UNIVERSIDADE DO SUL DE SANTA CATARINA

FABIANA DE CAMPOS FIRMIANO BERKEMBROCK

CRIMES VIRTUAIS COMETIDOS CONTRA CLIENTES DE INSTITUIÇÕES FINANCEIRAS NO PERÍODO DA PANDEMIA DA COVID 19

Tubarão

2021

FABIANA DE CAMPOS FIRMIANO BERKEMBROCK

CRIMES VIRTUAIS COMETIDOS CONTRA CLIENTES DE INSTITUIÇÕES FINANCEIRAS NO PERÍODO DA PANDEMIA DA COVID 19

Monografia apresentada ao Curso de Direito da Universidade do Sul de Santa Catarina como requisito parcial à obtenção do título de Bacharel em Direito.

Orientador: Profº. Cristiano de Souza Selig, Esp.

Tubarão

2021

FABIANA DE CAMPOS FIRMIANO BERKEMBROCK

CRIMES VIRTUAIS COMETIDOS CONTRA CLIENTES DE INSTITUIÇÕES FINANCEIRAS NO PERÍODO DA PANDEMIA DA COVID 19

Esta Monografia foi julgada adequada à obtenção do título de Bacharel em Direito e aprovada em sua forma final pelo Curso de Direito da Universidade do Sul de Santa Catarina.

Tubarão, 10 de dezembro de 2021.

Professor e orientador Cristiano de Souza Selig, Esp.
Universidade do Sul de Santa Catarina

Heitor Wensing Júnior, MSc.
Universidade do Sul de Santa Catarina

Mário Luiz da Silva, Esp.
Universidade do Sul de Santa Catarina

Dedico este trabalho à minha família, em especial meu esposo Roque e aos meus filhos Luca e Clara, minhas fontes de inspiração.

AGRADECIMENTOS

Agradeço primeiramente a Deus, que me permitiu a vida e concedeu-me saúde.

Ao meu esposo, grande companheiro de vida, que me deu todo suporte e força para que buscasse o meu sonho;

Aos meus filhos Luca e Clara, minhas fontes de luz, desculpem-me pelas muitas ausências, é “por vocês e para vocês”, sempre.

À minha mãe (*in memorian*) que, quando iniciei, ainda estava conosco, que me ensinou o valor da educação, meu exemplo de vida.

Aos meus amigos que acreditaram e sempre me incentivaram a continuar, apesar das adversidades.

Aos amigos e colegas feitos ao longo do curso, pelos ensinamentos compartilhados, momentos de alegria e companheirismo, muitos levarei para vida.

Aos professores do curso que nos acompanharam e nos repassaram seus sábios ensinamentos que nos possibilitaram finalizar mais esta etapa.

Em especial, ao meu orientador Cristiano de Souza Selig, pela dedicação, tempo desprendido, conhecimentos repassados e paciência, ao longo deste ano, não somente na finalização desta pesquisa, bem como do projeto jurídico.

“Não tente achar um atalho, porque não há atalhos. O mundo é uma luta, é árduo, é uma tarefa penosa, mas é assim que a pessoa chega ao pico”. Osho.

RESUMO

O presente trabalho de conclusão de curso teve como objetivo analisar se Pandemia da Covid-19 foi fator agravante para o aumento de casos de fraudes virtuais contra indivíduos que têm contas em instituição financeira, uma vez que houve aumento significativo de usuários nesse meio. Para tanto, foi desenvolvida uma pesquisa exploratória com abordagem qualitativa. Quanto aos procedimentos de coleta de dados, classificou-se como uma pesquisa bibliográfica e documental. Foram utilizadas leis, principalmente aquelas que regulamentam, em certa medida, os crimes virtuais, como o Marco Civil da Internet e a recente Lei 14155/21 sancionada em 27 de maio de 2021, entre outros documentos legais. Também serviram de base tanto para a fundamentação teórica quanto para a análise doutrinas, artigos científicos etc. Nesse sentido, esta pesquisa traz os tipos penais mais cometidos, classificações, condutas que caracterizam crimes, a obtenção de provas e as punições. Apresenta informações sobre alguns mecanismos mais utilizados para realização de fraudes e, assim, mostra algumas medidas de proteção e educação digital, para que os cidadãos, usuários desses meios, não caiam facilmente em golpes. Aponta, ainda, as responsabilidades das instituições financeiras, dos provedores de internet e da vítima, bem como possibilidades de ressarcimento. A partir da análise, foi possível verificar que, com a pandemia da Covid-19 e com as medidas de distanciamento social, os ambientes e serviços virtuais passaram a ser utilizados com maior frequência, e o cidadão ficou mais suscetível a tornar-se uma potencial vítima deste tipo de delito. E com as Instituições Financeiras, não foi diferente, atualmente a fraude bancária é o crime que mais movimenta a internet. Conseguintemente, concluiu-se que a pandemia foi um dos fatores que contribuiu significativamente para o aumento de atividades ilícitas no meio digital.

Palavras-chave: Crimes no ambiente virtual. Fraudes virtuais contra Instituições Financeiras. Pandemia da Covid-19 e crimes virtuais.

ABSTRACT

This course conclusion work aimed to analyze whether the Covid-19 Pandemic was an aggravating factor for the increase in cases of virtual fraud against individuals who have accounts in a financial institution, since there was a significant increase in users in this environment. Therefore, an exploratory research with a qualitative approach was developed. As for the data collection procedures, it was classified as a bibliographic and documentary research. Laws were used, mainly those that regulate, to some extent, virtual crimes, such as the Marco Civil da Internet and the recent Law 14155/21 enacted on May 27, 2021, among other legal documents. They also served as a basis for both the theoretical foundation and the analysis of doctrines, scientific articles etc. In this sense, this research brings the most committed criminal types, classifications, behaviors that characterize crimes, obtaining evidence and punishments. It presents information about some of the most used mechanisms for carrying out fraud and, thus, it shows some measures of protection and digital education, so that citizens, users of these means, do not easily fall for scams. It also points out the responsibilities of financial institutions, internet providers and the victim, as well as possibilities for compensation. From the analysis, it was possible to verify that, with the Covid-19 pandemic and with the measures of social distancing, virtual environments and services started to be used more frequently, and the citizen became more susceptible to becoming a potential victim of this type of crime. And with Financial Institutions, it was no different, currently bank fraud is the crime that moves the most on the internet. Consequently, it was concluded that the pandemic was one of the factors that significantly contributed to the increase in illegal activities in the digital environment.

Keywords : Crimes in the virtual environment. Virtual Fraud against Financial Institutions. Covid-19 pandemic and cybercrime.

LISTA DE ABREVIATURAS E SIGLAS

§	Parágrafo
ADI	Ação Direta de Inconstitucionalidade
Art	Artigo
Arts.	Artigos
BITNET	Because It´s Time Network
BO	Boletim de Ocorrência
Bps	Bits por segundo
CDC	Código de Defesa do Consumidor
CERT.br	Centro de Estudos, resposta e tratamento de incidentes de segurança no Brasil
CC	Código Civil
CF	Constituição Federal
Covid-19	Corona 9írus disease (doença do Coronavírus) ano de 2019
CP	Código Penal
CPP	Código de Processo Penal
ARPA	Advanced Research Projects Agency
EUA	Estados Unidos da América
FEBRABAN	Federação Brasileira de Bancos
HTML	Hyper Text Markup Language
IP	Internet Protocol
DNS	Domain Name System (sistema de nomes de domínios)
STJ	Supremo Tribunal de Justiça
STF	Supremo Tribunal Federal
TPC/IP	Transmission Control Protocol/ Internet Protocol
URL	Uniform Resource Locator (Endereço virtual de uma página)
WEB	Conjunto de Páginas na internet
WWW	World Wide Web
n.p.	Não paginado

SUMÁRIO

1 INTRODUÇÃO

O desenvolvimento tecnológico trouxe muitas facilidades e rapidez de comunicação, ao passo que alguns delitos virtuais foram expandindo-se e crescendo nas mesmas proporções.

Nesse compasso, sendo o Direito um agente regulatório, composto de regras e leis que regulam a vida em sociedade, deve acompanhar tal evolução, adequando-se e aprimorando-se frente à nova realidade.

Assim, diante do aumento dos crimes virtuais, um tipo de delito, merece cuidado especial, qual seja, o crime contra os indivíduos que têm contas em instituições financeiras, objeto deste trabalho, o que se agravou ainda mais, durante o período de isolamento social, em função da Pandemia da Covid-19, iniciada em março de 2019, visto que as pessoas foram obrigadas a se habituarem a uma nova realidade, passando a utilizar mais os sistemas digitais, aumentando, como dito acima, significativamente a ocorrência desses delitos.

Por crimes virtuais, entende-se que são aqueles cometidos por meio da informática em geral, contra um sistema, sendo atividades criminosas que se utilizam de aplicativos conectados a uma rede e, em geral, são cometidos com a intenção de obter vantagem financeira.

Somam-se aos crimes os riscos de navegação pela internet que colocam em jogo a perda ou diminuição desses novos valores informáticos, dentre eles tranquilidade para navegar, segurança para se fazer operações, nas plataformas digitais, integridade dos arquivos armazenados, confiabilidade na nuvem, garantia de fornecimento de serviço digital de provimento de acessos, possibilidade de acesso aos sistemas contratados, entre outros.

À vista disso, pode-se dizer que ninguém está totalmente imune de ter seu computador ou smartphone invadido, por programas inadequados, podendo ser utilizados para cometimento de fraudes, tanto contra pessoas jurídicas quanto contra pessoas físicas.

Nessa trilha, em que pese o isolamento social foi e é uma das medidas mais eficazes e eficientes para proteger a população e para conter o avanço da doença. Por conseguinte, é possível dizer que esse isolamento intensificou as fraudes e crimes perpetrados pela internet, principalmente, no tocante às fraudes bancárias.

Em outros termos, com a pandemia da Covid-19 e as medidas de distanciamento, para evitar aglomerações e conter a disseminação da doença, passou-se a utilizar muito mais os ambientes e serviços virtuais, com as instituições financeiras não foi diferente. No entanto muitas pessoas ainda não estavam preparadas para essa migração virtual tão rapidamente. É a partir daí que os criminosos virtuais começam a intensificar suas investidas criminosas.

Embora existam leis que protejam os usuários desse meio, e que as instituições financeiras estejam constantemente aperfeiçoando seus sistemas de segurança, os criminosos virtuais estão sempre criando formas alternativas para burlar os sistemas.

Enfim, parece ser possível afirmar, que o aumento dos crimes virtuais nas instituições é mais um dos problemas ocasionados pela pandemia, haja vista que houve uma adesão maior aos seus canais digitais, como forma de evitar aglomerações e conter o avanço da doença e, proporcionalmente, o aumento das condutas ilícitas virtuais.

A título de exemplo, relativamente ao complexo normativo protetivo do usuário da internet, cita-se o Marco Civil da Internet, Lei 12.965/2014, que trata dos direitos e deveres dos internautas, protegendo os dados pessoais e a privacidade dos usuários. (BRASIL, 2014).

Além dessa legislação denominada, há, também, a Lei 12.737/2012, conhecida como Lei Carolina Dieckmann que promoveu algumas alterações no Código Penal em seus artigos 154-A, 154-B, 266 e 298. Essa lei sofreu alterações recentemente pela Lei 14.155/21 que promoveu mudanças novamente no art. 154 A do CP, e passou a estabelecer que não é necessário que haja a violação de dispositivo de segurança, para a configuração do crime, condição que era prevista anteriormente, tornou as penalidades para os art. 155, §4º B e 4º C do CP; e art. 171 §2ºA, 2ºB, §4º do CP (fraude eletrônica e estelionato contra idosos) mais gravosas. Promoveu alterações no art. 70, §4º do CPP, estabelecendo novas regras relativamente à competência, passando para o domicílio da vítima, ou em caso mais vítimas, a competência será fixada pela prevenção. (BRASIL, 2012a; 2021a).

Ainda, no que diz respeito às legislações protetivas do usuário da internet, cita-se a Lei 12.735/12, que tipifica condutas realizadas mediante uso de sistema eletrônico, digitais ou similares que sejam praticadas contra sistemas informatizados, além disso, determina também a instalação de delegacias especializadas. (BRASIL, 2012b).

Todo esse aparato de leis visa à proteção dos cidadãos e promover a inibição da prática desses delitos cometidos, no ambiente virtual.

Dessa forma, torna-se relevante esta pesquisa diante de todo esse cenário que a sociedade está vivendo, dado que traz contribuições para a sociedade em geral, na medida em que elucida as práticas criminosas no meio digital contra os indivíduos; para operadores do Direito, por se tratar de um tema recente e que explicita sobre o tema, correlacionando com a pandemia vivenciada, ainda. Também faz-se relevante para acadêmicos não só do Curso de Direito, mas também de outras áreas.

Ante ao exposto, esta pesquisa tem como problema:: A Pandemia da Covid-19 é fator agravante para o aumento de casos de fraudes virtuais contra indivíduos que têm contas em instituição financeira, uma vez que houve aumento significativo de usuários nesse meio?

Como objetivo geral: analisar se Pandemia da Covid-19 é fator agravante para o aumento de casos de fraudes virtuais contra indivíduos que têm contas em instituição financeira, uma vez que houve aumento significativo de usuários nesse meio.

Foram traçados alguns objetivos específicos, quais sejam:

a) apresentar situações em que o Estado deve ser chamado a interferir com o *jus puniendi*, garantindo o direito a quem necessitar de sua tutela, aplicando a correspondente punição;

b) dissertar sobre o surgimento da internet, crimes virtuais e o Marco Civil da Internet;

c) apresentar aspectos gerais da relação dos crimes virtuais com o Direito Penal;

d) verificar os principais crimes cometidos nas Instituições Financeiras contra seus clientes, no período de Pandemia da Covid-19 e os principais obstáculos para a identificação e punição dos criminosos;

e) relacionar pandemia e crimes virtuais;

f) verificar mecanismos utilizados para a aplicação de fraudes eletrônicas bem como a qualificação desses crimes;

g) apresentar fatores que influenciaram no aumento das fraudes e crimes virtuais, durante o período da pandemia;

h) verificar as principais legislações do ordenamento jurídico brasileiro que servem de apoio ao combate contra os crimes virtuais e o alinhamento com o direito internacional; e

i) discorrer sobre mecanismos de educação digital que possam ser utilizados como forma de proteção;

Em relação à metodologia, esta pesquisa é de natureza exploratória, dado que tem como principal finalidade desenvolver, esclarecer e modificar conceitos e ideias, tendo em vista a formulação de problemas mais precisos ou hipóteses pesquisáveis, para estudos posteriores. De todos os tipos de pesquisa, essas são as que apresentam menor rigidez no planejamento. (GIL, 1995).

Quanto ao tipo de abordagem, classifica-se como qualitativa haja vista que segue uma rota similar às demais pesquisas, uma vez que necessita da escolha de um tema, assunto ou problema, uma coleta e análise de dados e informações e sua apresentação. (TRIVIÑOS, 1987, *apud* LEONEL; MARCOMIM, 2015).

No que se refere aos procedimentos de coleta de dados, trata-se de pesquisa bibliográfica e documental. Para Gil (1995, p. 50):

> A pesquisa bibliográfica é desenvolvida a partir de material já elaborado, constituído, principalmente, de livros e artigos científicos. Embora em quase todos os estudos seja exigido algum tipo de trabalho desta natureza, há pesquisas desenvolvidas exclusivamente a partir de fontes bibliográficas. Parte dos estudos exploratórios podem ser definidos como pesquisas bibliográficas, assim como certo número de pesquisas desenvolvidas a partir da técnica de análise de conteúdo.

Os materiais utilizados nesta pesquisa são compostos de acervos bibliográficos da área de Direito Penal, Informático, Direito Penal, artigos, teses, doutrinas que dissertam e suscitam estudos e análises sobre os Crimes Virtuais, no sistema bancário.

Gil (1995, p. 51) apresenta a pesquisa documental como semelhante à pesquisa bibliográfica. Acrescenta, ainda, que:

> A única diferença entre ambas está na natureza das fontes. Enquanto a pesquisa bibliográfica se utiliza fundamentalmente das contribuições dos diversos autores sobre determinado assunto, a pesquisa documental vale-se de materiais que não receberam ainda um tratamento analítico, ou que ainda podem ser reelaborados de acordo com os objetivos da pesquisa.

Em referência à estrutura, este trabalho está dividido em cinco capítulos. Neste capítulo, faz-se uma apresentação sobre o tema.

No segundo capítulo, discorre-se sobre histórico da internet e surgimento dos crimes virtuais, bem como alguns conceitos sobre instituição financeira; a lei considerada o Marco Civil da Internet, bem como alguns dados atualizados sobre os crimes virtuais no Brasil, demostrando uma visão geral acerca do tema desta pesquisa.

No terceiro capítulo, trata-se de crimes virtuais propriamente ditos e a sua relação com Direito Penal, tipos penais, condutas que caracterizam crimes, dificuldades das autoridades em investigar, obtenção de provas, competência para processar e julgar, ação penal, bem como alguns entraves, para punição e investigação dos criminosos.

No quarto capítulo, disserta-se sobre os crimes cometidos contra nas Instituições Financeiras contra seus clientes, no período de Pandemia da Covid-19, a relação entre pandemia e crimes virtuais, fraudes praticadas, utilizando as mídias sociais, mecanismos utilizados para a aplicação de fraudes eletrônicas, qualificação dos crimes praticados pela internet, no sistema do *internet banking*, dando enfoque ao estelionato virtual e furto mediante fraude, fatores que influenciaram no aumento das fraudes e crimes virtuais, durante o período da pandemia,

responsabilização dos agentes envolvidos, formas de prevenção e educação digital, bem como legislações nacionais aplicáveis à internet.

No quinto capítulo, apresenta-se a conclusão da pesquisa, em seguida, as referências.

Por fim, a pesquisa visa contribuir para aprimorar os saberes no campo jurídico fornecendo informações relevantes e precisas acerca do tema em epígrafe, mostrando as dificuldades na atualidade, contribuindo para futuros estudos, no âmbito jurídico, bem como servir de base para futuras pesquisas na área.

2 INTERNET E PANDEMIA

Este capítulo apresenta o histórico da internet, a internet no Brasil, o conceito de Instituição Financeira, o *internet banking*, o surgimento de crimes virtuais, o Marco Civil da Internet, dados atualizados sobre crimes virtuais no Brasil.

2.1 HISTÓRICO DA INTERNET

Leonard (2019, p. 10) define a internet "[...] como uma rede internacional de computadores, conectados entre si. Trata-se de um meio de comunicação que possibilita a troca de informações de toda natureza, mundialmente, com nível de interação jamais visto".

Foi por volta da década de 1950 que a internet surgiu, durante o período da Guerra Fria, mas somente na década de 1960, em que dois grupos ideológicos e contrários politicamente, liderados por duas superpotências à época: EUA e União Soviética já percebiam a eficácia e a necessidade vital dos meios de comunicação. EUA temendo ter suas informações sigilosas expostas idealizou um modelo de troca e compartilhamento de informações, com medo de um ataque nuclear, da então União Soviética, uma potência militar à época. (CORRÊA, 2002).

Em 1958, nos EUA, foi criada a DARPA (Defense Advanced Projects Agency), Agência de Projetos de Pesquisa Avançada de Defesa, com a finalidade de ser responsável por pesquisas e desenvolvimento de novas tecnologias com finalidade defensiva e militar.

Sendo assim, tornou-se necessária a criação de uma rede, e por volta de 1960, foi criada a ARPANET (Advanced Research Projects Agency), Agência de Pesquisa Avançada e Rede, e mais tarde, daria origem à internet, integrando muitos centros de pesquisa, alinhados com os EUA.

A ARPANET era um sistema de transmissão de dados em rede de computadores em que as informações eram divididas em pacotes, trechos de dados, endereço, destinatário e informações que permitiam a remontagem da mensagem original.

O tal ataque esperado pelos EUA, nunca se concretizou, mas sabiam os americanos que estavam dando o pontapé inicial para o maior fenômeno do século 20, único meio de comunicação a conseguir atingir uma grande escala de usuários, cerca de 50 milhões de pessoas.

E, posto isso, várias pequenas redes começaram a utilizar a tecnologia desenvolvida pela ARPANET. Neste sentido, nas palavras de Leonardi (2019, p. 22):

> E a internet continuou em constante evolução, a comunicação fora da ARPANET, já não era suficiente, foi criado então o protocolo TPC/IP, esses protocolos adicionam a cada pacote de dados o endereço dos destinatários para que eles alcancem seus destinos corretos.
> Em sua essência, A Internet funciona graças ao TPC/IP, acrônimo de Transmission Control Protocol/ Internet Protocol, o qual permite que diferentes computadores e dispositivos se comuniquem entre si, bastando, para tanto, que transmitam informações utilizando pacotes de dados.

Discorrendo sobre internet, faz se necessário explicar o que é um IP, conforme segue:

> [...] o IP, é o código único que identifica determinado computador conectado à Internet em determinado momento. Toda vez que um usuário se conecta à rede, seu computador recebe automaticamente de seu provedor de acessou m endereço IP que é único durante aquela conexão. Sem conhecer tal endereço, um pacote de dados não tem como chegar a seu destino. (LEONARDI, 2019, p. 10).

Para o direito digital, o IP constitui uma forma de identificação virtual. Isso significa que o anonimato na rede é relativo, assim como muitas identidades virtuais podem não ter um correspondente de identidade real. (PINHEIRO, 2021).

