sobre tecnologia no mercado brasileiro, destaca-se de maneira astronômica, as instituições bancárias, como objetivo facilitar o uso de seu ‘’produto’’ para seus clientes e diminuir grandes lotações em agências e diminuindo seus gastos, sendo possível fazer transações com o uso da internet mediante aplicativos móveis para celulare o *internet banking*.

Com esse acesso remoto para todos, houve um grande aumento de crimes por mal intencionados, ou seja, *cyber*-criminosos, os quais se aproveitam de devida falta de informação e boa-fé de clientes e usuários leigos dos serviços via internet oferecidos pelas instituições bancárias.

No que diz respeito a esses mecanismos, a responsabilidade das agências e instituições é por intermédio de contratos assinados por clientes. Por se tratar de ação entre instituição e consumidor, a mesma é regrada pelo Código de Defesa do Consumidor(CDC).

Sobre as fraudes por meio da internet, estas ocasionam prejuízos materiais e morais do consumidor, e podem ser denominadas como defeito do serviço, vício, ou acidente de consumo.

Segundo Sérgio Cavalieri Filho (2012):

> A palavra-chave neste ponto é defeito. Ambos decorrem de um defeito do produto, só que no fato do produto ou do serviço o defeito é tão grave que provoca um acidente que atinge o consumidor, causando-lhe dano material ou moral. O defeito compromete a segurança do produto ou serviço. Vício, por sua vez, é defeito menos grave, circunscrito ao produto ou serviço em si; um defeito que lhe é inerente ou intrínseco, que apenas causa o seu mau funcionamento ou não funcionamento (2012, pg.558).

Alguns doutrinadores julgam ser um vício por inadequação do serviço Internet banking e aplicativos móveis. Porém, Sergio Cavalieri Filho, por ser um grande defensor e adepto do Código de Defesa do Consumidor (CDC), vai contra esse pensamento. Segundo o mesmo, deve-se levar em conta na prática e o defeito, que nada mais é que uma falha de obrigação no Código de Defesa do Consumidor de colocar no mercado

‘’produtos’’ executados de defeitos.

Nessa circunstância, atenta-se ao dever de qualidade, o qual a instituição bancáriae seus serviços móveis não estão desobrigados da isenção. Salienta-se que, embora a proteção ao consumidor seja ampla, a responsabilidade civil das instituições bancárias mediante fraudes pela internet não é total.

Como forma excludente, por exemplo, o cliente bancário permite que terceiros façam operações em seu nome, mediante os serviços remotos, fornecendo dados e senhas para que a operação seja feita. No caso, o próprio cliente assume para si mesmoo risco da fraude ocorrer, sendo unicamente culpa da vítima e excluindo a culpa da instituição bancária.

Em outra hipótese de excludente, refletindo quanto à responsabilidade dos bancos, está a não colocação do produto no mercado, isto é, o seu fornecedor, enquanto fabricante, não introduz no mercado o produto defeituoso ou vicioso.

A inexistência do defeito, ou seja, quando o produto não apresenta defeito que o possa diminuir qualidade e quantidade.

> Juíza titular do 2º Juizado Especial Cível de Brasília julgou improcedentes os pedidos de restituição de valores e indenização por danos morais feitos por um consumidor contra o Banco Santander. O autor teria sido vítima de fraude ao repassar seus dados de acesso bancário, indevidamente, por telefone, e assim teve prejuízo de R$ 18 mil. Segundo os autos, o autor recebeu mensagem alertando sobre bloqueio de acesso à central de atendimento do banco e, sem averiguar a legitimidade da fonte, entrou em contato e repassou seus dados e senha pessoal – dando causa ao prejuízo de R$ 27 mil, referente a três transferências de R$ 9 mil, além das taxas bancárias.

Por se tratar de responsabilidade civil, o defeito do serviço é o que acaba motivando o dever da reparação de quem o fornece, haja vista que, na maioria das vezes,o banco terá que indenizar o valor ‘’roubado’’ da vítima, mediante a fraude bancária feita por *cyber*-criminosos.

Sendo assim aplicada a Súmula 479 do STJ: Instituição responde objetivamente

> “As instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbitode operações bancárias.”

Acerca desse assunto, há poucas jurisprudências que tratam de fraudes pelainternet, por se refererir a um assunto novo em nosso país e apenas alguns tribunais

efetivaram sobre as fraudes no ambiente digital:

> TJ-SP - Apelação APL 10028557220138260100 SP 1002855- 72.2013.8.26.0100 (TJ-SP) Ementa: "RESPONSABILIDADE CIVIL Danos materiais - Transferência de numerário via 'internet' não reconhecida pelo correntista - Banco que não se desincumbiu do ônus de provar a culpa exclusiva do consumidor na transação Aplicação da teoria do risco profissional Responsabilidade do banco reconhecida Restituição dos valores Dano material devido Recurso do banco improvido. RESPONSABILIDADE CIVIL Danos morais Banco que inicialmente reconheceu a fraude e estornou o valor da transferência não reconhecido pelo consumidor e após um ano descontou referido valor da conta da autora - Dano moral reconhecido Indenização fixada em R$ 5 000,00 - Recurso da autora provido." Data de publicação: 10/09/2013.
>
> TJ-SC - Apelação Cível AC 20130844756 SC 2013.084475-6 (Acórdão) (TJ- SC) Ementa: APELAÇÃO CÍVEL. AÇÃO DE INDENIZAÇÃO POR DANOS MATERIAIS E MORAIS. DÉBITOS INDEVIDOS EFETUADOS POR MEIO ELETRÔNICO-INTERNETNA CONTA BANCÁRIA DO AUTOR. RESPONSABILIDADE DO BANCO PELA FRAUDE ELETRÔNICA. MATÉRIA EMINENTEMENTE CIVIL. COMPETÊNCIA DAS CÂMARAS DE DIREITO CIVIL. ATO REGIMENTAL N. 41/00. PRECEDENTES DESTE TRIBUNAL. REDISTRIBUIÇÃO QUE SE IMPÕE. RECURSO NÃO CONHECIDO. Data de publicação: 16/07/2014.

5. CONCLUSÃO

Urge salientar que a Sociedade da Informação, aliada às novas tecnologias de comunicação, resultaram em mudanças drásticas no cotidiano do cidadão no Brasil e no mundo. Devido a enorme facilidade em ter acesso a essas tecnologias, percebe-seenormes melhorias como a otimização de relações, revolução de métodos e crescimento na produtividade de grandes empresas, instituições e indústrias.

Nesse âmbito, o universo da internet, totalmente tecnológico, engloba as mais diferentes formas de uso e de serviços, e por intermédio desses, centenas de milhares de dados são enviados e recebidos a todo o momento, num eterno *looping*. Nesse sentido, faz-se necessário investir na segurança, afim de proteger os dados recebidos a todo e qualquer momento.

No entanto, com o enorme avanço do mundo digital e tecnológico, foram abertas diversas fronteiras para o então aparecimento de novos crimes, permitindo que usuários com intenções maldosas ou com intuito de se aproveitar de uma situação, combinados a um grande conhecimento sobre o mundo digital, se adaptem ao progresso de práticas criminosas, aumentando de forma exorbitante as fraudes eletrônicas ao passar de anos.

No que se refere às fraudes eletrônicas, a relação entre instituições bancárias e clientes deve ser considerada de consumo. Atentando que a instituição bancária forneça serviços com fins lucrativos por meio de sua atividade, portanto, responsabiliza-se em caso de danos e fraudes causados por *cyber*-criminosos. Assim entendida pela a aplicação da responsabilidade civil objetiva, aquele que independe da culpa da instituição bancária.

Visto em cena anteriormente, os doutrinadores e jurisprudências brasileiras, em sua imensa maioria, se colocam a favor da responsabilização das instituições bancárias em casos de fraudes e danos causados via ambiente digital. Portanto, observa-se o enorme atraso quanto à atualização legislativa perante o assunto em nosso país e faz-se imprescíndivel medidas acertivas pelos os legisladores, visto que o Brasil é um dos países com o índice mais alto de criminalidade mediante ambiente virtual. Em contrapartida,

países ditos como mais desenvolvidos, já tem leis e medidas próprias acerca dos crimes e fraudes pela internet.

De perspectiva ampla, a internet surgiu para tornar a vida das pessoas mais fácil, mantendo sua liberdade e autonomia. Nesse contexto, ainda há um princípio em que sites devem ser intangíveis, mas *cyber*-criminosos mostram o contrário, levando em consideração que vão além dos limites legais e acessam os sistemas sem problemas e restrições, tendo acesso a dados e informações.