Nesta trilha, no início dos anos 1970 foi criado um *software* básico de *e-mail*, se tornando um dos aplicativos mais utilizados, pelo engenheiro Ray Tomlinson, aliás é dele a criação do caracter @ (arroba) que significa “at”, ou seja “em’, e o primeiro *e-mail* da história foi: tomlinson@bbn-tenexa. (CORRÊA, 2002).

Foi por volta dos anos 90 que a internet começou a atingir a população em geral, surgindo a WWW (World Wide Web), que significa “teia em todo mundo” ou rede de alcance mundial, sendo um sistema de distribuição de documentos de hipertexto (HTTP), conectados entre si e sendo acessados via navegador Web, conectados à internet. (CORRÊA, 2002).

A criação da gigante *Google* foi em 1997, outro marco na história da internet, levando a rede para um grande público, oferecendo serviços de navegação, sendo hoje um mecanismo de busca muito utilizado, com quase 1 Bilhão de páginas, oferecendo fácil acesso e informações gratuitas a grande número de pessoas.

Atualmente, as principais formas de transmissão e informações via internet são a *world wide web*, os mecanismos de busca (*Google, Bing, Yahoo*), as redes sociais (*facebook, Instagram, Twitter, Snapchat, Youtube, TikTok*), os serviços de mensagem (*WhatsApp, Telegram, Signail, Snapchat* e similares), o correio eletrônico (e-mail), voz sobre IP (*FaceTime, Skype, Hangouts, Blue Jeans*, aplicativos móveis em geral (App).

Em um planeta com aproximadamente 8 bilhões de pessoas, segundo dados da ONU, aproximadamente 4.66 bilhões (janeiro de 2021) utilizam a rede, sendo que este número

corresponde a mais de 50% da população mundial, ou seja, mais da metade da população mundial está *online* ou conectada de alguma forma. (NÚMERO..., 2020).

Contudo, infelizmente, é preciso registrar que a pandemia da Covid-19 marcou negativamente a vida no mundo. Com as mudanças nas rotinas, em função do isolamento social, passou-se a ficar mais dependentes da internet, seja para estudos, entretenimento, ou para acesso a serviços simples, o surto da doença provocou um impacto significativo, no número de usuários da internet, números que podem se tornar ainda mais expressivos.

2.2 A INTERNET NO BRASIL

A City University of New York (CUNY), em 1981, depois da realização de uma pesquisa entre universidades, decidiu "[...] montar uma rede que pudesse interligar pessoas de uma forma simples e barata, criando a Because It's Time Network (BITNET) que inicialmente conectou a CUNY com a Yale University". (CARVALHO, 2006, p. 50).

No Brasil, o processo de iniciação da internet ocorreu de forma lenta e gradativa, chegando por volta de 1988, por iniciativa da FAPESP (Fundação de Amparo à Pesquisa do Estado de São Paulo) e LNCC (Laboratório Nacional de Computação Científica).

Em 1988, foi realizado o primeiro acesso à BITNET, no Brasil, pelo LNCC, do Rio de Janeiro, estabelecendo uma conexão de 9600 bps através da Universidade de Maryland. (GUIZZO, 2002).

A exploração comercial da Internet foi iniciada em dezembro de 1994 pela Embratel, permitindo acesso à Internet, inicialmente, através de linhas discadas. Paralelamente a isso, a partir de abril de 1995 foi iniciada pela RNP (Rede Nacional de Pesquisas) um processo para implantação comercial da Internet no Brasil, com uma série de etapas, entre as quais a ampliação do backbone RNP no que se refere à velocidade e número de POP's, a fim de suportar o tráfego comercial de futuras redes conectadas a esses POP's; esse backbone a partir de então passou a se chamar Internet/BR. No mesmo ano, foi criado o Comitê Gestor Internet pelo Ministério das Comunicações, Ciência e Tecnologia, que tinha por objetivo a coordenação da implantação do acesso à Internet no Brasil. (INTERNET..., [2020?]).

Hoje, o Brasil com uma população estimada em 213,3 milhões de habitantes, segundo dados do IBGE (01/07/2021), registra cerca de 134 milhões de pessoas acessando a internet, o telefone celular é a principal ferramenta utilizada pelos conectados, sendo que nas residências com acesso à internet, ele foi encontrado em 99,5 % dos domicílios, logo após vem o

computador com 45,1%, depois a TV com 31,7% e os tablets com 12% dos acessos. (BRASIL, 2021).

Segundo o Ministério das Comunicações, são desenvolvidas importantes ações a fim de acabar com o deserto digital do país que atinge mais de 45 milhões de brasileiros. Ações como o Wi-Fi Brasil, Norte Conectado, Nordeste Conectado e Cidades Digitais contribuem para a evolução da conectividade em território nacional. Ainda, durante o ano de 2021, deve ocorrer o Leilão do 5G, que possui a finalidade de levar conectividade a todos os brasileiros. O edital prevê que até o fim de 2022 todas as capitais brasileiras tenham o 5G funcionando, e a tecnologia 4G chegar aos locais onde o acesso ainda é precário e inexistente, como escolas e postos de saúde. (BRASIL, 2021).

2.3 CONCEITO DE INSTITUIÇÃO FINANCEIRA

A Lei 4.595/64 que dispõe sobre a Política e as Instituições Monetárias, Bancárias e Creditícias traz em seu artigo 17 a definição de Instituição Financeira:

> Art. 17. Consideram-se instituições financeiras, para os efeitos da legislação em vigor, as pessoas jurídicas públicas ou privadas, que tenham como atividade principal ou acessória a coleta, intermediação ou aplicação de recursos financeiros próprios ou de terceiros, em moeda nacional ou estrangeira, e a custódia de valor de propriedade de terceiros.
> Parágrafo único. Para os efeitos desta lei e da legislação em vigor, equiparam-se às instituições financeiras as pessoas físicas que exerçam qualquer das atividades referidas neste artigo, de forma permanente ou eventual. (BRASIL, 1964).

As Instituições Financeiras são pessoas jurídicas públicas ou privadas que tem como atividade principal ou acessória a coleta, intermediação ou aplicação de recursos financeiros e a guarda desses valores.

Estas instituições desempenham um importante papel, fazendo a intermediação entre os agentes superavitários, ou seja, aqueles que possuem recursos para guardar, também chamados de poupadores e entre os agentes deficitários, aqueles que necessitam de empréstimos, também conhecidos como tomadores de recursos.

2.4 INTERNET BANKING

Por *Internet Banking* ou *home banking* ou banco *on-line*, entende-se os serviços ofertados pelas instituições financeiras aos clientes que desejam realizar operações bancárias por meio da Internet, sem a necessidade de estar presencialmente em uma agência bancária.

Trata-se de plataformas disponibilizadas pelas Instituições financeiras para que os clientes possam acessar à distância, ou seja, quase todas as transações que podem ser realizadas presencialmente, podem ser feitas de forma virtual, dentro dos limites de segurança estipulados por cada Instituição Financeira.

O cliente mediante autorização (senhas) e acesso à internet, realiza transações financeiras como: saldos, extratos, depósitos em cheque, transferências, pagamentos, abertura de contas pessoa física e pessoa Jurídica, através de dispositivos como computador, notebook, celulares, *tablets* sem precisar dirigir-se a uma agência bancária.

Para as instituições financeiras, a grande vantagem destes serviços se dá pela redução de custos, uma vez que diminui drasticamente o trânsito de clientes na agência, e consequentemente reduz a quantidade de funcionários contratados. Em contrapartida, os clientes ganham em comodidade, praticidade e tempo, uma vez que podem realizar suas operações financeiras de onde estiverem, sem se deslocarem a uma agência física.

O termo *internet banking* ou *home banking* (Banco *Online*) faz referência ao acesso bancário via computador ou notebook, enquanto os serviços prestados via dispositivo móvel (celulares, *tablets*, relógios), são conhecidos por mobile banking.

Neste sentido, ensina Pinheiro. (2021, p. 383):

> Segundo Adam Smith, um dos pais da economia, a principal fonte de riqueza, do crescimento e do desenvolvimento de um país provém da divisão e da especialização do trabalho e da invenção de máquinas que facilitem a mão de obra. Nesta busca, desenvolvemos tecnologias que possam permitir inclusive aprimorar o ganho de conhecimento.

Registre-se, ainda, a existência de aplicativos, que são programas desenvolvidos para serem utilizados em dispositivos móveis, alguns já vem nos próprios aparelhos, outros precisam ser baixados e, com as mais diversas finalidades: serviços, entretenimento, comunicação, informações em geral. A utilização de App significa ter acesso rapidamente a diversos serviços com praticidade e economia de tempo.

Essa era dos aplicativos teve impulso maior com a Pandemia da Covid-19, em que milhões de pessoas em função das medidas de distanciamento, para evitar aglomerações e conter a disseminação da doença passaram a utilizar muito mais destes canais.

2.5 SURGIMENTO DOS CRIMES VIRTUAIS

Com o crescimento da internet acontecendo muito rapidamente, e dos inúmeros benefícios e facilidades oferecidos pelo meio digital, proporcionalmente surgiram ameaças, crimes cometidos por pessoas com ou sem conhecimento tecnológico, através da rede.

"A internet é rica, e onde há riqueza existe crime". (NERY; BITTENCOURT; AZAMBUJA, 2013, *apud* JESUS; MILAGRE, 2016 p. 1).

Sabe-se que hoje é praticamente impossível viver sem internet e que ela é um instrumento importante de interação, comunicação, além de muita influência no dia a dia das pessoas, e como consequência, surgem os crimes virtuais, que se utilizam desse meio para propagarem-se.

Quanto mais crescem os equipamentos conectados à rede, mais possibilidades de ataques, cresce proporcionalmente a criminalidade.

Neste meio, com criminosos influenciados pelo anonimato e as dificuldades de investigação que o mundo digital apresenta, se aproveitam da rapidez com que as informações se fundem para praticar infrações contra instituições e pessoas.

A doutrina diverge acerca do primeiro delito virtual cometido, aduzindo que:

> Para alguns, o primeiro delito teria ocorrido no âmbito do MIT (Massachusetts Institute of Technology), no ano de 1964, onde um aluno de 18 anos teria cometido um ato classificado como cibercrime, tendo sido advertido pelos superiores. Outros ainda referenciam o primeiro caso de que se tem notícia sobre hacking no ano de 1978, na Universidade de Oxford, onde um estudante copiou de uma rede de computadores uma prova. Uma invasão seguida de uma cópia. Até essa data não existia lei sobre crimes informáticos nos EUA. A Florida, no mesmo ano, foi o primeiro Estado americano a formular leis sobre informática. (JESUS; MILAGRE, 2016, p. 22-23).

Outro relato de fraude virtual aconteceu no ano de 1973, quando John Draper, um programador norte americano, conhecido como *hacker* da telefonia, usou um apito plástico para produzir o tom de 2600 Hz, capaz de enganar o sistema de telefonia americano, fazendo ligações gratuitamente, em razão do fato, foi preso por 5 anos e condenado por fraude.

As condutas mais comuns nesta época eram disseminação de vírus, invasão de sistemas, pirataria e pornografia infantil.

No ano de 1976, existem relatos da primeira iniciativa internacional sobre o cibercrime, a conferência sobre Aspectos Criminológicos do Crime Econômico, ocorrida no Conselho da Europa, em Estrasburgo.

Em 1990, Kevin Mitnick, um dos hackers mais famosos da história, ganhou notoriedade ao invadir sistema de diversas empresas, furtando senhas, copiando softwares, visualizando e-mail particulares. Foi condenado e preso por 5 anos.

No Brasil, há relatos de que os crimes virtuais começaram a surgir por volta de 1996, quando foram descobertas diversas invasões de sites ligados ao governo, como por exemplo o site do STF e a partir daí os delitos virtuais passaram a ser conhecidos. (MEDEIROS, 2015).

No Brasil, consta os primeiros crimes envolvendo *phishing scam* bancário (pescaria de senhas) por volta de 1999. Ações criminosas como pirataria de programas de informática, manipulação de dados bancários, pornografia infantil a abuso nas telecomunicações começaram a surgir.

Assim sendo, verifica-se que os delitos virtuais permeiam no Brasil há aproximadamente duas décadas e cabe ao direito acompanhar e proteger os indivíduos que tem seus bens jurídicos lesados, aplicando a legislação vigente, o direito deve acompanhar tais transformações, regulando as relações interpessoais da vida em sociedade.

2.6 MARCO CIVIL DA INTERNET

Finalizando esse tópico, é preciso, antes de adentrar nos crimes pela internet, apresentar algumas leis importantes ao tema, a começar pela Lei 12.965/14, conhecida como Marco Civil da Internet, considerada a "Constituição da Internet", já que estabelece princípios, garantias, direitos e deveres dos usuários, provedores e serviços, em geral, da internet, no Brasil, bem como orientações necessárias onde o Estado pode intervir.

"Art. 1º Esta Lei estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria". (BRASIL, 2014).

A lei em questão regulamenta o direito comunicativo na era digital, especialmente na internet, trata dos direitos e deveres dos internautas, protegendo os dados pessoais e a privacidade dos usuários. Esta lei é integrada às demais leis e complementar nas atividades que envolve o combate aos crimes virtuais.

A Lei do Marco Civil da Internet tem como um dos seus princípios a proteção da privacidade:

> Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:
> I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;
> II - proteção da privacidade;
> III - proteção dos dados pessoais, na forma da lei;
> IV - preservação e garantia da neutralidade de rede;
> V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;
> VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei;

> VII - preservação da natureza participativa da rede;
> VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei.
> Parágrafo único. Os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte.
> (BRASIL, 2014).

Vale destacar que é muito difícil alcançar a proteção da intimidade e a privacidade, sendo que muitas informações pessoais estão disponíveis na rede, seja por vontade própria, seja como condição para uso da internet.

Neste compasso, em termos de privacidade, é preciso trazer à baila um dispositivo de grande importância previsto na Constituição Federal, qual seja, o art. 5º, inciso X, que assim estabelece:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> [...] X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação.
> (BRASIL, 1988).

Ainda, quanto à Lei do Marco Civil, é preciso lembrar que a referida lei não exclui outros princípios previstos no ordenamento jurídico ou em tratados internacionais.

Ademais, o Marco Civil da Internet fomenta no Brasil os direitos comunicativos à medida que considera a Internet como ferramenta essencial para a liberdade da expressão e o exercício da cidadania, bem como para a promoção da cultura e o desenvolvimento tecnológico. Isso demonstra que o acesso à Internet tem ligação direta com o tema dos direitos humanos, eis que auxilia na concretização do direito à liberdade de expressão e no exercício da cidadania. (MENDES, 2021).

Bem como mencionado nos termos do art. 7º do Marco Civil da Internet, Lei 12.965/2014, o acesso à internet é essencial para o exercício da cidadania.

In verbis:

> Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
> I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;
> II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;
> III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;
> IV - não suspensão da conexão à internet, salvo por débito diretamente decorrente de sua utilização;
> V - manutenção da qualidade contratada da conexão à internet;

> VI - informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade;
> VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;
> VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:
> a) justifiquem sua coleta;
> b) não sejam vedadas pela legislação; e
> c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;
> IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;
> X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei;
> XI - publicidade e clareza de eventuais políticas de uso dos provedores de conexão à internet e de aplicações de internet;
> XII - acessibilidade, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, nos termos da lei; e
> XIII - aplicação das normas de proteção e defesa do consumidor nas relações de consumo realizadas na internet.
> (BRASIL, 2014).

Outro ponto importante que merece ser mencionado pela lei, refere-se à neutralidade, de forma que fique proibido às operadoras, a venda de pacotes de internet, além disso, não é permitido criar entraves para determinados conteúdo em troca de vantagem econômica, ou seja, o tráfego de qualquer dado deve ser com a mesma velocidade e qualidade, não podendo priorizar um ou outro. Esta distinção pode ocorrer somente nos casos em que seja indispensável para a prestação do serviço ou para emergências.

No ponto, colhe-se da lei em questão:

> Art. 9º O responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação.
> § 1º A discriminação ou degradação do tráfego será regulamentada nos termos das atribuições privativas do Presidente da República previstas no inciso IV do art. 84 da Constituição Federal, para a fiel execução desta Lei, ouvidos o Comitê Gestor da Internet e a Agência Nacional de Telecomunicações, e somente poderá decorrer de:
> I - requisitos técnicos indispensáveis à prestação adequada dos serviços e aplicações; e
> II - priorização de serviços de emergência.
> § 2º Na hipótese de discriminação ou degradação do tráfego prevista no § 1º, o responsável mencionado no caput deve:
> I - abster-se de causar dano aos usuários, na forma do art. 927 da Lei nº 10.406, de 10 de janeiro de 2002 - Código Civil;
> II - agir com proporcionalidade, transparência e isonomia;
> III - informar previamente de modo transparente, claro e suficientemente descritivo aos seus usuários sobre as práticas de gerenciamento e mitigação de tráfego adotadas, inclusive as relacionadas à segurança da rede; e

> IV - oferecer serviços em condições comerciais não discriminatórias e abster-se de praticar condutas anticoncorrenciais.
> § 3º Na provisão de conexão à internet, onerosa ou gratuita, bem como na transmissão, comutação ou roteamento, é vedado bloquear, monitorar, filtrar ou analisar o conteúdo dos pacotes de dados, respeitado o disposto neste artigo.
> (BRASIL, 2014).

No que tange à responsabilidade, os provedores deixam de ser responsabilizados pelos conteúdos gerados por terceiros e não poderão retirá-los do ar sem determinação judicial, exceto casos de nudez ou atos sexuais de caráter privado. Assim a lei corrobora:

> Art. 21. O provedor de aplicações de internet que disponibilize conteúdo gerado por terceiros será responsabilizado subsidiariamente pela violação da intimidade decorrente da divulgação, sem autorização de seus participantes, de imagens, de vídeos ou de outros materiais contendo cenas de nudez ou de atos sexuais de caráter privado quando, após o recebimento de notificação pelo participante ou seu representante legal, deixar de promover, de forma diligente, no âmbito e nos limites técnicos do seu serviço, a indisponibilização desse conteúdo.
> (BRASIL, 2014).

Por fim, é preciso estabelecer que a lei foi um importante regulador do uso da internet e dos conteúdos que nela poderão ser veiculados, quanto à regulamentação de direitos, garantias e deveres dos seus usuários, provedores e poder público, mas ainda é tímida em relação à solução de conflitos.

Além disso, não se olvide que as normas jurídicas devem estar constantemente em evolução para que possam acompanhar as mudanças proporcionadas pelo uso da tecnologia.

2.7 DADOS SOBRE CRIMES VIRTUAIS NO BRASIL

Antes mesmo da pandemia da Covid-19, o Brasil ocupava o terceiro lugar mundial em fraudes cometidas virtualmente, segundo pesquisa realizada pela Experian, líder mundial do segmento de serviços de Informações e marketing, intitulada de “2019 Global Identity and Fraud Report” (Pesquisa Global de Identidade e Fraude), ficando atrás somente de gigantes como os EUA e Reino Unido.

No ano de 2020, os crimes virtuais cresceram consideravelmente, de acordo com a *Fortinet Threat Intelligence Insider Latin America*, líder global em segurança de rede, de janeiro a setembro de 2020, o Brasil sofreu mais de 3,4 bilhões de tentativas de ataques na internet. Já a Interpol, durante os meses de janeiro a abril de 2020, detectou mais de 907 mil spams, 737 incidentes relacionados a softwares maliciosos (*malwares*) e 48 mil links suspeitos. (CRESCIMENTO..., 2021).

Dentre os golpes mais praticados que aconteceram durante a pandemia da Covid-19 estão os golpes envolvendo *phishing*, cartões de crédito clonados, boletos bancários fraudados, *WhatsApp* clonado, falso funcionário, falsa central telefônica, golpe do *motoboy* e auxílio emergencial falso, conforme Febraban – Federação Nacional dos Bancos. (CONHEÇA..., 2020).

2.8 CONCEITO DE PANDEMIA

Segundo a OMS (Organização Mundial de Saúde), pandemia é a disseminação de uma nova doença, e o termo passa a ser usado quando uma Epidemia (surto) que afeta uma região, se espalha por diferentes continentes com transmissão sustentada de pessoa para pessoa. (BRASIL, 2021c).

Para a epidemiologia, é a área que estuda como doenças afetam populações humanas, é uma epidemia que se origina em um ponto específico do globo e se propaga através dos continentes ao longo do tempo. Significa algo que afeta a todos de uma forma geral.

A OMS classifica uma Pandemia através de algumas etapas;

- Começam com a infecção de humanos por um vírus;
- Espalham-se para as populações locais, se fixando em uma região;
- Propagam-se por vários pontos no mundo por viagens e movimentos da população;
- Finalizam numa transmissão comunitária, ou seja, quando a população de uma mesma região como a se transmitir uma doença.

Em 2020, entretanto, o mundo foi obrigado a parar. “Para evitar que os mais frágeis perecessem, todos se isolaram. Os danos à economia serão nefastos. Nem sequer se consegue mensurá-los neste momento. Embora a perda seja reconhecida, a escolha foi a de salvas vidas. Uma opção consciente”. (NEVES, 2020, p. 12).

A melhor forma de se prevenir contra doenças infecciosas é através da vacina. O indivíduo que se vacina não está cuidando apenas de si, mas da saúde coletiva em geral.

Quanto mais pessoas se vacinam, mais chance de se acabar com a circulação do vírus, evitando a propagação da doença, mais vidas se preservam, e mais chance de retornar à normalidade.

Naturalmente o tema da pandemia domina nossos pensamentos e nossas mentes. Não imaginava que o mundo pudesse parar. A perplexidade avança para compreender como será o amanhã. Afinal, como essa dramática experiência afetará nossas vidas? Passado o isolamento,

controlada a disseminação da doença, nosso dia a dia voltará ao “normal”? Ou ainda: o que será o normal? (NEVES, 2020, p. 13).

O tema Pandemia ainda nos causa muitas incertezas, muita estranheza, como bem nos cita o autor, apesar de o ser humano ter uma capacidade incrível de adaptação, não se sabe como será o amanhã.

Na sequência, no próximo capítulo, serão abordados os crimes virtuais propriamente ditos.

3 DOS CRIMES VIRTUAIS

Neste capítulo, disserta-se sobre conceito jurídico de crimes virtuais, a elação entre o Direito Penal e o Direito Digital, tipicidade penal e classificações dos crimes virtuais, sujeito ativo e passivo dos crimes virtuais, condutas que se caracterizam crimes, valor probatório das provas digitais, competência para processar e julgar e sobre a ação penal.

3.1 CONCEITO JURÍDICO DOS CRIMES VIRTUAIS

Crimes virtuais, crimes cibernéticos, crimes de informática, crimes eletrônicos ou digitais, diversas são as nomenclaturas para nominar os delitos praticados por meio da rede mundial de computadores.

Conceitua-se crime informático como o fato típico e antijurídico cometido por meio da ou contra a tecnologia da informação. Decorre, pois, do direito informático, que é o conjunto de princípios, normas e entendimentos jurídicos oriundos da atividade informática. Assim é um ato típico e antijurídico, cometido através da informática em geral, ou contra um sistema, dispositivo informático ou rede de computadores. Em verdade, pode afirmar que, no crime informático, a informática ou é o bem ofendido ou o meio para a ofensa a bens já protegidos pelo Direito Pena. (JESUS; MILAGRE, 2016).

Para Bittencourt (2020, p. 6):

> Cibercrimes são todas as ações tipificadas criminalmente realizadas por meio eletrônico e que seus efeitos podem ser sentidos tanto no mundo digital quanto no mundo real. Nesse sentido, podemos afirmar que um crime digital é uma ação de natureza humana, cujos efeitos estendem-se além do meio eletrônico, causando algum tipo de prejuízo às pessoas, a grupos e/ou instituições. Tais prejuízos não se limitam somente ao financeiro, sendo possível repercutir na esfera física e/ou psicológica contra os respectivos alvos da ilicitude praticada, essas condutas terão seus efeitos estendidos ao mundo real.

Pode-se afirmar que informática é a ciência dedicada ao tratamento da informação mediante o uso de computadores e demais dispositivos de processamento de dados. E, neste sentido, a boa prática impõe que os tipos sejam dominados de acordo com o bem jurídico que visam proteger (JESUS; MILAGRE, 2016)

São delitos que dispensam a presença física do ofensor, dispensa contatos diretos com a vítima, planejamento e força, ocorrem não raro a partir de uma ação contra uma multiplicidade de pessoas (crimes de um contra muitos e de alastramento rápido) e não respeitam lógica e

estilo, sendo alvo pois de constantes modificações em suas táticas e ardis. (SYDOW, 2021, p. 644).

À vista disso, tem-se por crime virtual, a prática criminosa ligada a qualquer ação ilícita que utilize tecnologia de informática, são condutas de acesso a sistemas de informática não permitidas, como alteração de dados, fraudes bancárias, atos de terrorismo, pornografia infantil, entre outros.

Podem ser definidos como condutas ilegais praticadas através do uso de equipamentos eletrônicos como computadores, *smarthphones*, *tablets*, que estejam interligados com a rede mundial de computadores, infrações penais realizadas no âmbito virtual ou que estejam ligadas com informação digital.

3.2 RELAÇÃO ENTRE O DIREITO DIGITAL E O DIREITO PENAL

O Estado deve acompanhar as mudanças da sociedade para manutenção da ordem, bem como para estimular seu crescimento.

Na contextualização do Estado democrático de Direito, o Estado tem como principal função organizar e manter a sociedade edificada sobre os valores da justiça, liberdade, solidariedade, respeito aos direitos humanos e garantias fundamentais.

Por sua vez, o Direito Penal visa proteger o bem jurídico, punindo quem os tenha violado, através da prática de condutas ilícitas.

O direito Penal é um dos ramos do direito, essenciais para regular a vida em sociedade, dado que seu principal objetivo, é, regulamentar o poder punitivo do Estado através de seu conjunto de normas, que definem quais condutas são admissíveis, o que caracteriza crimes, e estabelece as punições aplicáveis. E uma de suas principais funções é proteger o bem jurídico.

Nesse sentido entende-se como bem jurídico aquilo que é importante para a o indivíduo e para a sociedade, a ponto de precisar de proteção jurídica, como por exemplo a vida, a integridade física, a propriedade, entre outros.

A noção de bem jurídico está ligada à conjuntura em que se encontra determinada sociedade, visto que cada uma delas apresenta demandas distintas, resultando em uma tutela diferenciada. Em vista disso, os valores sociais se modificam a medida em que passam as gerações, que trazem consigo novos pensamentos e ideais, de modo a alterar substancialmente aquilo que é tido como essencial e passível de tutela pelo Direito Penal. (PRADO, 2011).

As relações jurídicas resultantes das relações virtuais nos mostram a cada dia a substituição do meio físico pelo meio digital, surgindo, conseguintemente, essa nova necessidade: o Direito Digital.

A ordem jurídica brasileira que versa sobre as relações virtuais ou digitais englobam um conjunto de leis que serão aplicadas separadamente.

Esse ramo do direito é relativamente novo, se comparado aos demais ramos do direito, utilizando-se princípios e regras já existentes e que eram aplicáveis a outras áreas do direito, criando leis e institutos aplicáveis a ele especificamente.

O Direito digital é um ramo do direito que trata de todo o aparato de normas e regras, que regulam as relações virtuais como forma de oferecer maior segurança aos usuários deste meio. Vem para estabelecer Leis e garantias, para que os cidadãos, não sejam lesados, enquanto utilizam do espaço virtual.

Seguem algumas leis são aplicáveis aos crimes virtuais no Brasil:

- Lei Marco Civil da Internet;
- Lei 12737/2012 – Lei Crimes informáticos (Carolina Dieckmann)
- Lei 12735/2012 (Tipificação de condutas no sistema eletrônico)
- Lei 14155/2021
- Lei Proteção Geral de Dados;
- CPC (normas para o processo eletrônico)
- Código Penal Brasileiro
- Decreto 10222/ 2020
- Convenção de Budapeste

Algumas dessas leis e tratados serão abordadas mais adiante em capítulo próprio.

3.3 TIPICIDADE PENAL E CLASSIFICAÇÕES DOS CRIMES VIRTUAIS

Tipo penal é um modelo de conduta previsto em lei, com a finalidade de estabelecer padrões incriminadores, fixar alternativas de ilicitude e estabelecer parâmetros obrigacionais. Existem tipos penais incriminadores, ou seja, modelos de condutas proibidas, fixando uma pena (ex. art. 171, CP, estelionato), que têm a função de delimitar o que é penalmente ilícito e o que é penalmente irrelevante. (NUCCI, 2019).

É a adequação de um ato com características que o enquadram à norma relatada na Lei Penal como crime, encontrando amparo no Código Penal, sendo que o fato é considerado típico quando se enquadra na descrição legal de um crime, apresentando todos os seus elementos.

Para Nucci (2019, p. 309):

> Trata-se da adequação do fato ao tipo penal. A tipicidade é o fenômeno representado pela congruência entre o fato ocorrido no mundo real e o fato previsto no mundo abstrato das normas. Exemplo: quando A mata B(fato), o operador do direito elabora o juízo da tipicidade, ou seja, promove a adequação desse fato ao modelo de conduta previsto no art. 121 do Código Penal (matar alguém).

O tipo penal é uma das premissas básicas do princípio da Legalidade ou da Reserva legal: alguém só está obrigado a fazer ou deixar de fazer algo em virtude da Lei.

O princípio da legalidade se manifesta no artigo 1º, do Código Penal brasileiro, em que menciona "não há crime sem lei anterior que o defina, nem há pena sem prévia cominação legal". (BRASIL, 1940).

Frise-se que a Constituição Federal, afirma esse princípio em seu artigo 5º, XXXIX, dispõe:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> [...] XXXIX - não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal;
> (BRASIL, 1988).

Outrossim, significa que o indivíduo só poderá ser punido, caso haja Lei, anteriormente ao ato praticado, considerando a conduta praticada como delituosa. O indivíduo será punido somente se a conduta for configurada como crime e com a respectiva sanção.

No que concerne às classificações,

> [...] muitos doutrinadores procuram classificar os crimes digitais. No que tange à nomenclatura, referem-se às "infrações cometidas por meio de computador". Há ainda quem prefira a expressão crimes de computador, cybercrimes, computer crimes, delito informático, crimes virtuais, crimes eletrônicos, ou ainda, crimes digitais, crimes cibernéticos, infocrimes, crimes perpetrados pela internet, denominações distintas, mas, que, no fundo, acabam por significar basicamente a mesma coisa. (ROSA, 2007, p. 53).

A expressão crimes virtuais é toda ação típica, antijurídica e culpável, contra ou através de processamento eletrônico de dados ou através de sua transmissão, ou seja, através do sistema de informática, para violar um bem juridicamente protegido.

Conforme a visão do doutrinador sobre a criminalidade informática, há determinadas classificações, dentre as mais conhecidas e comuns há alguns tipos de classificações diferentes, Jesus e Milagre (2016) apresentam as seguintes:

- Manipulações, espionagem, sabotagem e furto de tempo;

- Violação à privacidade, crimes econômicos (*hacking*, espionagem, pirataria em geral, sabotagem e extorsão, fraude), conteúdos ilegais e nocivos, outros ilícitos: contra a vida, crime organizado, guerra eletrônica;

- Manipulação de dados; acesso a dados não autorizados; introdução de programas para destruição de dados, informações ou programas; utilização de programas com a finalidade de obter vantagem financeira; utilização de computadores com fins fraudulentos; agressão à privacidade mediante à utilização de dados pessoais não autorizados.

- Infrações à intimidade, ilícitos econômicos, ilícitos de comunicação ou divulgação de conteúdos ilegais ou perigosos, e outros delitos.

- Manipulação, falsificação e deterioração de dados ou programas; divulgação, utilização ou reprodução ilícita de dados e programas; uso e acesso não autorizado à sistemas de informática.

A classificação mais precisa tem semelhança com esta última mencionada.

Para Jesus e Milagre (2016, p. 52):

> Diga-se, a distinção entre crimes informáticos em que a informática é o meio para a prática de velhos crimes ou agressão a bem jurídico protegido pelo Direito Penal, e crimes informáticos em que a informática (inviolabilidade dos dados) é o bem jurídico protegido, propriamente dito. Estas classificações podem se fundir, como por exemplo, no delito em que um bem jurídico informático é agredido para que o agente possa cometer o crime-fim, diga-se, agredir outro bem jurídico, ou mesmo no caso em que da agressão ao bem jurídico outros bens também são afetados, ainda que não informáticos.

Dessa forma, Jesus e Milagre (2016, p. 52-53) classificam os crimes informáticos da seguinte forma:

Crimes informáticos próprios: em que o bem jurídico protegido é a tecnologia da informação em si. Para estes delitos, a legislação penal era lacunosa, sendo que, diante do princípio da reserva legal penal, muitas práticas não poderiam ser enquadradas criminalmente;

Crimes Informáticos impróprios: em que a tecnologia da informação é o meio utilizado para a agressão a bens jurídicos já protegidos pelo Código Penal Brasileiro. Para estes delitos, a legislação criminal é suficiente, já que grande parte das realizadas encontra correspondências em alguns dos tipos penais;

Crimes informáticos mistos: são crimes complexos em que, além da proteção do bem jurídico informático (inviolabilidade dos dados), a legislação protege outro bem jurídico. Ocorre a existência de dois tipos penais distintos, cada qual protegendo um bem jurídico;

Crime informático mediato ou indireto: trata-se do delito informático praticado para a ocorrência de um delito não informático consumado ao final. Em direito informático, comumente um delito informático é cometido como meio para a prática de um delito-fim de ordem patrimonial. Como por exemplo, no caso do agente que captura dados bancários e usa para desfalcar a conta corrente da vítima. Pelo princípio da consumação, o agente só será punido pelo delito-fim (furto).

Importante ressaltar as definições de Crespo (2011, p. 63), acerca dos crimes informáticos: "A simples perpetração de um delito como um estelionato não deveria ser, repita-se, com precisão técnica, considerada um crime informático".

Ocorre que, não só para doutrinadores, mas para as mídias em geral, ficou convencionado nomear de crime virtual qualquer conduta delitiva praticada com uso da tecnologia, sendo ela o instrumento da conduta ou objeto do ilícito, ou seja, o meio para prática do delito ou o delito- fim.

3.4 SUJEITO ATIVO E PASSIVO DOS CRIMES VIRTUAIS

3.4.1 Sujeito Ativo

Proporcionalmente aos bônus surgidos com a Internet, também vieram os ônus, isto significa que juntamente com os benefícios ora proporcionados aos usuários da rede, também aparecem condutas ilícitas praticadas neste meio.

Entende-se por sujeito ativo aquele que comete a conduta criminosa, *i. e.*, o que comete o ilícito penal. É muito comum os sujeitos ativos dos ilícitos virtuais serem chamados de hackers, o que não procede.

Muitos utilizam o termo *Hacker*, para se referirem ao criminoso digital. Explica-se a expressão *hacking* é o uso não autorizado do computador e de seus recursos de rede. O termo *hacker* originariamente significava um habilidoso programador, recentemente, com o fácil acesso a múltiplos sistemas, passa a ter uma conotação negativa. Essa conduta havida por alguns como inofensiva, vez que há hackers que acessam a sistemas apenas pelo desafio, pode ser comparada com a entrada de um estranho na sua casa, que a tudo olha, toca e depois sai. Não se pode consentir com esta cultura. (LIMA *apud* JESUS; MILAGRE, 2016).

Equivoca-se quem pensa que os delitos virtuais são praticados única e exclusivamente por especialistas em informática, já que com a crescente evolução dos meios de comunicação, dos equipamentos, da tecnologia e, principalmente, do acesso aos sistemas disponíveis, qualquer pessoa pode se tornar um criminoso virtual.

Na verdade qualquer pessoa pode ser o sujeito ativo nos crimes virtuais e cometer um delito, no mundo virtual.

Os *hackers* são pessoas com conhecimentos ímpares dos sistemas de informática, e isso não significa que usarão suas habilidades para fins ilícitos. São programadores dotados de grande conhecimento sobre tecnologia e internet, desprovidos de intenções criminosas, podendo ou não utilizar para este fim.

Enquanto os crackers, o termo deriva do inglês *to crack,* que significa quebrar, praticam quebras de sistemas de segurança, senhas, códigos de criptografia, ilegalmente, com a finalidade exclusiva para fins criminosos. (MEDEIROS, 2020).

Neste âmbito, seguem algumas classificações, segundo Crespo (2011, p. 95) para denominar os responsáveis por condutas ilícitas, reforçando que nem sempre os *hackers* são os vilões da internet:

- *Hacker*s: Fuçador. Expressão que surgiu nos laboratórios do MIT (Massachusetts Institute of Tecnology). Qualquer um que tenha um grande conhecimento sobre tecnologia e que faça invasões.

- *Carders*: Estelionatários especializados em fraudes com cartões.

- Crackers: Seriam os verdadeiros criminosos da rede. Utilizam seus conhecimentos de tecnologia para más finalidades.

- *Phreakers*: São os Hackers da telefonia, capazes de realizar interceptações, paralisar serviços e até mesmo utilizar a telefonia em nome de terceiros.

- *Lammers* e *Wannables*: Os que não possuem conhecimentos em informática e pensam que tem. Sobre o prisma de uma defesa criminal, demonstrar que o cliente é *Lammer* tem o seu sentido, pois poderia ser importante prova a atestar a ausência de autoria de um crime informático, como a invasão, por exemplo.

3.4.2 Sujeito passivo

O sujeito passivo é todo aquele que sofre a ofensa, refere-se ao sujeito lesado pela ação criminosa, podendo ser ele, um indivíduo ou uma pessoa jurídica, desde que possuam patrimônio, que possam ser desviados, deteriorados, ter suas informações usurpadas ou lesado de alguma outra forma.

Sobre o sujeito passivo, para Rosa (2006, p. 63):

> [...] é o ente sobre o qual recai a ação ou omissão realizada pelo sujeito ativo. É a pessoa ou entidade titular do bem jurídico tutelado pelo legislador e sobre a qual recai a conduta do sujeito ativo. De qualquer modo, o sujeito passivo dos crimes de informática pode ser qualquer pessoa, física ou jurídica, de natureza pública ou privada.

Sendo assim, o sujeito passivo é todo aquele que sofre a ofensa, o sujeito lesado pela ação criminosa, podendo ser ele, um indivíduo ou uma pessoa jurídica, desde que possuam patrimônio, que possam ser desviados, deteriorados, ter suas informações usurpadas ou lesado de alguma outra forma.

É muito mais fácil identificar o sujeito passivo do ilícito penal, uma vez que qualquer pessoa pode ser vítima de um delito virtual.

Segundo Rosa (2006, p. 63), “A maioria desses delitos nem chega ao conhecimento das autoridades, em virtude das empresas ou Instituições Financeiras não desejarem expor suas fragilidades ou falhas em relação à segurança de seus sistemas e perderem sua credibilidade”.

Ocorre que com esta omissão em relação as denúncias desses delitos, acabam por facilitar o aumento desses crimes.

3.5 CONDUTAS QUE CARACTERIZAM CRIMES

Comportamentos (ou condutas) são relacionados a potenciais crimes próprios, em que a informática é o bem jurídico agredido. Logicamente, crimes que ofendem outros bens jurídicos, e que podem ser realizados por intermédio da informática, como, por exemplo, encartados nos delitos de pornografia infantil, contrafação, pirataria de software, a ameaça, a injúria, dentre outros. Para estes, é suficientemente claro. (JESUS; MILAGRE, 2016).

São elencados a seguir, os principais comportamentos, que poderão ou não ser considerados crimes, variando conforme ordem jurídica em matéria de informática vigente no país:

- Acesso Ilegítimo: conduta daquele que ilegalmente acessa um sistema de informática sem ter autorização ou se mantenha sem autorização expressa ou tácita de quem tenha o direito

de exclui-la. Trata-se do acesso sem permissão, não necessariamente violando medidas de segurança. No Brasil, com a lei 12.737/2012, o acesso ilegítimo ganhou status de tipo penal, mas necessitava que houvesse a violação de dispositivo de segurança, caso contrário não configuraria crime. A recente lei 14.155, de 27/05/2021, alterou novamente o artigo, tornando o crime de invasão de dispositivo mais gravoso.

> Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita: (Redação dada pela Lei nº 14.155, de 2021)
> Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa. (Redação dada pela Lei nº 14.155, de 2021)
> § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput. (Incluído pela Lei nº 12.737, de 2012) Vigência
> § 2º Aumenta-se a pena de 1/3 (um terço) a 2/3 (dois terços) se da invasão resulta prejuízo econômico. (Redação dada pela Lei nº 14.155, de 2021)
> § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido: (Incluído pela Lei nº 12.737, de 2012) Vigência
> Pena – reclusão, de 2 (dois) a 5 (cinco) anos, e multa. (Redação dada pela Lei nº 14.155, de 2021)
> § 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos. (Incluído pela Lei nº 12.737, de 2012) Vigência
> § 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra: (Incluído pela Lei nº 12.737, de 2012) Vigência
> I - Presidente da República, governadores e prefeitos; (Incluído pela Lei nº 12.737, de 2012) Vigência
> II - Presidente do Supremo Tribunal Federal; (Incluído pela Lei nº 12.737, de 2012) Vigência
> III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou (Incluído pela Lei nº 12.737, de 2012) Vigência
> IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal. (Incluído pela Lei nº 12.737, de 2012).
> (BRASIL, 2021a).

A nova lei 14155/21 trouxe outras alterações para o tipo penal, como majoramento da pena (pena de 1 a 4 amos), forma qualificada (passando a pena para reclusão de 2 a 5 anos) e retirada da previsão de subsidiariedade expressa (se a conduta não constitui crime mais grave).

- *Interceptação Ilegítima*: São condutas relacionadas ao uso de meios técnicos, em transmissões não públicas, para interceptação, captura de dados e informações. Essas condutas podem ser puníveis pela Lei 9.296/96, artigo 10. (BRASIL, 1996a).

- *Interferência de Dados (Dano Informático):* São condutas dolosas praticadas com o intuito de danificar, apagar, deteriorar, alterar ou suprimir dados informáticos ou sistemas. Se

o agente não invade, apenas provoca o dano, são puníveis com art. 163, do Código Penal. da invasão resultar dano.

- *Interferência em sistema:* Condutas dolosas, com o objetivo de causar obstrução grave, intencional e ilegítima aos sistemas de informática, através da introdução, danificação, eliminação, deterioração, ou supressão de dados informáticos. A tipificação deste delito está no art. 266, do Código Penal, também sofreu alteração com a Lei 12.737/12.

- *Uso abusivo de dispositivos*: refere-se à conduta de produzir, vender, obter, utilizar, importar ou distribuir dispositivos ou programa de informática para prática de outras condutas criminosas ou senhas, código de acessos e dados informáticos que possibilitem acessos indevidos a sistemas. Uma parte dessas condutas, estão tipificadas no art. 154-A do código Penal, com punições tanto para invasor, quanto para quem desenvolve e distribui dispositivos. Há, também o art. 325 do Código Penal que dispõe sobre a violação de sigilo funcional para o sujeito que permite ou contribui para o acesso de não-autorizados aos sistemas de informática, como fornecimento ou empréstimo de senhas. (BRASIL, 1940).