Embora a internet seja uma experiêcia de sucesso, os limites de sua real finalidade foram ultrapassados e é difícil exterminar a prática de criminosos na área digital e tecnológica. Sendo assim, é necessário que a instituição/empresa que oferece um serviço virtual, não possa ser exclusa de culpa e responsabilidade quando um dano é causado por um *cyber*-criminoso, visto que é de sua responsabilidade e obrigação manter um sistema ou *software* seguro seus clientes e para que não haja riscos para o cliente e titular da conta.

Destarte, sabe-se que os bancos, atualmente, são os principais alvos das investidas de *cyber*-criminosos. Portanto, deve haver planos e ações de defesa, juntamente a políticas internas da instituição, visando a criação medidas e alertas preventivos, a fim de garantir o acesso seguro de clientes e a proteção de seus dados, além da proteção da própria instituição bancária quanto a futuros processos, danospatrimoniais atrelados à imagem e reputação da instituição aos quais devem ser zelados.

6. REFERÊNCIAS

BBC, **Mundo vive pandemia de ciberataques e Brasil está despreparado, diz CEO de empresa que descobriu megavazamento.** Disponível em: https://www.bbc.com/portuguese/brasil-56048010.

CAVALIERI FILHO, Sergio. **Programa de Responsabilidade Civil.** 8. ed. São Paulo: Atlas, 2010.

CAVALIERI FILHO, SERGIO. **Programa de Responsabilidade Civil.** 12 ed. São Paulo: Atlas, 2015**.**

CISO ADVISOR, **Fraudes financeiras crescem 650% com uso maior de banco online e e-commerce.** Disponível em: https://www.cisoadvisor.com.br/fraudes-financeiras-crescem-650-com-uso-maior-de-banco-online-e-e-commerce/.

CONVENÇÃO SOBRE O CIBERCRIME. Budapeste, 2001. Disponível em: < http://www.mpf.mp.br/atuacao-tematica/sci/normas-e-legislacao/legislacao/legislacoes-pertinentes-do-brasil/docs_legislacao/convencao_cibercrime.pdf.

CONJUR, **A responsabilidade civil dos profissionais e a nova legislação.** Disponível em: https://www.conjur.com.br/2003-fev-05/responsabilidade_civil_legislacao_brasil

EDUCALINGO, **Cyber-crime.** Disponível em https://educalingo.com/pt/dic-en/cybercrime.

EXTRA, **Mais de 5 milhões de brasileiros tiveram WhatsApp clonado em 2020.** Disponível em: https://extra.globo.com/economia/mais-de-5-milhoes-de-brasileiros-tiveram-whatsapp-clonado-em-2020-24857614.html.

FEBRABAN, **Anti fraudes FEBRABAN.** Disponível em: https://antifraudes.febraban.org.br/.

FEBRABAN, **A FEBRABAN.** Disponível em: https://portal.febraban.org.br/pagina/3031/9/pt-br/institucional.

GAGLIANO, Pablo Stolze; PAMPLONA FILHO, Rodolfo. **Novo curso de direito civil – Responsabilidade civil.** 6. ed. São Paulo: Saraiva, 2008.

GONÇALVES, Carlos Roberto. **Direito Civil Brasileiro:** Responsabilidade Civil. 7. ed. São Paulo: Saraiva, 2012. V. 4.

INELLAS, Gabriel Cesar Zaccaria de. **Crimes na Internet.** Editora Juarez de Oliveira. Ano

2009.

JESUS, D. E**. Direito penal – Parte Geral.** Vol. 1. São Paulo: Saraiva: 2003.

JORNAL JURID, **Crimes cibernéticos crescem 50% durante o período de isolamento social.** Disponível em: https://www.jornaljurid.com.br/noticias/crimes-ciberneticos-cresce-50-durante-o-periodos-de-isolamento-social.

JUNQUEIRA, Maria Dias. **Computer crimes: a criminalidade na era dos computadores.** Disponível em: http://biblioteca2.senado.gov.br:8991/F/?func=item-global&doc_library=SEN01&doc_number=000183521.