- *Fraude informática ou falsidade*: É a alteração, eliminação, introdução ou supressão intencionalmente e ilegítima de dados informáticos, produzindo informações inverídicas, com a finalidade de que sejam considerados e utilizados como se verdadeiros fossem. Não há um tipo específico para tutelar estas condutas em banco de dados privados, são puníveis pelo art. 299, do Código Penal (falsidade ideológica). Já se o crime for praticado contra a administração pública por funcionário público, se enquadram no tipo penal descrito no art. 313-A do código Penal. Já o art. 313 B, do Código Penal pune aquele que modificar ou alterar sistema de informação sem autorização da autoridade competente. (BRASIL, 1940).

- *Burla informática*: conduta intencional e ilegítima, da qual origine dano, através da introdução, alteração, eliminação ou supressão de dados informáticos, com a finalidade de obter benefício econômico, conhecido também como sabotagem informática. Não possui no ordenamento jurídico brasileiro um tipo aplicável a sua conduta.

- *Furto de dados ou vazamento de informações*: cópia intencional e ilegal de informações protegidas ou sigilosas. Alguns autores utilizam a analogia, para classificar o ato como contrafação, furto de dados, já outros acreditam tratar-se de interceptação telemática, com previsão na Lei 9.279/96. Ao certo é que esta conduta não possui não um tipo específico. Ao passo que, para o vazamento de informações é aplicado o art. 153 do código Penal, principalmente quando a divulgação refere-se às informações confidenciais dos bancos de dados ou não da Administração Pública. (BRASIL, 1996). A Lei 12.737, trata como uma qualificadora do crime de invasão de dispositivo eletrônico. (BRASIL, 2012a)

- *Pichação informática*: Conduta do sujeito que altera indevidamente textos ou layout de páginas, sites ou intranet, incluindo textos ou figuras indevidas no código do site (html) ou no banco de dados. Uma grande parte da doutrina concorda que a conduta deve ser punida com o art. 154 A do Código Penal, já outra parte, concorda que a pichação enquadra-se em crime de dano, art. 163 do Código Penal ou concorrência desleal, prevista em Lei especial. (BRASIL, 1940).

- *Envio de mensagens não solicitadas* – É o envio de mensagens não solicitadas por qualquer meio, principalmente e-mails e que de alguma forma possam causar dano ou prejuízo, são usualmente conhecido como Spam. Não existe na ordem jurídica brasileira, legislação para o Spam.

3.6 VALOR PROBATÓRIO DAS PROVAS DIGITAIS

A constituição da prova é elemento fundamental para a ordem jurídica, é através dela que o juiz terá embasamento e convicção para solucionar a lide. São os meio utilizados para convencer o magistrado acerca de fatos que sejam importantes para solucionar a demanda.

No tocante às provas, o doutrinador Guilherme de Souza Nucci, faz algumas considerações:

> Convencendo-se disso, o magistrado, ainda que possa estar equivocado, alcança a certeza necessária para proferir a decisão. Quando forma sua convicção, ela pode ser verdadeira (correspondente à realidade – verdade objetiva) ou errônea (não correspondendo à realidade – verdade subjetiva), mas jamais falsa, que é um "juízo não verdadeiro". Sustentar que o juiz atingiu uma convicção falsa seria o mesmo que dizer que o julgador atingiu uma "certeza incerta", o que é um contrassenso. (NUCCI, 2019, p. 15).

A prova é o conjunto de elementos de que se serve o juiz para formar a convicção sobre os fatos que se funda a demanda. (MARTINS, 2011 p. 383).

No ordenamento jurídico brasileiro, não há nada que proíba as provas por meio eletrônico, conforme dispõe o Código Civil em seu art. 225:

> Art. 225. As reproduções fotográficas, cinematográficas, os registros fonográficos e, em geral, quaisquer outras reproduções mecânicas ou eletrônicas de fatos ou de coisas fazem prova plena destes, se a parte, contra quem forem exibidos, não lhes impugnar a exatidão.
> (BRASIL, 2002).

Corrobora o Código de Processo Civil, em seu artigo 369:

> Art. 369. As partes têm o direito de empregar todos os meios legais, bem como os moralmente legítimos, ainda que não especificados neste Código, para provar a verdade dos fatos em que se funda o pedido ou a defesa e influir eficazmente na convicção do juiz.
> (BRASIL, 2002).

O Código de Processo Penal segue no mesmo sentido, aceitando o documento eletrônico como prova: "salvo os casos expressos em Lei, as partes poderão apresentar documentos em qualquer fase do processo (art. 231) e consideram-se documentos quaisquer escritos, instrumentos ou papéis, públicos ou particulares (art. 232)". (BRASIL, 1941).

Atualmente, a internet vem colaborando em todos os âmbitos do judiciário e utilizá-la para provar fatos está cada vez mais comum. Com o propósito de garantir que os documentos não sejam alterados digitalmente surgiu a MP 2.200-2/2001, que instituiu a Infraestrutura de Chaves públicas Brasileira – ICP Brasil, passando a ser utilizada por Instituições públicas e privadas, visando garantir a autenticidade, integridade e validade jurídica dos documentos eletrônicos.

> Art. 1º Fica instituída a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, para garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras. (BRASIL, 2001).

A assinatura eletrônica é um método seguro e íntegro, substituindo a assinatura da forma convencional pela criptografada (codificada) por meio de certificados digitais. É utilizado como forma de identificar o assinante do documento garantindo, conseguintemente autenticidade, proteção das informações e validade jurídica aos documentos.

O Decreto 8.539/2015, fez a distinção de documento digital e documento digitalizado:

> Art. 2 º Para o disposto neste Decreto, consideram-se as seguintes definições:
> I - documento - unidade de registro de informações, independentemente do formato, do suporte ou da natureza;
> II - documento digital - informação registrada, codificada em dígitos binários, acessível e interpretável por meio de sistema computacional, podendo ser:
> a) documento nato-digital - documento criado originariamente em meio eletrônico; ou
> b) documento digitalizado - documento obtido a partir da conversão de um documento não digital, gerando uma fiel representação em código digital; [...]
> (BRASIL, 2015).

O IP (*Internet Protocol*) também pode ser solicitado aos provedores da Internet, sendo que as informações obtidas com a quebra do sigilo são essenciais para que se chegue ao autor do delito.

Leonardi (2019, p. 10), sobre o IP, aduz que:

> [...] é o código único que identifica determinado computador conectado à Internet, em determinado momento. Toda vez que um usuário se conecta à rede, seu computador recebe automaticamente de seu provedor de acessou um endereço IP que é único durante aquela conexão. Sem conhecer tal endereço, um pacote de dados não tem como chegar a seu destino.

O endereço de IP é a identificação virtual dos dispositivos conectados à internet e pode ser útil, em diversas situações, para que possa identificar de onde estão sendo feitos os acessos na rede de computadores.

No Brasil, somente após o surgimento da lei Marco Civil da Internet, é que os provedores passaram a disponibilizar informações do endereço de IP, data e hora dos acessos, bem como a origem da chamada.

Sabe-se que no Brasil, ninguém é obrigado a fazer ou deixar de fazer algo, senão em virtude da lei (Princípio da Legalidade). (BRASIL, 1988). Neste sentido, antes do Marco Civil, no Brasil, não existia lei que obrigasse os provedores de internet ou de serviços a registrarem *logs* das atividades de seus usuários. Por outro lado, existia apenas "recomendação" do Comitê Gestor Internet do Brasil, para que os provedores (de acesso) passassem a manter, por prazo mínimo de 3(três) anos, dados de conexão e de comunicação realizadas por seus equipamentos (identificação de endereço de IP, data e hora de início e término da conexão e origem da chamada), o que refletia também o posicionamento do Supremo Tribunal de Justiça. (JESUS; MILAGRE, 2016, p. 169).

À vista disso, quando se utiliza os serviços de um provedor, sendo ele gratuito ou pago, mesmo que, anonimamente, de forma criminosa, os dados de quem os acessou e as atividades realizadas permanecem registradas. E, mediante autorização judicial, estes dados poderão ser fornecidos.

Jesus e Milagre (2016, p. 170) explicitam que:

> Obtendo-se os dados de acesso às aplicações daquele que utilizou o serviço para más finalidades, pode-se, através do IP (Internet Protocol), que será fornecido, descobrir qual provedor de acesso associado ao IP (caso o usuário não tenha mascarado a conexão), e, com isto, oficiá-lo, para que apresente os dados físicos (nome, endereço, RG, CPF, CNPJ, entre outros) da pessoa responsável pela conta de Internet a qual estava atribuído o referido IP, na exata data e hora da atividade maliciosa.

Outro ponto importante, para descobrir a autoria do delito, é imprescindível a colaboração de terceiros, ou seja, aqueles que administram e que oferecem serviços, aplicações ou *hosts* (qualquer computador conectado a uma rede), utilizados para a prática de ilícitos virtuais ou que serviriam para a prática da conduta criminosa, que são os provedores de serviços de Internet (aplicações) e os provedores de conexão à internet.

3.7 COMPETÊNCIA PARA PROCESSAR E JULGAR

Competência é a delimitação do poder jurisdicional, ou seja, fixa os limites nos quais os juízes poderão prestar jurisdição.

Insta mencionar que:

> [...] um juiz apenas não tem condições físicas e materiais de julgar todas as causas, diante disso a lei distribui a jurisdição por vários órgãos do Poder Judiciário. Dessa forma, cada órgão jurisdicional somente poderá aplicar o direito dentro dos limites que lhe foram conferidos, nessa distribuição. A competência é, então, a medida e o limite da jurisdição, dentro dos quais o órgão judicial poderá dizer o direito. (CAPEZ, 2016 p. 296).

Vale destacar que a jurisdição é a função estatal exercida com exclusividade pelo Poder Judiciário, consistente na aplicação de normas da ordem jurídica a um caso concreto, com a consequente solução do litígio. É o poder de julgar um caso concreto, de acordo com o ordenamento jurídico, por meio do processo. (CAPEZ, 2016, p. 295).

Em suma, competência é medida de jurisdição, uma medida da extensão do poder de julgar, onde o Estado tem o poder e dever de aplicar o direito ao caso concreto.

Determinar a Territorialidade significar determinar o juiz competente para processar e julgar os delitos virtuais.

Ressalta-se que o Direito Penal Brasileiro está restrito ao território nacional, sendo amparado pelo Código Penal em seus artigos 5º, 6º e 7º, conforme disposto:

> Art. 5º - Aplica-se a lei brasileira, sem prejuízo de convenções, tratados e regras de direito internacional, ao crime cometido no território nacional. (Redação dada pela Lei nº 7.209, de 1984)
> § 1º - Para os efeitos penais, consideram-se como extensão do território nacional as embarcações e aeronaves brasileiras, de natureza pública ou a serviço do governo brasileiro onde quer que se encontrem, bem como as aeronaves e as embarcações brasileiras, mercantes ou de propriedade privada, que se achem, respectivamente, no espaço aéreo correspondente ou em alto-mar. (Redação dada pela Lei nº 7.209, de 1984)
> § 2º - É também aplicável a lei brasileira aos crimes praticados a bordo de aeronaves ou embarcações estrangeiras de propriedade privada, achando-se aquelas em pouso no território nacional ou em vôo no espaço aéreo correspondente, e estas em porto ou mar territorial do Brasil.(Redação dada pela Lei nº 7.209, de 1984)
> **Lugar do crime** (Redação dada pela Lei nº 7.209, de 1984)
> Art. 6º - Considera-se praticado o crime no lugar em que ocorreu a ação ou omissão, no todo ou em parte, bem como onde se produziu ou deveria produzir-se o resultado.(Redação dada pela Lei nº 7.209, de 1984)
> **Extraterritorialidade** (Redação dada pela Lei nº 7.209, de 1984)
> Art. 7º - Ficam sujeitos à lei brasileira, embora cometidos no estrangeiro: (Redação dada pela Lei nº 7.209, de 1984)
> I - os crimes: (Redação dada pela Lei nº 7.209, de 11.7.1984)

> a) contra a vida ou a liberdade do Presidente da República; (Incluído pela Lei nº 7.209, de 1984)
> b) contra o patrimônio ou a fé pública da União, do Distrito Federal, de Estado, de Território, de Município, de empresa pública, sociedade de economia mista, autarquia ou fundação instituída pelo Poder Público; (Incluído pela Lei nº 7.209, de 1984)
> c) contra a administração pública, por quem está a seu serviço; (Incluído pela Lei nº 7.209, de 1984)
> d) de genocídio, quando o agente for brasileiro ou domiciliado no Brasil; (Incluído pela Lei nº 7.209, de 1984)
> II - os crimes: (Redação dada pela Lei nº 7.209, de 11.7.1984)
> a) que, por tratado ou convenção, o Brasil se obrigou a reprimir; (Incluído pela Lei nº 7.209, de 1984)
> b) praticados por brasileiro; (Incluído pela Lei nº 7.209, de 1984)
> c) praticados em aeronaves ou embarcações brasileiras, mercantes ou de propriedade privada, quando em território estrangeiro e aí não sejam julgados. (Incluído pela Lei nº 7.209, de 1984)
> § 1º - Nos casos do inciso I, o agente é punido segundo a lei brasileira, ainda que absolvido ou condenado no estrangeiro.(Incluído pela Lei nº 7.209, de 1984)
> § 2º - Nos casos do inciso II, a aplicação da lei brasileira depende do concurso das seguintes condições: (Incluído pela Lei nº 7.209, de 1984)
> a) entrar o agente no território nacional; (Incluído pela Lei nº 7.209, de 1984)
> b) ser o fato punível também no país em que foi praticado; (Incluído pela Lei nº 7.209, de 1984)
> c) estar o crime incluído entre aqueles pelos quais a lei brasileira autoriza a extradição; (Incluído pela Lei nº 7.209, de 1984)
> d) não ter sido o agente absolvido no estrangeiro ou não ter aí cumprido a pena; (Incluído pela Lei nº 7.209, de 1984)
> e) não ter sido o agente perdoado no estrangeiro ou, por outro motivo, não estar extinta a punibilidade, segundo a lei mais favorável. (Incluído pela Lei nº 7.209, de 1984)
> § 3º - A lei brasileira aplica-se também ao crime cometido por estrangeiro contra brasileiro fora do Brasil, se, reunidas as condições previstas no parágrafo anterior: (Incluído pela Lei nº 7.209, de 1984)
> a) não foi pedida ou foi negada a extradição; (Incluído pela Lei nº 7.209, de 1984)
> b) houve requisição do Ministro da Justiça. (Incluído pela Lei nº 7.209, de 1984). (BRASIL, 1940).

Cumpre, ainda, frisar que, para delitos ocorridos fora do território Nacional, há uma necessidade de revisão entre Acordos dos países envolvidos, Jesus e Milagre (2016, p. 60) tem o seguinte entendimento: “No que diz respeito a condutas ilícitas praticadas em território estrangeiro, não se aplicariam as normas brasileiras, considerando a soberania do pais, sendo que a questão deverá ser tratada pela extradição”.

A autoridade brasileira é competente para processar um crime virtual, cometido por agente brasileiro no exterior, com vítima no Brasil, mas será necessário que este agente retorne para território brasileiro.

> Sendo que para crimes cometidos com *proxy e vpns* (rede privada virtual, servidor remoto que faz a conexão com a internet), ou seja, com recursos que podem mascarar a origem da conexão, com agentes brasileiros, só utilizando a conexão do exterior, poderão ser processados no Brasil desde que identificados o autor do delito. E aí reside mais um dificultador, normalmente os provedores estrangeiros se recusam a fornecer informações sobre acessos, feitos por brasileiros, mas armazenados no exterior. (JESUS; MILAGRE, 2016 p. 60).

Caso o crime virtual seja cometido contra bens da União, a competência será da exercida pela Justiça Federal.

No que se refere ao lugar do crime, o Código Penal Brasileiro, *in casu*, adotou a teoria da Ubiquidade que considera o lugar do crime, o local onde aconteceu a ação ou omissão, no todo ou em parte, bem como onde se produziu ou deveria produzir o resultado. Sendo assim, se um indivíduo está em um Estado e invade um computador em outro estado, que é competente para processar e julgar o delito é o "juízo de onde encontra-se o equipamento invadido". (BRASIL, 1940).

Mas há algumas divergências doutrinarias acerca da teoria a ser adotada, com os seguintes entendimentos:

Para casos relacionados à internet deveria ser adotado a teoria da Atividade, que determina como sendo o local do crime, aquele em que o agente praticou o delito (FERREIRA, 2004, *apud* JESUS; MILAGRE, 2016).

Outro entendimento seria adotar a teoria do Resultado como local do crime, aquele em que se encontra o autor dos delitos, ou seja, onde o resultado foi produzido. Sendo que aquele país, onde ocorreu o delito teria melhores condições de aplicar as devidas punições, sem necessidade de extradições.

Importante mencionar que para crimes praticados por brasileiros, no exterior, que façam vítimas no Brasil, por questões de soberania, a conduta praticada pelo agente é considerada ilícita em ambos os países, e o agente deverá ingressar em solo nacional para ser processado:

> Art. 7º - Ficam sujeitos à lei brasileira, embora cometidos no estrangeiro:
> [...]II - os crimes
> [...] § 2º - Nos casos do inciso II, a aplicação da lei brasileira depende do concurso das seguintes condições:
> a) entrar o agente no território nacional;
> b) ser o fato punível também no país em que foi praticado. (BRASIL, 1940).

Vale destacar que, no Processo Penal, a competência se dá no lugar onde ocorre a infração penal, mas que existem outras regras a serem consideradas, para nortear a competência, conforme orienta o art. 69 do Código de Processo Penal:

> Art. 69. Determinará a competência jurisdicional:
> I - o lugar da infração:
> IV - a distribuição;
> V - a conexão ou continência;
> VI - a prevenção;
> VII - a prerrogativa de função.
> (BRASIL, 1941).

A competência, via de regra, será definida pelo local onde se consumou a infração ou a tentativa, conforme disposto no art. 70 caput, do Código de Processo Penal: “Art. 70. A competência será, de regra, determinada pelo lugar em que se consumar a infração, ou, no caso de tentativa, pelo lugar em que for praticado o último ato de execução”. (BRASIL, 1941).

Outro fator a ressaltar, quando o último ato executório ocorrer fora do território nacional, a competência será do lugar onde o crime ocorreu ou onde o delito foi concluído (resultado), conforme os termos do artigo 70, §2º, do Código de Processo Penal. (BRASIL, 1941).

De acordo com Súmula 48 do STJ: “Compete ao juízo do local da obtenção da vantagem ilícita processar e julgar crime de estelionato cometido mediante falsificação de cheque”. Entretanto, essa competência era definida pelo local onde o estelionatário possuía a conta bancária, pois a vantagem ilícita ocorre no momento que o estelionatário tomava posse do dinheiro, no momento que o montante ingressava em sua conta bancária. (BRASIL, 1992).

Um outro problema acerca da definição da competência para julgar e processar crimes de estelionato (fraudes bancárias na internet), residia em face de vítimas correntistas de Bancos Digitais. Diante da inexistência de agências físicas, continuava sendo o local da obtenção da vantagem ilícita (ou onde o cliente possuía a conta corrente ou onde o estelionatário possuía sua conta), não era possível determinar onde ocorreu a vantagem ilícita, em razão de que não se sabia onde se situava a conta creditada. (LEITÃO, 2020).

A fixação da competência se dava de acordo com o disposto no art. 72 do Código de Processo Penal: Art. 72. Não sendo conhecido o lugar da infração, a competência regular-se-á pelo domicílio ou residência do réu. (BRASIL, 1940).O STJ esclareceu por meio do informativo 663 de 2020 que quando o estelionato fosse cometido por meio de depósito de cheque clonado ou fraudado, a competência era do juízo do local onde a vítima possuía conta bancária. Em casos de transferências ou depósitos na conta do beneficiário da fraude, a competência era do juízo em que tivesse localizada a agência bancária beneficiada, no caso, onde estivesse localizada a conta do estelionatário. (GUEIROS; NUNES, 2021).

A recente Lei 14.155, sancionada em 27 de maio de 2021, veio com propósito de sanar essas discrepâncias, alterando a competência para o crime de estelionato, artigo 171 do Código Penal, com a inclusão do §4º, ao art. 70, do Código Processo Penal: para crimes de estelionato (art. 171, do CP) cometidos mediante depósito, emissão de cheques sem suficiente provisão de fundos em poder do sacado ou com o pagamento frustrado ou mediante transferência de valores, alterou a competência para domicílio da vítima, e em caso, de mais de uma vítima, a competência será definida por prevenção. (BRASIL, 2021a).

A partir da nova lei, a competência passou a ser definida pelo local do domicílio da vítima e não mais pelo local onde o estelionato foi consumado, ou em caso de tentativa, onde foi praticado o último ato de execução, de acordo com artigo 70 do Código de Processo Penal. Salienta-se que para casos ocorridos anteriormente à promulgação da Lei, permanece o entendimento firmado anteriormente pelo STJ.

3.8 DA AÇÃO PENAL

Para os delitos previstos no art. 154- A – Invasão de dispositivo Informático (crimes virtuais) só se procedem por intermédio de representação do ofendido, sendo a ação penal pública, condicionada à representação da vítima, observando a legitimidade e o prazo decadencial.

In verbis:

> Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos. (BRASIL, 2012a).

Entretanto, se os crimes ocorrerem conta a administração pública direta ou indireta da União, Estados, Distrito Federal ou Munícipios, ou Concessionárias de serviços públicos, a ação será pública incondicionada, ou seja, não necessitando da autorização ou representação da vítima.

4 DOS CRIMES COMETIDOS NAS INSTITUIÇÕES FINANCEIRAS DURANTE O PERÍODO DA PANDEMIA DA COVID-19

Este capítulo apresenta dados sobre a pandemia, isolamento social e os crimes virtuais, fraudes eletrônicas pelas mídias sociais, mecanismos utilizados para aplicação de fraudes eletrônicas no ambiente do *internet banking*, qualificação dos crimes virtuais praticados nas Instituições Financeiras, responsabilidade dos agentes envolvidos em relação às fraudes no *internet banking*, formas de prevenção: educação digital e direito brasileiro aplicável à internet.

4.1 PANDEMIA, ISOLAMENTO SOCIAL, E OS CRIMES VIRTUAIS

Com a decretação da situação de Pandemia, o distanciamento social e as medidas de isolamento são medidas eficazes e eficientes para proteger a população e, em vista disso, conter a disseminação e avanço da doença.

Neste compasso a lei 13.979/2020, em seu art. 2º traz algumas definições acerca do tema:

> Considera-se:
> I - isolamento: separação de pessoas doentes ou contaminadas, ou de bagagens, meios de transporte, mercadorias ou encomendas postais afetadas, de outros, de maneira a evitar a contaminação ou a propagação do coronavírus; e
> II - quarentena: restrição de atividades ou separação de pessoas suspeitas de contaminação das pessoas que não estejam doentes, ou de bagagens, contêineres, animais, meios de transporte ou mercadorias suspeitos de contaminação, de maneira a evitar a possível contaminação ou a propagação do coronavírus.
> (BRASIL, 2020a).

O isolamento preconizado atualmente pela OMS para combater a Covid-19 é um procedimento bíblico, realizados desde a antiguidade, para distanciar os leprosos, único recurso existente, então, para evitar a propagação da hanseníase. Ao longo dos séculos, o confinamento continuou a ser utilizado nas epidemias, incluindo também quarentenas obrigatórias aos navios que chegavam aos portos. É uma conduta eficiente quando se está diante de uma doença transmissível e que não tem tratamento, apesar da dificuldade de cumpri-la, posto que muda os hábitos pessoais e familiares, podendo causar alterações no humor e na saúde mental. (NEVES, 2020, p. 18).

Isolamento social é o ato voluntário ou involuntário de manter o indivíduo afastado dos demais indivíduos ou sociedade como um todo.

O isolamento é involuntário quando decorre de fatos que não sepoder prever, como guerras, crimes, questões sanitárias, como a que se está vivenciando no momento, a Pandemia da Covid-19, ou seja, se reestabelece por uma força maior, compulsória, imposta pelo Estado ou por força de situações, como descritas anteriormente. (PORFÍRIO, [2019?]).

Já o mesmo não ocorre no isolamento voluntário, que se dá quando o indivíduo decide única e exclusivamente se afastar da sociedade, por questões particulares, religiosas, de saúde, por exemplo. (PORFÍRIO, [2019?]).

A Pandemia da Covid-19, vivenciada no momento, é um exemplo de isolamento involuntário, decorrente de situação não prevista, em que os governos estão impondo isolamento e distanciamento social, a fim de que se possa reestabelecer o controle, a propagação do vírus e disseminação da doença.

Em consonância com o SINESP (Sistema Nacional de Informações de Segurança Pública do Ministério da Justiça e Segurança) houve uma diminuição nos crimes contra a pessoa, como furtos, roubos, lesão corporal. Em compensação os delitos cibernéticos, objeto desta pesquisa, cresceram absurdamente. (COSTA, 2020).

Nesta fase em que as pessoas permanecem mais tempo conectadas, trabalhando de suas casas, utilizando-se mais de serviços e ambientes digitais, consequentemente aumentando o fluxo de circulação pela rede, possibilitam aos criminosos virtuais, mais oportunidades em suas investidas.

Em função dessas medidas de distanciamento social, as pessoas, aumentaram seu consumo de conteúdo digital sem estarem totalmente preparados para essa migração, sendo este, um dos propulsores para o aumento significativo dos crimes virtuais.

O que por um lado propicia aos usuários acesso a muitas facilidades, paralelamente expõe a riscos e deixa-os mais vulneráveis, ambiente propício para que os criminosos virtuais possam diversificar seus ataques.

Pode-se compreender os crimes virtuais como:

> [...] delitos que dispensam a presença física do ofensor, dispensam contatos diretos com a vítima, planejamento e força, ocorre não raro a partir de uma ação contra uma multiplicidade de pessoas (crimes de um contra muitos e de alastramento rápido) e não respeitam lógica e estilo, sendo alvo pois de constantes modificações em suas táticas e ardis. (SYDOW, 2021, p .644).

A maioria dos crimes cometidos no mundo virtual ocorre também no mundo real, a internet surge apenas como mero facilitador, geralmente pelo anonimato que proporciona, sendo que as definições sobre crime, delitos, atos e efeitos serão as mesmas, quer sejam

aplicadas pelo direito penal ou pelo direito penal virtual. Alguns diferenciais ocorrem às questões referentes à territorialidade, investigação probatória e alguns tipos penais de modalidades, que em função de suas peculiaridades, merecem tipo penal próprio.

Neste sentido, aduz Pinheiro (2021, p. 389):

> O crime eletrônico é, em princípio um crime de meio, ou seja, utiliza-se de um meio virtual. Não é um crime de fim, por natureza, ou seja, o crime cuja modalidade só ocorra em ambiente virtual, à exceção dos crimes cometidos por *hackers*, que de algum modo possam ser enquadrados na categoria de estelionato, extorsão, falsidade ideológica, fraude, entre outros. Isto quer dizer que o meio de materialização da conduta criminosa pode ser virtual; contudo, em certos casos, o crime não.

A ocorrência dos crimes virtuais produz efeitos não apenas no mundo digital, mas no mundo real, causando uma serie de prejuízos, moral e material.

Os crimes não são novos, mas evoluem conforme as oportunidades “online” se apresentam, usando de tempo disponível e criatividade, os criminosos virtuais vão elaborando novas técnicas de abordagem e ataques às suas vítimas.

A pandemia da Covid-19 intensificou significativamente o aumento dos delitos envolvendo o ambiente virtual, principalmente no ambiente bancário. O aumento do uso dos meios digitais tem gerado preocupação com a segurança de dados, principalmente quando se refere às informações financeiras.

Cumpre evidenciar que as medidas de distanciamento social possibilitaram aos criminosos virtuais potencializar suas investidas, devido ao grande fluxo de usuários que utilizam-se desses espaços, explorando a fragilidade e falta de conhecimento das pessoas.

Sabe-se que por mais que exista um aparato de leis para proteger os usuários deste meio, e que as instituições financeiras estejam seguidamente atualizando seus sistemas de segurança, os criminosos virtuais estão cada vez mais ousados e criativos quanto aos métodos para burlar os sistemas.

4.2 FRAUDES ELETRÔNICAS PELAS MÍDIAS SOCIAIS

Importa apresentar o que se entende por rede social, pode-se dizer que é “[...] todo sistema informático capaz de integrar um grupo de usuários em um ambiente em que sejam possíveis a fácil publicação e a propagação de conteúdo”. (LIMA, 2016, p. 123).

Algumas das fraudes eletrônicas muito praticadas ultimamente são pelas mídias sociais, aplicativos como WhatsApp, Instagram, Facebook, são frequentemente utilizados para esta finalidade. (ROHR, 2021).

Como forma de prevenção à disseminação da doença provocada pela Pandemia da Covid-19 empresas e pessoas físicas estão experimentando modos diferentes de trabalhos e os fraudadores aproveitam para intensificar seus golpes.

Há um novo tipo de golpe ofertado, nas redes sociais, chamados de “métodos” (*clicking*), são guias que os influenciadores digitais vendem com técnicas que ensinam como aplicar fraudes *online*. Normalmente, os influenciadores referem-se como *clicking*, seus alvos potenciais são as Instituições Financeiras, e de posse de informações completas (conhecidas pelo termo inglês como *full information ou fullz*), sobre a vítima como nome, telefone, dados bancários, endereço, começam a praticar golpes. (OS INFLUENCIADORES..., 2021?).

Estes métodos negociados têm como principais focos a atingir bancos e sistemas de créditos do governo. De posse dos dados completos das potenciais vítimas, geralmente obtidos através de golpes de *plishing*, que são “e-mails *fakes*, que aparentando ter fontes legitimas, visam influenciar as pessoas a fim de que compartilhem suas informações confidenciais como senhas, números de cartão, códigos de segurança, entre outros”, intensificam suas tentativas, muitas vezes exitosas. (OS INFLUENCIADORES..., 2021?).

Cita-se alguns dos tipos mais comuns: compras usando dados de outra pessoa, falsa vaga de emprego, promoções de lojas conhecidas, vaquinhas *online*, assinaturas gratuitas de serviços conhecidos, notícias alarmantes, geralmente ao clicar em *links*, o usuário é direcionado para outras páginas em que tem seus dados e senhas copiados ou até mesmo permitindo acesso ao seu perfil, onde os criminosos possam se passar por ele livremente.

O WhatsApp tem sido o “queridinho” para aplicação de fraudes, isso se dá em função do grande volume de mensagens que circulam diariamente pelo aplicativo, como roubo de senhas, links falsos, perfis falsos, enfim, infinitas possibilidades de fraudes.

Com as recentes alterações promovidas pela recente Lei 14.155/2021, nos artigos 154A, 155 e 171 do Código Penal, ampliando a abrangência do tipo penal, majorando penas, incluindo qualificadoras, tornando o tipo penal mais rígido contra violação de dispositivo informático, furto, estelionato, busca-se, uma maior inibição à atuação dos criminosos e aplicação de penas mais gravosas, pois anteriormente as penas eram excessivamente brandas. (LIMA, 2016).

4.3 MECANISMOS UTILIZADOS PARA APLICAÇÃO DE FRAUDES ELETRÔNICAS NO AMBIENTE DO *INTERNET BANKING*

Dentre os mecanismos mais utilizados para a prática do delito virtual, no ambiente do *Internet Banking*, destacam-se os casos de engenharia social, que são técnicas de

convencimento para enganar as pessoas, a fim de que estas forneçam informações pessoais ou permitam acessos a sistemas, como indicação de usuários e senhas.

Segundo informações da FEBRABAN – Federação Nacional dos Bancos, os golpes de engenharia social são os mais utilizados atualmente. Pode-se entender a "engenharia social" como os golpes em que o cliente é induzido a informar espontaneamente seus dados pessoais, fornecendo códigos de segurança e senhas. Antigamente, eram mais comuns fraudes em documentos e falsificação de assinaturas como nos casos dos cheques, falsificação de documentos de identificação para efetuar saques, mas atualmente os golpes de engenharia social dominam este setor, e as pessoas viraram alvo principal. (BANCOS..., 2020).

"O engenheiro social é o especialista em manipular a mente humana". (SOUZA, 2020).

Ainda, faz-se oportuno enfatizar que,

> [...] a engenharia social é um dos maiores riscos à segurança das pessoas e das organizações. Com técnicas cada vez mais ousadas e sofisticadas, que se aproveitam da inocência e desconhecimento das pessoas, utilizam da psicologia humana, explorando sentimentos e emoções de forma a controlar o comportamento da vítima. (SILVA, 2013 p. 18).

A engenharia social é uma técnica de persuasão, em que os criminosos virtuais tornam-se mestres em técnicas de manipulação psicológica, a fim de que os usuários forneçam informações confidenciais como senhas, números de cartão de crédito e códigos de segurança, podendo ser aplicada não somente na internet, mas fora dela também. Dentre as mais utilizadas destacam-se o *Phishing*, *Smishing, vishing, Spam.*

4.3.1 Phishing

O *Phishing,* ou *phishing scam,* uma técnicas mais comuns da engenharia social, origina-se do termo inglês *fishing*, que significa pescaria. Através dela o criminoso virtual tenta enganar as pessoas para que compartilhem informações confidenciais, buscando adquirir ilicitamente dados pessoais, como senhas, dados bancários, números de cartão de crédito.

Sobre a fraude por *phishing scan,* Pinheiro (2021, p. 405) esclarece que ela corre da seguinte maneira:

> [...] (1) um código malicioso é enviado por e-mail para as vítimas, (2) as quais, não analisando a veracidade do conteúdo nem o remetente da mensagem, acessam a informação, executam o arquivo e, consequentemente, (3) o computador do usuário é infectado, (4) comprometendo suas informações confidenciais, tais como senhas, dados pessoais, etc., (5) essas informações são transmitidas para o fraudador, (6) que as utiliza para acessar, por exemplo, (7) o *Internet Banking* da vítima e desviar dinheiro para outra conta.

A maioria das fraudes utilizam de engenharia social, técnicas empregadas pelos criminosos virtuais para induzir as pessoas a fornecerem dados pessoais, infectar seus computadores com vírus ou orientar a abrir links infectados. É a manipulação para que o indivíduo forneça informações sigilosas como senhas, número de cartões ou faça transações.

O fraudador utiliza e-mails, aplicativos e sites que parecem ser legítimos, para convencer o usuário de que se trata realmente de fontes confiáveis, induzindo a vítima a baixar programas maliciosos, com a finalidade única e exclusiva de cometer fraudes e obter vantagem financeira. (HARÁN, 2019).

Posteriormente o usuário é direcionado a uma página falsa, em que seus dados são copiados pelo fraudador.

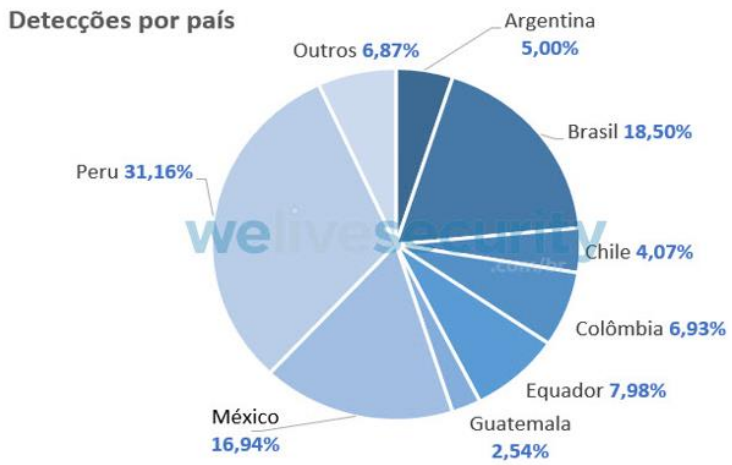
O contato pode ocorrer por mecanismos como: *e-mail* falsos, *sms* ou telefone, por pessoa ou empresa, se passando por fonte genuína

Um clássico exemplo, bastante utilizado e com sucesso nas investidas, é daquele que liga identificando-se como funcionário da Instituição Financeira, pedindo para fazer algumas verificações remotas no cadastro ou conta, ou precisar testar um acesso, ou atualizar o sistema, dependendo da técnica de argumentativa, pode resultar em sucesso.

Outros exemplos são a falsa central telefônica, falso *motoboy*, em que são utilizadas técnicas pesadas de persuasão.

Ao analisar o comportamento das detecções de ataques de engenharia social na América Latina, o Brasil registrou estar em segundo lugar em ataques de *phishing* no ano de 2020, conforme pode ser visualizado no Gráfico abaixo:

Gráfico 1 – Detecções de ataque de engenharia social na América Latina no ano de 2020.



Fonte: Lubeck (2021).

4.3.2 Smishing

É uma variante do *Phishing*, utiliza mensagens curtas como *SMS*, ou mensagens longas que são enviados para Smartphones. Técnicas de persuasão para que o usuário forneça dados confidenciais via mensagem de texto ou *SMS.*

Geralmente as pessoas são mais cientes dos riscos, quando se trata de e-mails ou links, mas não tem o mesmo cuidado em relação às mensagens de texto ou SMS, por isso o *smishing* pode ser extremamente perigoso. De posse dos dados, uma prática bastante comum é solicitar cartões de crédito em nome de suas vítimas. (AMEAÇAS..., [2021?]).

4.3.3 Vishing

É uma abreviação de *voice phishing* (fraude por voz), também derivada do *Phishing*, utiliza sistema de voz automática para fazer chamadas de voz, solicitando informações pessoais. (ABREU, 2020).

Usam técnicas de persuasão para manipulação emocionalmente os indivíduos, induzindo a repassar informações confidenciais.

Um exemplo muito comum ocorre nos casos em que a vítima recebe uma ligação para confirmar informações. Na verdade, quem está do outro lado da linha, não tem nenhuma ou tem muito pouca informação, mas tentará convencer a passar os dados pessoais ou financeiros.

4.3.4 Spam

Na prática, o *SPAM* é uma mensagem eletrônica que chega ao usuário sem a sua permissão ou sem seu desejo em recebê-lo. Geralmente são recebidas por e-mail, mas também podem circular pelas redes sociais ou comentários de blogs. O *SPAM* tem um fundo geralmente comercial, mas também pode assumir um viés criminoso. (O QUE É SPAM, 2016).

É o termo utilizado para os e-mails que são enviados para as pessoas, sem a sua permissão, normalmente direcionadas a um grande público, contendo geralmente propagandas.

Enviar e postar informação em massa, atingindo um grande público.

São e-mails indesejáveis para uma quantidade muito grande de pessoas, contem publicidades ou em alguns casos, tem intenção de copiar dados pessoais ou financeiros.

4.3.5 Pharming

Pharming é uma prática fraudulenta semelhante ao phishing, com a diferença que, no *pharming*, o tráfego de um site legítimo é manipulado para direcionar usuários para sites falsos, que vão instalar softwares maliciosos nos computadores dos visitantes ou coletar dados pessoais, tais como senhas ou informações financeiras.

Este tipo de ataque é particularmente traiçoeiro porque, se um servidor de DNS for comprometido, mesmo os usuários com aparelhos protegidos e livres de malwares podem se tornar vítimas. (PHARMING, [2016?]).

Sendo que, o serviço DNS (*Domain Name System*): "[...] é o principal responsável pela resolução de nomes na Internet. Esse serviço é construído por um conjunto de servidores operando de forma descentralizada. Cada servidor DNS é responsável por um domínio ou sub-domínio de nomes na Internet". (MAZIERO, [2021?], n.p.).

É um tipo de crime virtual muito semelhante ao Phishing, sendo que também leva o usuário a um endereço (URL) falso, por alteração no domínio da página (DNS).

No *pharming*, o criminoso virtual, faz com que um usuário da internet acesse um site falso, em vez do legítimo que ele estava procurando. A página fraudulenta simula o layout dos sites verdadeiros, para conseguir capturar informações confidenciais da vítima. (BRANCO, 2021).

Os criminosos normalmente copiam as páginas dos Bancos fielmente, para enganar o usuário, que pensa estar no site da instituição e, consequentemente acaba por fornecer informações confidenciais ao digitar senhas, números de contas, que serão armazenadas por estes servidores.

Um exemplo muito comum de *phaming*, que acontece muito atualmente é a geração de boletos falsos. O usuário tentado gerar um boleto ou recalcular seu valor, digita no site de buscas, cálculo de boletos/ gerar boleto, e é direcionado a um site de banco falso, que gera o boleto com dados alterados, alterando a linha digitável e consequentemente os dados do receber do crédito. (ROHR, 2020).

4.4 QUALIFICAÇÃO DOS CRIMES VIRTUAIS PRATICADOS NAS INSTITUIÇÕES FINANCEIRAS

4.4.1 Estelionato virtual

O estelionato é uma das práticas mais comuns do ordenamento jurídico brasileiro. Para que o delito seja configurado, é necessário a existência de quatro requisitos no tipo penal: obtenção de vantagem ilícita, causar prejuízo à outra pessoa, utilização de meio ardil ou artifício e indução a erro. Admite apenas a forma dolosa, ou seja, quando há a intenção de lesar outrem.

No Brasil, o crime de estelionato está descrito no caput artigo 171 do Código Penal Brasileiro:

> **Estelionato**
> 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. (Vide Lei nº 7.209, de 1984)
> § 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.
> (BRASIL, 1940).