JUSBRASIL, **Classificação dos Crimes Digitais.** Disponível em: http://victortateoki.jusbrasil.com.br/artigos/307254758/classificacao-dos-crimes-digitais.

JUSBRASIL, **Cartão de Crédito clonado.** Disponível em: https://annelbrito.jusbrasil.com.br/artigos/115354955/cartao-de-credito-clonado?ref=serp.

JUSBRASIL, **Clonagem de Whatsapp e Dano Moral.** Disponível em: https://ezanin.jusbrasil.com.br/artigos/800145541/clonagem-de-whatsapp-e-dano-moral.

JUSBRASI, **Artigo 171 do Decreto Lei nº 2.848 de 07 de Dezembro de 1940.** Disponível em: https://www.jusbrasil.com.br/topicos/10617301/artigo-171-do-decreto-lei-n-2848-de-07-de-dezembro-de-1940.

JUSBRASIL, **Artigo 154A do Decreto Lei nº 2.848 de 07 de Dezembro de 1940.** Disponível em: https://www.jusbrasil.com.br/topicos/28004011/artigo-154a-do-decreto-lei-n-2848-de-07-de-dezembro-de-1940.

JUSBRASIL, **Artigo 14 da Lei nº 8.078 de 11 de Setembro de 1990.** Disponível em: https://www.jusbrasil.com.br/topicos/10606184/artigo-14-da-lei-n-8078-de-11-de-setembro-de-1990.

JUSBRASIL, **Artigo 3 da Lei nº 8.078 de 11 de Setembro de 1990.** Disponível em: https://www.jusbrasil.com.br/topicos/10608617/artigo-3-da-lei-n-8078-de-11-de-setembro-de-1990.

JUSBRASIL, **Artigo 927 da Lei nº 10.406 de 10 de Janeiro de 2002.** Disponível em: https://www.jusbrasil.com.br/topicos/10677854/artigo-927-da-lei-n-10406-de-10-de-janeiro-de-2002.

JUSBRASIL, **Pesquisa de Jurisprudências.** Disponível em: https://www.jusbrasil.com.br/busca?q=Pesquisa+Jurisprudencial.

LAU, Marcelo**. Análise das Fraudes Aplicadas sobre o ambiente do internet banking.** Disponível em: https://www.teses.usp.br/teses/disponiveis/3/3142/tde-19092006-164238/.

MARCON et. al., 2016. **Deep Web: O lado sombrio da internet.** Disponível em: http://www.humanas.ufpr.br/portal/conjunturaglobal/files/2016/02/DEEPWEB-O-Lado-Sombrio-da-Internet_Jo%C3%A3o-Paulo-falavinha-Marcon-Thais-Pereira-Dias.pdf.

MIGALHAS, **Convenção de Budapeste e crimes cibernéticos no Brasil.** Disponívelem: https://www.migalhas.com.br/depeso/335230/convencao-de-budapeste-e-crimes-ciberneticos-no-brasil.

NETSPEED, **Qual a diferença entre phishing e pharming.** Disponível em: https://netspeed.com.br/mais/blog/empreendedorismo/empresarial/qual-a-diferenca-entre-phishing-e-pharming-2/.

STOCO, Rui. **Tratado de responsabilidade civil: doutrina e jurisprudência.** 7 ed.. São Paulo Editora Revista dos Tribunais, 2007.

TJDFT, **Culpa exclusiva do consumidor afasta responsabilidade de banco em caso de fraude.** Disponível em: https://www.tjdft.jus.br/institucional/imprensa/noticias/2018/fevereiro/culpa-exclusiva-do-consumidor-afasta-responsabilidade-de-banco-em-caso-de-fraude.

TOR PROJECT, **A História.** Disponível em: https://www.torproject.org/pt-BR/about/history/.

VIANNA, Túlio Lima. **Do Acesso Não Autorizado a Sistemas Computacionais: Fundamentos de Direito Penal Informático.** Disponível em: https://repositorio.ufmg.br/bitstream/1843/BUOS-96MPWG/1/disserta__o_t_lio_lima_vianna.pdf.

WENDT, E.; JORGE, H. V. N. **Crimes Cibernéticos.** São Paulo: BRASPORT, 2012.

WIZIKERO, **Deep Web e Surface Web.** Disponível em: https://www.wikizero.com/pt/Deep_web.