Trata-se de crime em que, em vez da violência ou grave ameaça, o agente emprega um estratagema para induzir em erro a vítima, levando-a a ter uma errônea percepção dos fatos, ou para mantê-la em erro, utilizando-se de manobras, para impedir que ela perceba o equívoco em que labora. Dessa forma, são os ensinamentos de Capez (2020, p. 642):

> Os meios empregados para tanto são:
> (i) **Artifício**: significa fraude no sentido material. "o artifício existe quando o agente se utilizar de um aparato que modifica, ao menos aparentemente, o aspecto material da coisa, figurando entre esses meios o documento falso ou outra falsificação qualquer, o disfarce, a modificação por aparelhos mecânicos ou elétricos, filmes, efeitos de luz etc."
> (ii) **Ardil**: é fraude no sentido imaterial, intelectualizada, dirigindo--se à inteligência da vítima e objetivando excitar nela uma paixão, emoção ou convicção pela criação de uma motivação ilusória. Uma boa conversa, uma simulação de doença, sem nenhum outro disfarce ou aparato, além da "cara de pau".
> (iii) **Qualquer outro meio fraudulento**: embora compreenda o artifício e o ardil (o que torna a distinção sem importância prática), constitui expressão genérica, a qual deve ser interpretada de acordo com os casos expressamente enumerados (interpretação analógica), de modo que, além das duas formas anteriores, alcança todos os outros comportamentos a elas equiparados.
> **– Idoneidade do meio fraudulento empregado**: seja qual for o meio empregado, só há estelionato quando existir aptidão para iludir o ofendido. A aferição dessa potencialidade deve ser realizada segundo as características pessoais da vítima (sua maior ou menor experiência e capacidade de percepção) e as circunstâncias específicas do caso concreto. Desde que o meio fraudulento empregado pelo agente seja apto a burlar a boa-fé da vítima, pouco importa que a fraude seja grosseira ou inteligente, pois o mundo do estelionatário comporta gente de variada densidade intelectual. No entanto, quando totalmente inapta a iludir, mesmo o mais ingênuo dos mortais, o fato será atípico.
> **– Erro**: consiste na falsa percepção da realidade, provocando uma manifestação de vontade viciada. A situação na qual a vítima acredita não existe. Houvesse o conhecimento verdadeiro dos fatos, jamais teria ocorrido a vantagem patrimonial ao agente, que, para obtê-la, provoca ou mantém a vítima no erro (nesta última hipótese, o autor aproveita uma situação preexistente, um erro espontâneo anterior por ele não

> provocado, e emprega manobras fraudulentas para manter esse estado e assim obter a vantagem ilícita).
> **– Vantagem ilícita**: é o objeto material do crime em tela. O agente emprega meio fraudulento capaz de iludir a vítima com a finalidade de obter vantagem ilícita em prejuízo alheio. Deve a vantagem ser econômica, pois trata-se de crime patrimonial.. Deve também ser ilícita, ou seja, não corresponder a qualquer direito. Se for lícita, haverá o crime de exercício arbitrário das próprias razões. Cumpre ressalvar que se o agente obtém a vantagem ilícita em prejuízo alheio, afasta-se qualquer indagação relativa à idoneidade do meio fraudulento empregado. Tal questionamento somente é cabível na tentativa.
> **– Prejuízo alheio**: é o dano de natureza patrimonial. Concomitantemente à obtenção da vantagem ilícita pelo agente, deve ocorrer prejuízo para a vítima, ou seja, uma perda patrimonial. Temos, portanto, quatro momentos no crime de estelionato: (i) o do emprego da fraude pelo agente; (ii) o do erro em que incidiu a vítima; (iii) o da vantagem ilícita obtida pelo agente; (iv) o do prejuízo sofrido pela vítima.
> (CAPEZ, 2020, p. 642-643).

O crime de estelionato virtual possui previsão legal no artigo 171 do Código Penal, foi recentemente alterado pela Lei 14.155 de 27 de maio de 2021, acrescentando-se os §§ 2º A e 2º B, criando a figura da Fraude Eletrônica. Veja-se como ficou a nova redação do artigo:

> **Fraude eletrônica**
> § 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. (Incluído pela Lei nº 14.155, de 2021)
> § 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. (Incluído pela Lei nº 14.155, de 2021)
> § 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.
> (BRASIL, 2021a).

GIL (1999, p. 15) dispõe:

> [...] a fraude corresponde a uma ação intencional e prejudicial a um ativo intangível, causada por procedimentos e informações (software e banco de dados), de propriedade de pessoa física, ou jurídica, com o objetivo de alcançar benefício, ou satisfação psicológica, financeira e material.

As fraudes podem ser praticadas por funcionários ou terceiros que se encontram dentro do local a ser fraudado (internas) ou por pessoas que não tenham vínculo com o local a ser fraudado (externas).

Pinheiro (2020 p. 404), ao tratar da fraude eletrônica, define como “[...] uma mensagem não solicitada que se passa por comunicação de uma instituição conhecida, como um banco,

empresa ou site popular, procurando induzir usuários ao fornecimento de seus dados financeiros e pessoais".

A Fraude eletrônica se dá quando o agente comete crime com a utilização de informações fornecidas pela própria vítima ou terceiros, incluído o ato de induzir ao erro através das redes sociais, contatos telefônicos ou e-mails fraudulentos (*phishing*).

Inicialmente, a fraude eletrônica dizia respeito apenas às páginas fraudulentas em que o usuário acessava, atualmente referem-se também às mensagens em que o usuário é induzido à instalação de programas maliciosos, e acaba ela mesma enviando os seus dados pessoais e financeiros.

O crime de estelionato virtual será caracterizado se houver invasão, adulteração ou clonagem de aplicativos de mensagens instantânea e chamadas de voz para *smartphones*, ou com emprego da rede de computadores, dispositivo de comunicação, ou sistema informatizado. (BRASIL, 2020b).

Para Pinheiro (2021, p. 404), "em termos de panorama das fraudes eletrônicas, em nosso país, o Brasil é tido como o maior exportador de crimes eletrônicos do mundo e, obviamente, as fraudes estão inclusas nessas estatísticas".

Ressalte-se que, para combater o crime eletrônico, foi realizada a Convenção de Budapeste sobre cibercriminalidade do Conselho da Europa, um dos instrumentos mais importantes para a cooperação internacional digital, em questões referentes à internet, à sistemas informáticos e à computação. Dessa Convenção, foram elaboradas estratégias jurídicas conjuntas para tipificação, combate e prevenção de crimes pela internet, medidas de cooperação para acesso a dados e obtenção de provas digitais. Lembrando que o Brasil ainda não é signatário dessa Convenção, e seu ingresso seria um importante passo rumo ao combate da criminalidade virtual.

A atualização trazida pela nova Lei surge como medida de inibição às fraudes virtuais, que aumentaram significativamente no período da Pandemia, em função das medidas de isolamento social e da maior utilização dos canais digitais.

A nova Lei alterou o Código Penal nos crimes de invasão de dispositivo, furto qualificado e estelionato, ocorridos nos meios eletrônicos, além dos crimes cometidos com a utilização de dados fornecidos por pessoas induzidas ao erro pelas redes sociais, contatos telefônicos, mensagens ou e-mail fraudulentos.

Essa resposta mais rigorosa por parte do direito penal, é vista como medida positiva, principalmente, durante a pandemia, em que a incidência dos crimes virtuais sofreu aumento

significativo. Essas alterações, visam inibir a ação dos criminosos virtuais, elevando as penas que anteriormente eram de detenção 3 meses a 1 ano, para reclusão de 1 a 4 anos.

Tal medida se fez necessária, visto que anteriormente o delito era tratado com punições relativamente irrisórias, penas muito brandas e restritivas de direito ineficazes, ou seja, penas muito leves e insuficientes para inibir novos crimes se comparado aos danos e prejuízos financeiros ocasionados às vítimas.

4.4.2 Furto mediante fraude

O crime de furto é descrito como subtração, ou seja, ato de retirar de alguém o que é seu por direito, é a diminuição do patrimônio de outrem, sem que haja violência. Sua previsão legal é trazida no artigo 155, do Código Penal Brasileiro: Art. 155 - Subtrair, para si ou para outrem, coisa alheia móvel: Pena - reclusão, de um a quatro anos, e multa. (BRASIL, 1940).

No crime de furto, a fraude é empregada com a finalidade de dificultar, reduzir ou impedir a vigilância da vítima, que passa a ficar distraída, momento em que o agente aproveita para subtrair o bem, sem a vítima perceba. Eis sua tipificação:

> **Furto**
> Art. 155 - Subtrair, para si ou para outrem, coisa alheia móvel:
> Pena - reclusão, de um a quatro anos, e multa.
> [...] § 4º-B. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se o furto mediante fraude é cometido por meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem a violação de mecanismo de segurança ou a utilização de programa malicioso, ou por qualquer outro meio fraudulento análogo. (Incluído pela Lei nº 14.155, de 2021)
> § 4º-C. A pena prevista no § 4º-B deste artigo, considerada a relevância do resultado gravoso: (Incluído pela Lei nº 14.155, de 2021)
> I – 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; (Incluído pela Lei nº 14.155, de 2021)
> II – aumenta-se de 1/3 (um terço) ao dobro, se o crime é praticado contra idoso ou vulnerável. (Incluído pela Lei nº 14.155, de 2021).
> (BRASIL, 1940).

A fraude é qualquer artifício ou artimanha que o agente utiliza para facilitar a subtração, utilizando-se dos mais variados métodos fraudulentos possíveis. Existem hipóteses em que a fraude é empregada pelo agente para enganar a vítima, distrair ou desviar sua atenção, e outras ainda mais elaboradas, como a criação de falsos sites que imitam o site verdadeiro dos bancos, e as vítimas enganadas acessam o site e digitam suas informações financeiras, como número de

conta e senhas, e os criminosos de posse dessas informações, subtrai dinheiro das contas, efetuam transferências, sem terem autorização (GONÇALVES, 2016 p. 425).

4.4.3 Algumas diferenças entre Estelionato e furto mediante fraude

Para Gonçalves (2016 p. 425):

> Estes crimes não se confundem. No furto, há a subtração do bem (não se podendo esquecer de que o conceito de furto abrange os casos de posse vigiada), enquanto, no estelionato, a vítima entrega a posse desvigiada (com autorização para deixar o local com o bem) do bem por ter sido ludibriada pelo golpista. Quando é o próprio agente quem, após empregar a fraude, se apodera do bem, levando-o, fica evidente a configuração do furto mediante fraude, mas torna-se um pouco mais complexo quando a própria vítima entrega o bem em decorrência de uma fraude empregada pelo agente.

Neste sentido, a respeito da diferenciação entre esses dois crimes que causa muita confusão na doutrina, o STJ manifestou seu posicionamento:

> [...] a distinção se faz primordialmente com a análise do elemento comum da fraude que, no furto**,** é utilizada pelo agente com o fim de burlar a vigilância da vítima que, desatenta**,** tem seu bem subtraído, sem que se perceba; no estelionato**,** a fraude é usada como meio de obter o consentimento da vítima que, enganada**,** entrega espontaneamente o bem ao agente. (AGRAVO EM RECURSO ESPECIAL Nº 1.418.119 - DF (2018/0333774-2). (BRASIL, 2007).

O ministro Paciornik apontou estudos doutrinários sobre a distinção dos crimes de furto e estelionato, salientou que no caso do furto, caracterizado pela inversão de posse, a fraude visa a diminuir a vigilância da vítima e possibilitar a subtração do bem. E, no caso do estelionato, a fraude visa induzir vítima em erro e voluntariamente entregar o bem ao agente criminoso, baseada em uma falsa percepção da realidade (BRASIL, 2019).

Vejam-se alguns exemplos: saques indevidos em caixas eletrônicos, transferências pela internet, em que as senhas foram obtidas de forma fraudulenta pela internet ou através dos "chupa-cabras" instalados nos terminais eletrônicos, clonagem de cartões bancários, todas essas situações trata-se de furto mediante fraude (art. 155, §4, II, do Código Penal), visto que o agente ao conseguir de forma ilícita os dados para acessar a conta bancária da vítima, está empregando fraude, pois está dificultando ou impossibilitando a vigilância da vítima. Em todos esses relatos, a vítima tem seu bem subtraído pelo agente, e não entregue pela vítima. Normalmente, essas fraudes ocorrem por meio de *e-mail* falsos (*phishing*) em que a vítima, acaba inserindo dados

ou clicando em *links* e tendo, por conseguinte, suas informações copiadas, mediante instalação de arquivo malicioso em seu equipamento.

E um dos golpes mais utilizados é do falso funcionário bancário, golpe do motoboy, falsa central telefônica e *phishings*, todos esses casos relatados são situações em que a vítima é induzida a erro e repassa seus dados sigilosos espontaneamente, ou seja, a vítima não percebe que está colaborando com o criminoso, são enquadradas como crimes de estelionato (fraude eletrônica), artigo 171, do Código Penal.

Outro exemplo de crime que causa muita controvérsia é o furto de dados, partindo do pressuposto do que o Código Penal define como furto subtrair, para si ou para outrem, coisa alheia móvel. A doutrina considera que a subtração de um bem exige que ele se torne indisponível para seu proprietário, saindo de sua esfera de guarda e controle, logo, a questão que se coloca é se seria possível tipificar como furto a conduta de subtrair dados da empresa, reproduzindo os mesmos (replicando a base de dados), mas deixando-os ainda disponíveis para acesso da empresa, ou seja, sem eliminá-los ou apagá-los. Sendo assim, não existiria a tal indisponibilidade do bem, para o enquadramento legal em furto, seria então um delito de direito autoral? Ou seria crime de dano ou quebra de sigilo? (PINHEIRO, 2021, p. 405).

Em razão destas situações, muitos países estão ajustando suas legislações pátrias que podem gerar dúvidas ou até mesmo afastar a tipificação, ou enquadrar em outros tipos penais por analogia, com penas mais brandas.

4.4.4 A incidência dos Crimes virtuais durante o período de Pandemia

Com o avanço tecnológico, já existe uma tendência natural das pessoas irem migrando para os ambientes digitais, e com as medidas de isolamento social, essa migração ocorreu mais rapidamente, sem que as pessoas estivessem preparadas e cientes dos riscos que estavam expostas.

Com a chegada da pandemia da Covid-19, as pessoas passaram a se deslocar menos para as agências bancárias, ao mesmo tempo que, trouxe mais comodidade, também despertou a atenção dos criminosos, que viram oportunidades, ao saber que as pessoas passariam mais tempo *online*, aumentando suas investidas delituosas. (GUGELMIN, 2021).

Neste período de pandemia, o volume de ocorrências de fraudes virtuais, como o golpe da central telefônica e do funcionário aumentou cerca de 340%, durante os meses de janeiro e fevereiro de 2021, em consonância com a FEBRABAN. (SILVA, 2021.)

Durante a pandemia da Covid-19, os golpes envolvendo engenharia social crescem assustadoramente, um comparativo feito pela empresa Welive Security, informa que houve um aumento de 200% (duzentos pontos percentuais) no ano de 2020 em relação ao mesmo período no ano de 2019, em consequência do aumento do número de usuários que migraram para os canais digitais, em função do isolamento social, aliada a falta de conhecimento dos usuários, acabam por se tornarem mais vulneráveis e vítimas potenciais dos criminosos virtuais.

Segundo levantamento apontados pela Febraban – Federação Nacional dos Bancos, mostram o crescimento de tentativas de várias modalidades de fraudes financeiras contra os brasileiros durante a crise da Covid-19, durante o ano de 2020.

Atualmente, 70% das fraudes estão ligadas à engenharia social, no período de isolamento social, as instituições financeiras registraram aumento de 80% nas tentativas de ataques de *phishing* - que se inicia por meio de recebimento de e-mails que carregam vírus ou links falsos, o golpe do falso motoboy também aumentou cerca de 65% durante o período de isolamento social. Já os golpes do falso funcionário e falsas centrais telefônica cresceram 70%.

Recentemente, a FEBRABAN também revelou que no mesmo período, houve aumento de 60% em tentativas de golpes financeiros contra idosos, o que gerou um alerta com o apoio da Secretaria Nacional de Promoção e Defesa dos Direitos da Pessoa Idosa, vinculada ao Ministério da Mulher, da Família e dos Direitos Humanos, e do Banco Central.

Em 2020, o Brasil foi o país mais atingido pela prática do *phishing*, técnicas utilizadas para capturar dados pessoais e financeiros na internet, e de posse das informações, os criminosos, começam as tentativas de golpes, quer acessando os recursos ou utilizando de persuasão, para enganar as pessoas. (BRASIL, 2021d).

4.5 RESPONSABILIDADE DOS AGENTES ENVOLVIDOS EM RELAÇÃO ÀS FRAUDES NO *INTERNET BANKING*

4.5.1 Responsabilidade dos Bancos

O Código Civil estabelece em seu art. 927:

> Art. 927. Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo.
> 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, risco para os direitos de outrem.
> (BRASIL, 2002).

Para a análise do art. 927, precisa-se conceituar o ato ilícito, conceituado pelos artigos 186 e 187, do Código Civil Brasileiro:

> Art. 186. Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito.
> Art. 187. Também comete ato ilícito o titular de um direito que, ao exercê-lo, excede manifestamente os limites impostos pelo seu fim econômico ou social, pela boa-fé ou pelos bons costumes.
> (BRASIL, 2002).

Em suma, aquele que causar dano a alguém, tem a obrigação de repará-lo.

O código civil adota a responsabilidade subjetiva, como regra, como estas definidas nos arts. 186 e 187, mas em alguns casos adota a responsabilidade objetiva, como mencionada no parágrafo único do art. 927. (BRASIL, 2002).

O Código de Defesa do Consumidor dispõe em seu art. 3º, § 2º, o enquadramento das instituições bancárias como fornecedores, sendo sua principal atividade a venda de produtos e prestação de serviços financeiros:

> 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.
> (BRASIL, 1990).

Teria a Instituição Financeira obrigação de ressarcimento das fraudes ocorridas nas contas de seus clientes?

Tanto a doutrina, quanto a jurisprudência defendem a aplicabilidade do CDC aos contratos bancários, e há também o entendimento do STF que julgou improcedente o pedido da ADI 2591, que demandava a inconstitucionalidade do art. 3º, § 2º do CDC, na parte referente às relações bancárias.

Coelho (2011, p. 493) traz a definição dos Contratos bancários:

> Contratos bancários são aqueles em que uma das partes é, necessariamente, um banco. Isto é, se a função econômica do contrato está relacionada ao exercício da atividade bancária, ou, dizendo o mesmo de outro modo, se o contrato configura ato de coleta, intermediação ou aplicação de recursos financeiros próprios ou de terceiros, então somente uma instituição financeira devidamente autorizada pelo governo poderá praticá-lo. Neste caso, o contrato será definido como bancário.

Para exercer a atividade bancária é necessário que haja a autorização do Banco Central do Brasil, sendo que para estrangeiros a autorização se dá por Decreto do Presidente da República, conforme trazido na Lei 4.595/64, em seu artigo 18.

A Súmula 297 do STJ corrobora: "O Código de Defesa do Consumidor é aplicável às instituições financeiras", ou seja, as relações jurídicas realizadas entre as pessoas físicas ou jurídicas e as instituições financeiras são relações de consumo.

Destarte, estando as Instituições financeiras enquadradas como prestadoras de serviço e comprovada a relação de consumo entre clientes e instituições financeiras, resta demonstrada também a necessidade de reparação dos danos ocasionados por estas aos seus consumidores provenientes da venda ou prestação de seus serviços.

A responsabilidade civil das Instituições Financeiras, enquadra-se na responsabilidade inerente ao do serviço prestado, está baseado no art. 14, do CDC, que prevê:

> 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.
> (BRASIL, 1990).

Para o CDC, consumidor não é quem consome, e sim quem adquire ou utiliza serviços como consumidor final.

O dever de indenizar pressupõe dano, nexo causal e conduta do agente (ação ou omissão), não sendo exigida a culpa do agente, ou seja, a responsabilidade civil das Instituições financeiras é objetiva.

Na responsabilidade objetiva, o dever de indenizar o dano, independe que fique comprovado a culpa ou dolo, restando comprovado o nexo causal.

As instituições financeiras são responsabilizadas por danos sofridos pelo consumidor, ficando obrigadas a indenizar as vítimas pelos prejuízos causados, independente de culpa, assim como são responsáveis por manter a segurança de suas operações financeiros, e localizar os infratores responsáveis pelas fraudes. (BRASIL, 1990).

In verbis: "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". (BRASIL, 1990).

Para reafirmar esse entendimento a súmula 479 do STJ prevê: "As instituições Financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a

fraudes e delitos praticados por terceiros no âmbito de operações bancárias". (BRASIL, 2012c). Por exemplo: abertura de conta corrente com documentos falsos, clonagem de cartão de crédito, violação de sistema computador por *crackers*, se essas fraudes ou delitos contra o sistema bancário resultarem em danos para o correntista, dado que a responsabilidade provém do risco da atividade econômica bancária, no caso, configuram fortuito interno, ou seja, a instituição bancária deve ressarcir os prejuízos ao consumidor, independente de culpa, de ser ou não o causador do dano. (VILLAR, 2015).

Recente julgado do Egrégio Tribunal de Justiça de Minas Gerais, responsabilizando a instituição financeira objetivamente, pelos prejuízos sofridos pela vítima:

> AGRAVO DE INSTRUMENTO - AÇÃO DE DECLARAÇÃO DE INEXISTÊNCIA DE DÉBITO - TUTELA DE URGÊNCIA - ABSTENÇÃO DE COBRANÇA DE VALORES E DE INSCRIÇÃO DO AGRAVANTE NO ROL DE DEVEDORES - **GOLPE "PHISHING" - FRAUDE BANCÁRIA - REQUISITOS PREENCHIDOS -- RECURSO A QUE SE DÁ PROVIMENTO**. - Como é cediço, a concessão da tutela de urgência depende do preenchimento dos requisitos previstos no art. 300 do CPC, especificamente a probabilidade do direito alegado e o perigo da demora. Como fornecedor na relação de consumo, a instituição financeira responde objetivamente pelos danos ocasionados aos consumidores pela ocorrência de falha na prestação dos serviços. Configura falha na prestação dos serviços por parte da instituição financeira a ocorrência de fraude bancária pela aplicação do golpe denominado "**phishing"**, sobretudo quando há comprovação de que o agente financeiro, ciente da existência do golpe, não adotou todas as medidas que estava ao seu alcance para cientificar os consumidores e, principalmente, minimizar a incidência da fraude por meio de eficiente sistema de segurança que detecta operações financeiras estranhas ao perfil do cliente. Considerando que no presente caso a parte recorrente demonstrou nessa fase sumária, a ocorrência de falha na prestação de serviço, impõe-se o provimento do recurso. (TJMG - Agravo de Instrumento-Cv 1.0000.21.030411-9/001, Relator(a): Des.(a) Lílian Maciel, 20ª CÂMARA CÍVEL, julgamento em 22/09/2021, publicação da súmula em 23/09/2021). (BRASIL, 2012c).

A responsabilidade civil das instituições financeiras somente poderá ser afastada, se restar provado que o ato ilícito aconteceu, mesmo após a instituição ter tomado todas as medidas de segurança, para resguardar dados e conta do cliente, por culpa exclusiva da vítima ou do terceiro (art. 14, § 3° II, do CDC). (BRASIL, 1990).

Importante mencionar que em relação a seus clientes, a responsabilidade da Instituição é contratual, e em relação a não correntistas, as responsabilidade é extracontratual, continuando a ser objetiva a responsabilidade da Instituição financeira, conforme trazida pelo CDC: "Art. 17. Para os efeitos desta Seção, que cuida da responsabilidade dos fornecedores pelo fato do produto e do serviço, equiparam-se aos consumidores todas as vítimas do evento". (BRASIL, 1990).

Situações recentes, como as que envolvem o Pix, o novo sistema de transferência instantânea, implementada no final do ano de 2020 pelo Bacen, o ordenamento jurídico brasileiro tem se posicionado tanto a favor das instituições financeiras, quanto a favor dos clientes vítimas de fraudes. (GOLPES..., 2021).

4.5.2 Responsabilidade dos provedores

A expressão provedor de serviços de Internet, refere-se à pessoa natural ou jurídica que fornece serviços relacionados ao funcionamento da internet, ou por meio dela, ou seja, é todo aquele que viabiliza, direta ou indiretamente, "[...] meios materiais hábeis a manter os indivíduos conectados à rede mundial de computadores. São os provedores de serviço que permitem o estabelecimento da conexão entre os internautas e o meio digital". (COLAÇO, 2015, n.p.).

Como pode-se observar:

> Em linhas gerais, a responsabilidade civil pela prática de atos ilícitos na rede é imputada à pessoa natural ou jurídica que tenha efetivamente praticado o ato. Uma vez identificado e localizado, o usuário responsável arcará com as consequências. Em algumas situações, porém, essa responsabilidade pode ser imputada também aos provedores de serviços de internet. (LEONARDI, 2019 p. 73).

Para Leonardi (2019, p. 103): Os principais deveres que podem ser legalmente impostos aos provedores de serviços de internet são:

a) Utilizar tecnologias apropriadas;
b) Conhecer os dados de seus usuários;
c) Manter informações por tempo determinado;
d) Manter em sigilo os dados dos usuários;
e) Não monitorar, não censurar e informar em face de ato ilícito cometido por usuário;

Seu descumprimento gera responsabilidade direta, quando se referir a ato próprio ou corresponsabilidade por ato de terceiro, quando tal ato puder ser prevenido ou interrompido em razão de falha ou defeito.

Alguns pontos representavam controvérsias na jurisprudência brasileira como:

- se os provedores de serviços deveriam ou não utilizar meios e equipamentos tecnológicos para identificarem usuários, que praticavam ilícitos, e disponibilizar informações a quem necessitasse de direito;

- necessidade de ajuizamento de ação judicial específica para obtenção dos dados dos usuários que praticam atos ilícitos;

- deveriam ou não guardar dados a respeito de usuários para fins de investigação de ilícitos, quais dados, por quanto tempo, quem teria acessa a esses dados, quais medidas de segurança e sigilo sobre os dados;

- eventual remoção ou bloqueio de conteúdo;

Todos esses embates resultaram em normas específicas, com previsão na lei do Marco Civil da Internet, exemplo é o art. 19 da referida Lei:

> Art. 19. Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário.
> (BRASIL, 2014).

Outra possibilidade, é a responsabilização dos provedores de Internet pelos prejuízos provenientes de *phishing* e suas variações. Como os fraudadores não são facilmente identificados ou estão fora do território, onde não estão sujeitos à legislação pátria, discute-se a possibilidade da responsabilização de outros intermediários do processo, como os provedores de hospedagem de conteúdo na Internet (sítios e páginas eletrônicas).

Para a maioria da doutrina, os provedores de internet, não devem ser responsabilizados pelas fraudes eletrônicas, embora outros doutrinadores discordem.

Convém mencionar que a página eletrônica utilizada, na fraude, fica hospedada em um provedor, mesmo que não pratique o ilícito, fornece os meios materiais e físicos (tecnológicos) para a sua realização. Embora não seja o responsável direto pela fraude, é no seu sistema que o conteúdo da fraude é armazenado, o que, de certo modo, pode relacioná-lo ou vinculá-lo ao autor direto do ato ilícito. (COLAÇO, 2015).

4.5.3 Responsabilidade da vítima

A culpa exclusiva da vítima afasta a responsabilidade de ressarcimento de fraudes eletrônica por parte da instituição financeira. O Código de Defesa do Consumidor traz essa possiblidade em seu art. 14, § 3° II:

> 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:
> [...] II - a culpa exclusiva do consumidor ou de terceiro.
> (BRASIL, 1990).

Recentes julgados do Tribunal de Justiça de Santa Catarina, com a responsabilidade objetiva da instituição financeira afastada:

> APELAÇÃO CÍVEL. AÇÃO CONDENATÓRIA. FRAUDE NA EMISSÃO DE BOLETO BANCÁRIO. SENTENÇA DE PROCEDÊNCIA.
> INSURGÊNCIA DA REQUERIDA.
> PRELIMINAR. PEDIDO DE DENUNCIAÇÃO À LIDE. INSUBSISTÊNCIA. RELAÇÃO DE CONSUMO. INTELIGÊNCIA DA SÚMULA 83 DO STJ.
> "É vedada a denunciação da lide nas relações de consumo, nos termos do art. 88 do CDC" (AgRg no REsp 1288943/SP, Rel. Ministro JOÃO OTÁVIO DE NORONHA, TERCEIRA TURMA, julgado em 15/9/2015, DJe 21/9/2015).
> **ALEGADA INEXISTÊNCIA DE ATO ILÍCITO, SOB O ARGUMENTO DE QUE A FRAUDE SE CONSUMOU POR AUSÊNCIA DE CAUTELA DA PRÓPRIA PARTE AUTORA**. ACOLHIMENTO. FRAUDE EM BOLETOS DE QUITAÇÃO DE DÍVIDA EMITIDO PELA EMPRESA CREDORA. AUSÊNCIA DE COMPROVAÇÃO DA PARTICIPAÇÃO DA REQUERIDA OU DE SEUS PREPOSTOS NA PERPETRAÇÃO DA FRAUDE OU FALHA NA PRESTAÇÃO DE SERVIÇOS. EMISSÃO DE BOLETO QUE FOI REALIZADA FORA DOS CANAIS OFICIAIS DA INSTITUIÇÃO BANCÁRIA. REMESSA POR MENSAGEM ELETRÔNICA (E-MAIL) PELA EMPRESA CREDORA E INTERCEPTADA POR TERCEIRO. ADULTERAÇÃO DO CÓDIGO DE BARRA E DA EMPRESA BENEFICIÁRIA. RESPONSABILIDADE OBJETIVA AFASTADA. CULPA EXCLUSIVA DA VÍTIMA QUE NÃO AGIU COM AS CAUTELAS NECESSÁRIAS EM SE CERTIFICAR DA VERACIDADE DO DOCUMENTO, MESMO DIANTE DE TANTOS INDICIOS DE QUE SE TRATAVA DE ATO FRAUDULENTO. NEXO DE CAUSALIDADE INEXISTENTE. AUSENTE O DEVER DE INDENIZAR. INTELIGÊNCIA DO ARTIGO 14, § 3º, II DO CDC. SENTENÇA REFORMADA. INVERSÃO DOS ÔNUS SUCUMBENCIAIS. HONORÁRIOS RECURSAIS. INVIABILIDADE RECURSO DA REQUERIDA CONHECIDO E PROVIDO.
> (TJSC, Apelação n. 5000295-89.2019.8.24.0050, do Tribunal de Justiça de Santa Catarina, rel. José Agenor de Aragão, Quarta Câmara de Direito Civil, j. 19-08-2021). (SANTA CATARINA, 2021).

Como se pode perceber, no julgado acima, a vítima não pôde ressarcir seus prejuízos.

> APELAÇÃO CÍVEL. AÇÃO DECLARATÓRIA DE INEXISTÊNCIA DE DÉBITO C/C COMPENSATÓRIA DE DANOS MORAIS. AUTORA QUE, ALMEJANDO REEMITIR BOLETO PARA PAGAMENTO DE PARCELA DE FINANCIAMENTO CONTRATADO JUNTO À RÉ, TERIA SIDO DIRECIONADA, AO ACESSAR O SITE DA INSTITUIÇÃO FINANCEIRA, A CONTATO COM ESTELIONATÁRIO VIA APLICATIVO "WHATSAPP" E A PAGAR A ELE O VALOR DA PRESTAÇÃO, RESULTANDO EM INSCRIÇÃO DE SEU NOME NO CADASTRO DO SERASA. SENTENÇA DE IMPROCEDÊNCIA. INSURGÊNCIA DA AUTORA.
> INSISTÊNCIA NA ILICITUDE DO APONTAMENTO. INSUBSISTÊNCIA. INVERSÃO DO ÔNUS DA PROVA (ART. 6º, INC. VIII, CDC) QUE NÃO AFASTA O ÔNUS DA PARTE AUTORA DE DEMONSTRAR, AINDA QUE MINIMAMENTE, OS FATOS CONSTITUTIVOS DO SEU DIREITO (ART. 373, I, CPC). ACERVO PROBATÓRIO A INDICAR TER A CONSUMIDORA

> SIDO VÍTIMA DE "**PHISHING**", POIS ACESSOU SITE FALSO EM QUE DIRECIONADA A FAZER CONTATO COM O FALSÁRIO NO APLICATIVO DE MENSAGENS REFERIDO. SEQUÊNCIA DE EVENTOS CUJA **RESPONSABILIDADE NÃO PODE SER IMPUTADA À INSTITUIÇÃO FINANCEIRA**, MAS SIM À FALTA DE CAUTELA DA PRÓPRIA AUTORA. FORTUITO EXTERNO. INAPLICABILIDADE DA SÚMULA 479 DO STJ. PRECEDENTES DESTA CORTE. IMPROCEDÊNCIA DA PRETENSÃO INAUGURAL MANTIDA. PLEITO PELA CONDENAÇÃO DA RÉ ÀS PENALIDADES DECORRENTES DE PRÁTICA DE ATO ATENTATÓRIO À DIGNIDADE DA JUSTIÇA E DE LITIGÂNCIA DE MÁ-FÉ POR CONTA DE SUPOSTO DESCUMPRIMENTO À TUTELA DE URGÊNCIA ANTERIORMENTE CONCEDIDA. AUSÊNCIA DE PROVAS, CONTUDO, DE INOBSERVÂNCIA À ORDEM JUDICIAL. RECURSO CONHECIDO E DESPROVIDO. (TJSC, Apelação n. 5001582-92.2019.8.24.0016, do Tribunal de Justiça de Santa Catarina, rel. Saul Steil, Terceira Câmara de Direito Civil, j. 27-10-2020). (SANTA CATARINA, 2020).

Dessa forma, sendo invocada a culpa exclusiva da vítima, cabe a Instituição Financeira, o ônus de provar tal incumbência.

4.6 FORMAS DE PREVENÇÃO: EDUCAÇÃO DIGITAL

Com atual sociedade cada vez digital, é necessário orientar e educar os usuários quanto às condutas praticadas nos ambientes virtuais.

Educar na sociedade digital não é apenas ensinar como usar os aparatos tecnológicos ou fazer efetivo uso da tecnologia no ambiente escolar. Educar é preparar indivíduos adaptáveis e criativos com habilidades que lhes permitam lidar facilmente com a rapidez na fluência de informações e transformações. É preparar cidadãos digitais éticos para um novo mercado de trabalho cujas exigências tendem a ser maiores que as atuais. (PINHEIRO, 2021 p. 543).

É extremamente necessário que pais e escolas invistam na educação digital de seus filhos. Já não basta apenas orientá-los a não abrir a porta de casa para estranhos. Eles precisam saber também que não é seguro abrir e-mails de estranhos. Esse tipo de ensinamento deve ser aplicado e, atividades lúdicas e escolares, para, no futuro, ser adotado também no ambiente profissional. (PINHEIRO, 2021 p. 542)

Pinheiro (2021, p. 392) aduz que o maior problema jurídico dos crimes virtuais ainda é o fato de que os criminosos estão sempre um passo à frente. Há necessidade de investir mais no preparo da polícia para que tenham mais ferramentas para realizar perícia digital forense, bem como também em campanhas educativas da população, para que o cidadão saiba se defender melhor dos novos tipos de golpes e ameaças digitais. Além disso, a ação rápida, para pegar o "bandido com a mão na máquina" é essencial.

Existem várias medidas e cuidados que o usuário pode tomar para que não seja vítima de crimes virtuais nos ambientes virtuais bancários, que podem acarretar uma série prejuízos financeiros.

Segue cartilha de segurança para internet publicada pelo CERT.br, referentes ao uso do *Internet Banking*:

1) Certifique-se de usar computadores e dispositivos móveis seguros

2) Digite o endereço do site bancário diretamente no navegador web:

a) evite seguir ou clicar em *links* recebidos via mensagens eletrônicas (*e-mails*, mensagens SMS, redes sociais etc.);

b) Não utilize sites de busca para localizar o site bancário;

3) Sempre acesse sua conta usando a página ou o aplicativo fornecido pelo próprio banco;

4) Antes de instalar um módulo de proteção, certifique-se de que o autor do módulo é realmente a instituição em questão;

5) Evite usar dispositivos móveis e computadores de terceiros (como lan houses e Internet cafés): não há garantias de que os equipamentos estejam seguros;

6) Evite usar redes Wi-Fi públicas;

7) Utilize um endereço terminado em "b.br", caso seu banco ofereça essa opção: domínios terminados em "b.br", além de serem de uso exclusivo de instituições bancárias, também oferecem recursos adicionais de segurança;

8) Certifique-se de usar conexões seguras. Alguns indícios desse tipo de conexão são:

a) o endereço do site começa com https:// ;

b) o desenho de um "cadeado fechado" é mostrado na barra de endereço, ao clicar sobre ele, são exibidos detalhes sobre a conexão/certificado digital em uso;

c) um recorte colorido (branco ou azul) com o nome do domínio do site é mostrado ao lado da barra de endereço (à esquerda ou à direita), ao passar o mouse ou clicar sobre ele, são exibidos detalhes sobre conexão/certificado digital em uso;

d) a barra de endereço e/ou o recorte são apresentados na cor verde e no recorte é colocado o nome da instituição dona do site;

Outros cuidados a serem observados, em consonância com a Cartilha elaborada por CERT.br (2020):

1) Forneça apenas uma posição do seu cartão de segurança, desconfie caso, em um mesmo acesso, seja solicitada mais de uma posição;

2) Mantenha o número do seu celular atualizado, caso o tenha cadastrado, ele é utilizado para o envio de mensagens de confirmação e códigos de liberação de transações;
3) Use sempre a opção de "sair" quando deixar de utilizar seu *Internet Banking*;
4) Seja cuidadoso com mensagens sobre promoções;
5) Evite acessar a central de atendimento do seu banco por meio de celulares de terceiros, os dados digitados, como número da sua conta bancária e sua senha, podem ficar armazenados;
6) A maioria dos bancos não envia e-mails sem autorização prévia, desconsidere mensagens que receber, caso não tenha autorizado previamente o envio e principalmente de instituições com as quais você não tenha relação;
7) Verifique periodicamente o extrato da sua conta bancária e do seu cartão de crédito;
8) Entre imediatamente em contato com a central de relacionamento do seu banco, diretamente com o seu gerente ou com a operadora do seu cartão de crédito.

Segue Cartilha com dicas para se proteger de golpes, na internet, referentes ao *Phishing:*

1) fique atento a mensagens, recebidas em nome de alguma instituição, que tentem induzi-lo a fornecer informações, instalar/executar programas ou clicar em links;
2) questione-se por que instituições com as quais você não tem contato estão lhe enviando mensagens, como se houvesse alguma relação prévia entre vocês (por exemplo, se você não tem conta em um determinado banco, não há por que recadastrar dados ou atualizar módulos de segurança);
3) fique atento a mensagens que apelem demasiadamente pela sua atenção e que, de alguma forma, o ameacem caso você não execute os procedimentos descritos;
4) não considere que uma mensagem é confiável com base na confiança que você deposita em seu remetente, pois ela pode ter sido enviada de contas invadidas, de perfis falsos ou pode ter sido forjada;
5) seja cuidadoso ao acessar links. Procure digitar o endereço diretamente no navegador Web;
6) verifique o link apresentado na mensagem. Golpistas costumam usar técnicas para ofuscar o link real para o *phishing*. Ao posicionar o mouse sobre o link, muitas vezes é possível ver o endereço real da página falsa ou código malicioso;
7) utilize mecanismos de segurança, como programas *antimalware*, firewall pessoal e filtros *antiphishing;*

8) verifique se a página utiliza conexão segura. Sites de comércio eletrônico ou *Internet Banking* confiáveis sempre utilizam conexões seguras quando dados sensíveis são solicitados;
9) verifique as informações mostradas no certificado. Caso a página falsa utilize conexão segura, um novo certificado será apresentado e, possivelmente, o endereço mostrado no navegador *Web* será diferente do endereço correspondente ao site verdadeiro;
10) acesse a página da instituição que supostamente enviou a mensagem e procure por informações (você vai observar que não faz parte da política da maioria das empresas o envio de mensagens, de forma indiscriminada, para os seus usuários). (CARTILHA, 2020).

Quando o indivíduo é vítima de fraude virtual, o primeiro passo é fazer um BO na delegacia mais próxima, não importando se é especializada ou não em crimes virtuais. As ocorrências podem ser registradas via internet nas delegacias virtuais, em Santa Catarina pelo link: https://delegaciavirtual.sc.gov.br/inicio.aspx.

No Brasil existem hoje pouquíssimas delegacias especializadas em crimes virtuais, somente em alguns estados, sendo que. em Santa Catarina, há somente uma, que se localiza-se na capital catarinense, foi inaugurada em março de 2002.. (SANTA CATARINA, 2002).

Em consonância com Delegacia de Polícia Virtual de Santa Catarina, essa delegacia presta serviço de registro de ocorrências disponibilizado ao Cidadão via Internet, 24 horas por dia.

Ainda, excepcionalmente, e em caráter temporário (período de adoção de medidas de prevenção ao Covid-19),

> [...] é possível a comunicação via internet de “todos os fatos” atendidos pela Polícia Civil do Estado de Santa Catarina, com exceção dos seguintes fatos típicos (crimes), cujo atendimento será realizado de forma presencial em qualquer Delegacia de Polícia do Estado: Homicídio (art. 121, CP), Latrocínio (art. 157, §3, CP), Extorsão mediante sequestro (art. 159, CP), Furto e roubo de veículos e de cargas (art. 157, CP). (SANTA CATARINA, 2002).

Estas são algumas das orientações para que o usuário possa realizar suas transações financeiras no ambiente digital de forma segura, tomando alguns cuidados, evitando, em vista disso, cair em golpes e evitando prejuízos financeiros que possam ser ocasionados.

4.7 DIREITO BRASILEIRO APLICÁVEL À INTERNET

4.7.1 Lei 12.735/2012

A referida Lei 12.735/12 tipifica condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados.

O PL 84/99 que deu origem à lei era bastante extenso e criou polêmica quanto à responsabilização dos provedores de internet, durante sua tramitação foi reduzida somente a quatro artigos, dos quais dois foram vetados pela presidente Dilma Rousseff.

A lei determinou que as polícias civis dos estados brasileiros criem setores e equipes especializadas no combate aos crimes virtuais, conforme descrito no art. 4º: "Art. 4º Os órgãos da polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado". (BRASIL, 1940).

No Brasil, as forças policiais ainda carecem de treinamento e estruturas adequadas para que possam enfrentar com eficiência os delitos virtuais. (CASSANTI, 2014).

4.7.2 Lei 12.737/2012 e Lei 14.155/2021

Esta lei trata das tipificações das condutas criminais dos delitos informáticos. Popularmente conhecida com a Lei Carolina Dieckmann, enquanto ainda projeto de Lei, teve o ocorrido com a atriz, que teve seu computador invadido e fotos íntimas vazadas, vem com intuito de tipificar essas condutas delituosas. Incluiu e alterou alguns artigos do CP, como os Art. 154 A, 154 B, 266 e 298.

I - Invasão de dispositivo informático (arts. 154-A, 154-B, do CP)

Este artigo foi incluído pela Lei 12.737, e posteriormente alterado pela Lei 14.155, em 27 de maio de 2021, tornando as punições para os crimes de violação de dispositivo eletrônico, estelionato e furto, cometidos via internet ou por dispositivo informático, mais severas.

Redação do artigo antes da alteração promovida pela Lei 14.155 de 2021:

> Art. 154 A - 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: **Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa**.
> § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.

> § 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
> § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
> Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.
> § 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.
> § 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:
> I - Presidente da República, governadores e prefeitos;
> II - Presidente do Supremo Tribunal Federal;
> III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou
> IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal (BRASIL, 1940 [2021])

Apresenta-se como ficou a redação do artigo pós alteração pela Lei 14.155/21:

> Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita: (Redação dada pela Lei nº 14.155, de 2021)
> Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa. (Redação dada pela Lei nº 14.155, de 2021) (BRASIL, 2021).
> [...] § 2º Aumenta-se a pena de 1/3 (um terço) a 2/3 (dois terços) se da invasão resulta prejuízo econômico (Redação dada pela Lei nº 14.155, de 2021).
> § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido: (Incluído pela Lei nº 12.737, de 2012) Vigência.
> Pena – reclusão, de 2 (dois) a 5 (cinco) anos, e multa. (Redação dada pela Lei nº 14.155, de 2021). (BRASIL, 1940 [2021]).

A lei promoveu diversas alterações no artigo:

a) Não é necessário que seja violado dispositivo de segurança para configurar crime, a simples invasão já caracteriza a conduta;
b) Antes a lei mencionava invadir dispositivo informático alheio, agora, invadir dispositivo informático de uso alheio, ou seja, de uso de terceiro;
c) Configura crime invadir sem autorização expressa ou tácita do usuário, e não mais do titular do dispositivo, ou seja, o sujeito passivo do crime, não precisa ser necessariamente o proprietário, podendo a invasão ocorrer em um dispositivo que esteja sendo utilizado por alguém, que não o seu dono. Como exemplo computadores utilizados em empresas por vários usuários;

d) Majorou a pena, de detenção de 3 (três) meses a 1 (um) ano, e multa, para reclusão de 1 (um) a 4 (quatro) anos e multa;
e) Majorou os limites das causas de aumento, de 1/3 (um terço) a 2/3 (dois terços), caso cause prejuízo financeiro (causa de aumento);
f) Majorou a pena da qualificadora, prevista no §3º, reclusão de 2 (dois) a 5 (cinco) anos; se da invasão obter comunicações eletrônicas privadas como por exemplo: *e-mails*, *sms*, aplicativo de mensagens, segredos comerciais ou industriais, ou informações sigilosas, ou obter o controle remoto do dispositivo invadido.
(BRASIL, 1940 [2021]).

O bem jurídico protegido neste tipo penal é a privacidade, sendo invioláveis a intimidade e a vida privada, valores protegidos constitucionalmente (art. 5º, X, da CF/88). (BRASIL, 1988).

No tocante aos crimes virtuais, a Lei 12.737/2012 estabelece que as práticas criminosas previstas no art. 154-A, só se procederão através de representação do ofendido.

> **Ação penal**
> Art. 154-B - Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos. (BRASIL, 2012).

Dessa forma, a ação será pública, condicionada à representação da vítima, exceto se o crime ocorrer contra a administração pública direta ou indireta da União, Estados, Distrito Federal e Municípios, ou ainda concessionárias de serviços públicos, visto que, para estes, a ação penal será pública incondicionada.

Posto isto, o art. 154-B, vem para dispor qual tipo de ação penal deve ser movida, a fim de que a vítima tenha seu bem jurídico protegido, e o sujeito ativo do crime receba sua devida punição. (BRASIL, 1940).

A referida lei também trouxe nova redação ao art. 266:

> **Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública** (Redação dada pela Lei nº 12.737, de 2012)
> Art. 266 - Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento:
> Pena - detenção, de um a três anos, e multa.
> § 1º Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento. (Incluído pela Lei nº 12.737, de 2012)
> § 2º Aplicam-se as penas em dobro se o crime é cometido por ocasião de calamidade pública (Incluído pela Lei nº 12.737, de 2012). (BRASIL, 2012).

Entende-se por serviço telegráfico o serviço referente à transmissão de mensagens à distância, através de fios, código de sinais; o serviço radiotelegráfico, como sendo o serviço de transmissão de mensagens através de ondas eletromagnéticas, através de códigos de sinais; e serviço telefônico, como o serviço de transmissão de sons à distância por fios ou ondas. (SANTOS, 2020).

Equiparou na mesma pena quem interrompe ou dificulta o restabelecimento do serviço (art. 266, §1º, CP) e trouxe causa de aumento, no caso de o crime ser cometido por ocasião de calamidade pública (art. 266, §2º, CP). (BRASIL, 1940).

II – Alterações no Crime de Furto (art. 155 do CP)

A recente Lei também promoveu alterações no crime de furto.

> **Furto Qualificado**
> § 4º-B. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se o furto mediante fraude é cometido por meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem a violação de mecanismo de segurança ou a utilização de programa malicioso, ou por qualquer outro meio fraudulento análogo. (Incluído pela Lei nº 14.155, de 2021)
> § 4º-C. A pena prevista no § 4º-B deste artigo, considerada a relevância do resultado gravoso: (Incluído pela Lei nº 14.155, de 2021)
> I – 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; (Incluído pela Lei nº 14.155, de 2021)
> II – aumenta-se de 1/3 (um terço) ao dobro, se o crime é praticado contra idoso ou vulnerável. (Incluído pela Lei nº 14.155, de 2021).
> (BRASIL, 1940).

Com a nova Lei, caso o agente invada o dispositivo informático da vítima, instalando programas maliciosos, rastreando senhas, e subtraindo valores da conta bancária da vítima, será aplicativo o tipo penal específico do §4º B, furto mediante fraude por meio de dispositivo eletrônico ou informático, conectado ou não a internet, violando ou não mecanismo de segurança, ou programas maliciosos, e não mais o art. 155, § 4º, II, do CP (furto mediante fraude). (BRASIL, 1940).

A pena é majorada, se o autor da subtração utilizar de conexão internacional, isso se deve em razão do fato apresentar uma ameaça à soberania nacional, ou se o delito for cometido contra idoso (pessoa com idade igual ou superior a 60 anos) ou vulnerável (, circunstâncias essas, merecedoras de uma maior punição. Para que o criminoso responda pelas causas de aumento é necessário que haja dolo (vontade e ciência), ou seja, saiba que está utilizando um servidor mantido no exterior ou saiba que sua vítima seja idosa ou vulnerável. (CUNHA, 2021).

III – Alterações no crime de Estelionato (art. 171 do CP)

> **Fraude eletrônica**
> §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.
> (BRASIL, 1940).

O agente que obtêm vantagem através de informações retiradas da própria vítima ou terceiro induzido a erro, sendo tal vantagem por meio eletrônico: redes sociais, contatos telefônicos (ligação de central), *e-mail, links*.

O crime de estelionato também passou a ter uma qualificadora (art. 171, §2º-A, CP), semelhante ao do furto, mas a lei não faz referência a dispositivo eletrônico ou informático. (BRASIL, 1940). Condutas em que a vantagem é obtida por informações obtidas através da própria vítima ou por terceiro induzido a erro são consideradas mais gravosas:

a) Através de redes sociais: anúncio ofertado pelas redes sociais são muito comuns, sendo alguns deles fraudulentos, com armadilhas para que as pessoas forneçam seus dados pessoais;
b) Contatos telefônicos: as fraudes por este meio se tornaram muito frequentes, normalmente o estelionatário se passa por amigo ou familiar da vítima, geralmente por *WhatsApp*, e solicitando certa quantia por transferência ou depósito, não raras vezes a vítima efetua o que o criminoso pede.
c) *E-mail* fraudulento ou *links*: normalmente a vítima recebe um correio eletrônico de contato ou empresa conhecida, e a partir de links clicados, insere dados confidenciais, como números de cartão de crédito e senhas.
d) Outros meios fraudulentos análogos: aqui incluem-se outras abordagens fraudulentas que não são feitas diretamente pelo estelionatário, em que as vítimas são induzidas a erro como páginas falsas de *sites* conhecidos.

Nos casos de estelionato, ao contrário do crime de furto mediante fraude, a vítima, fornece informações para o estelionatário para a obtenção da vantagem indevida. No crime de furto mediante fraude, a vítima não percebe o meio ardil que está sendo envolvida.

A pena é majorada caso o crime praticado seja realizado mediante servidor mantido fora do país, de 1/3 (um terço) a 2/3 (dois terços) (art. 171, § 2º-B, CP). (BRASIL, 1940).

Um ponto importante é o crime cometido contra idoso, em que a pena pode variar de 1/3 (um terço) ao dobro (art. 171, § 4º, CP), pena esta, que foi amenizada em relação a Lei anterior (13.228/2015), que determinava a aplicação da pena em dobro, em caso do crime ser cometido contra pessoa idosa. (BRASIL, 1940).

Acrescentou o §4º no art. 70 no CPP para prever nos crimes de estelionato do art. 171 do CP quando praticados mediante depósito, emissão de cheques sem suficiente provisão de fundos em poder do sacado ou com o pagamento frustrado ou mediante transferência de valores, que a competência será definida pelo local do domicílio da vítima, e, em caso de pluralidade de vítimas, a competência firmar-se-á pela prevenção. (BRASIL, 1941).

A lei tornou os crimes de violação de dispositivo informático, estelionato e furto mediante fraude, cometidos eletronicamente ou pela internet, mais graves, aplicando penas mais rígidas, saindo de penas excessivamente brandas para aplicação de medidas mais gravosas.

A pandemia da Covid-19 mudou drasticamente as rotinas das pessoas, juntamente vieram as medidas de isolamento, o aumento do uso e dependência dos canais virtuais, o que refletiu diretamente na incidência dos crimes virtuais.

Estas medidas de alterações, trazidas pela recente lei 14.155/21 são vistas positivamente, uma vez que o legislador deve acompanhar a evolução da sociedade, buscando tutelar os interesses do cidadão de forma geral, atualizar o Código Penal, ante as mudanças sofridas frequentemente no mundo digital.

4.7.3 Lei 13709/2018 - Lei geral de proteção de dados ou LGPD

É objetivo da Lei Geral da Proteção de Dados ou LGPD proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Essa lei também tem a finalidade de criar uma conjuntura de segurança jurídica, padronizando "[...] regulamentos e práticas para promover a proteção aos dados pessoais de todo cidadão que esteja no Brasil, de acordo com os parâmetros internacionais existentes". (BRASIL, [2018?]a).

> 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 (BRASIL, 2019)
> Parágrafo único. As normas gerais contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios. (BRASIL, 2018).

A lei dispõe sobre o tratamento de dados feito por pessoa física ou jurídica de direito público ou privado, e compreende tanto operações feitas nos mecanismos digitais ou físicos.

É uma regulamentação considerada bastante técnica e que traz mais do que regras tratadas e diretrizes: traz princípios, direitos e obrigações relacionados ao uso das bases de dados pessoais, um importante e relevante ativo na sociedade atual. (PINHEIRO, 2021).

Segundo a LGPD:

> [...] é considerado "dado pessoal" qualquer informação que permita identificar, direta ou indiretamente, uma pessoa que esteja viva, tais como: nome, RG, CPF, gênero, data e local de nascimento, telefone, endereço residencial, localização via GPS, retrato em fotografia, prontuário de saúde, cartão bancário, renda, histórico de pagamentos, hábitos de consumo, preferências de lazer; endereço de IP (Protocolo da Internet) e cookies. (BRASIL, [2018?]a).

O art. 5º da LGPD considera:

> I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
> II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural; [...].
> (BRASIL, 2019)

Os dados sensíveis referem-se ao posicionamento político, orientação sexual, religião, etnia, sexo, dados bancários. Sendo as informações bancárias, consideradas como dados sensíveis, por conseguinte, podem ser tratadas somente com consentimento do usuário.

A LGPD tem como fundamentos:

- o respeito à privacidade;
- a autodeterminação informativa;
- a liberdade de expressão, de informação, de comunicação e de opinião;
- a inviolabilidade da intimidade, da honra e da imagem;
- o desenvolvimento econômico e tecnológico e a inovação;
- a livre iniciativa, a livre concorrência e a defesa do consumidor; e
- os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

A lei é aplicável para dados relacionados à pessoa física ou jurídica (de direito público ou privado) brasileiras ou não, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, que estejam no Brasil, no momento da coleta, dados tratados

dentro do território nacional, dados utilizados para fornecimento de bens ou serviços, conforme dispõe em seu art. 3º da referida Lei.

Não se aplica para fins jornalísticos e artísticos; acadêmicos (aplicando-se a esta hipótese os arts. 7º e 11 desta Lei), segurança pública, defesa nacional, segurança do Estado, atividades de investigação e repressão de infrações penais, por particulares e não econômicos, e de dados provenientes de fora do território nacional e não sejam objetos de transferência internacional (art. 4º, LGPD).

Como titular de dados pessoais, diversos direitos são garantidos pela LGPD, em seu art. 18:

> Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:
> I - confirmação da existência de tratamento;
> II - acesso aos dados;
> III - correção de dados incompletos, inexatos ou desatualizados;
> IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;
> V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; (Redação dada pela Lei nº 13.853, de 2019) Vigência
> VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;
> VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
> VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
> IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.
> § 1º O titular dos dados pessoais tem o direito de peticionar em relação aos seus dados contra o controlador perante a autoridade nacional.
> § 2º O titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto nesta Lei.
> § 3º Os direitos previstos neste artigo serão exercidos mediante requerimento expresso do titular ou de representante legalmente constituído, a agente de tratamento.
> § 4º Em caso de impossibilidade de adoção imediata da providência de que trata o § 3º deste artigo, o controlador enviará ao titular resposta em que poderá:
> I - comunicar que não é agente de tratamento dos dados e indicar, sempre que possível, o agente; ou
> II - indicar as razões de fato ou de direito que impedem a adoção imediata da providência.
> § 5º O requerimento referido no § 3º deste artigo será atendido sem custos para o titular, nos prazos e nos termos previstos em regulamento.
> § 6º O responsável deverá informar, de maneira imediata, aos agentes de tratamento com os quais tenha realizado uso compartilhado de dados a correção, a eliminação, a anonimização ou o bloqueio dos dados, para que repitam idêntico procedimento, exceto nos casos em que esta comunicação seja comprovadamente impossível ou implique esforço desproporcional. (Redação dada pela Lei nº 13.853, de 2019) Vigência
> § 7º A portabilidade dos dados pessoais a que se refere o inciso V do caput deste artigo não inclui dados que já tenham sido anonimizados pelo controlador.
> § 8º O direito a que se refere o § 1º deste artigo também poderá ser exercido perante os organismos de defesa do consumidor. (BRASIL, 2019).

Para as instituições financeiras a LGPD significa maior controle sobre os dados pessoais de clientes, funcionários e de qualquer outra pessoa que tenha suas informações tratadas. E Controle significa redução de riscos, mitigar os problemas, redução de custos. A proteção de dados, é considerada não só obrigação, mas uma vantagem competitiva e econômica. Já para o cidadão, que é o centro de todo o sistema de proteção de dados, significa controle sobre sua própria informação, implica confiança e confiança implica em melhores formas de utilização das informações. (MARINHO, 2021).

4.7.4 Convenção de Budapeste

A convenção de Budapeste é um tratado firmado, no ano de 2001, pelo Conselho da Europa. Possui 60 (sessenta) signatários, dentre os quais 44 (quarenta e quatro) são de países da Europa.

Em 2006, já existia um movimento para que o Brasil fizesse parte do tratado. Em 2019, foi convidado novamente a participar do tratado, o governo concordou, mas precisa de ratificação do Congresso Nacional.

A Comissão de Constituição e Justiça da Câmara dos deputados, aprovou o relatório em 18 de agosto de 2021, e o texto seguiu para apreciação do Plenário.

Sobre essa convenção:

> Convictos de que a presente Convenção é necessária para impedir os actos praticados contra a confidencialidade, integridade e disponibilidade de sistemas informáticos, de redes e dados informáticos, bem como a utilização fraudulenta de desses sistemas, redes e dados, assegurando a incriminação desses comportamentos tal como descritos na presente Convenção, e da adopção de poderes suficientes para combater eficazmente essas infracções, facilitando a detecção, a investigação e o procedimento criminal relativamente às referidas infracções, tanto ao nível nacional como internacional, e estabelecendo disposições materiais com vista a uma cooperação internacional rápida e fiável. (BUDAPESTE, 2001).

O tratado estabelece que os países membros, se comprometam a criar leis penais, que tipifiquem e punam condutas descritas no compromisso internacional, referentes aos crimes cibernéticos. Trata-se de um acordo internacional para estabelecer tipos penais e medidas de cooperação relacionadas aos crimes cometidos virtualmente.

A convenção é um importante instrumento de cooperação internacional digital, pois, facilita a cooperação nos assuntos referentes à internet e sistemas informáticos.

Além de conter estratégias para a tipificação, prevenção e combate aos crimes virtuais, e medidas de cooperação acerca das informações digitais, a Convenção vem com propósito de

contribuir para a cooperação internacional para a obtenção de provas digitais, que estiverem fora dos limites nacionais de seus Estados membros, durante as investigações e persecuções penais. (POLIDO, 2021)

4.7.5 Decreto 10.222/2020

Em consonância com o anexo do Decreto, o definiu como um importante instrumento de apoio ao planejamento dos órgãos e entidades do Governo, cujo objetivo foi de melhorar a segurança e a resiliência das infraestruturas críticas e dos serviços públicos nacionais. Esse documento impulsionou as discussões sobre o tema no âmbito da Administração Pública federal e, também, em outros setores da sociedade.

O decreto objetiva tornar o Brasil mais confiável no ambiente digital, aumentar a resiliência do Brasil às ameaças virtuais e fortalecendo segurança cibernética no cenário internacional.

A presente Estratégia Nacional de Segurança Cibernética - *E-Ciber* é orientação manifesta do Governo federal à sociedade brasileira sobre as principais ações por ele pretendidas, em termos nacionais e internacionais, na área da segurança cibernética e terá validade no quadriênio 2020-2023.

Um dos pontos mais importantes do Decreto se refere à preocupação com a Educação Digital.

“Construir uma sociedade conectada tem sido um desafio muito grande para o Brasil”. (BRASIL, 2020a).

Conforme o Decreto nº 10.222, de 5 de fevereiro de 2020:

> O rápido avanço tecnológico, acompanhado da transformação digital proposta para a sociedade moderna, tornou imprescindível o desenvolvimento de ações educacionais e pedagógicas para a formação em prol do uso criterioso, seguro e responsável das tecnologias. Nesse sentido, considera-se que a prioridade de investimentos em programas de educação relacionados à segurança cibernética é um pilar essencial para reduzir os riscos às empresas e à sociedade.
> Como consequência do maior acesso às redes digitais, e em virtude da pouca maturidade em segurança cibernética, o Brasil ocupa lugar de destaque no *ranking* dos países que mais recebem ataques cibernéticos. A falta de cultura em segurança cibernética, de habilitação e de conhecimento nesse tema de grande número de brasileiros conectados ao mundo digital mostra que a nossa sociedade não está preparada para o uso das ferramentas digitais com os cuidados adequados relativos à segurança cibernética. (BRASIL, 2020a).

Nesse decreto, há a recomendação para o desenvolvimento de “[...] uma cultura de segurança cibernética, por meio da educação, que alcance todos os setores da sociedade e níveis

de ensino, a fim de prevenir incidentes e proporcionar o uso responsável das tecnologias, sendo estes um dos pontos principais para o desenvolvimento do País". (BRASIL, 2020a).

5 CONCLUSÃO

O objetivo deste trabalho foi analisar se Pandemia da Covid-19 foi fator agravante para o aumento de casos de fraudes virtuais contra indivíduos que têm contas em instituição financeira, uma vez que houve aumento significativo de usuários nesse meio. Para alcançar esse objetivo, desenvolveu-se uma pesquisa exploratória com abordagem qualitativa. No que diz respeito aos procedimentos de coleta de dados, trata-se de uma pesquisa bibliográfica e documental. Foram utilizadas leis, principalmente aquelas que regulamentam, em certa medida, os crimes virtuais, como o Marco Civil da Internet e recente Lei 14.155/21 entre outros documentos legais. Também serviram de base tanto para a fundamentação teórica quanto para a análise doutrinas, artigos científicos etc.

Sabe-se que à medida que uma sociedade cria necessidades, os recursos tecnológicos se desenvolvem, no sentido de supri-las e, com isso, também a sociedade evolui. Em outros termos, o homem é produto e produtor. Desse modo, um dos grandes desafios do direito é entender e conseguir acompanhar tanto esses avanços tecnológicos quanto o próprio ser humano. O operador do direito tem papel fundamental nisso, dado que deve estar em constante atualização, dominar as novas tecnologias, conhecer as disciplinas do direito digital, com suas linguagens, terminologias e códigos.

É de conhecimento que a internet por ter amplo acesso, uso generalizado e velocidade de comunicação, fatores esses que, por si só, contribuem para aumentar os riscos provenientes da circulação neste meio e, quanto mais se faz uso dela, mais propício se torna esse meio para a prática de crimes virtuais.

Sabe-se que a internet trouxe uma série de facilidades e comodidades à sociedade, mas ao mesmo tempo despertou a atenção dos criminosos virtuais, que passaram a enxergar oportunidades, ao saber que os usuários passariam mais tempo conectados. Sendo que já existe uma tendência natural das pessoas irem migrando para os ambientes virtuais, e a Pandemia da Covid-19 acelerou este processo.

A Pandemia da Covid-19 assola o país há quase 2 (dois) anos, momento em que as pessoas tiveram que se isolar, em suas casas, como forma de conter o avanço da doença, passando a utilizar a internet para estudar, trabalhar e realizar outros serviços, tendo ela contribuído significativamente, para a potencialização destes delitos, inclusive, para o surgimento de novos crimes.

Importa considerar que internet e a criminalidade crescem em velocidade superior ao ordenamento jurídico existente, no país acerca do tema desta pesquisa, e que é de suma importância que a legislação pátria esteja atualizada e adequada aos novos crimes que surgirão, ante os avanços tecnológicos e conforme as técnicas criminosas vão se aperfeiçoando.

A lei Marco Civil da Internet, sancionada em 2014, conhecida como a "Constituição da Internet", foi um importante instrumento de regulação das relações digitais, principalmente no que tange à neutralidade da rede, inclusão digital, proteção à intimidade, sigilo de dados e orientar a relação das empresas prestadoras de serviços de internet com seus clientes.

A referida lei 12.737/12 não conseguiu alcançar todos os tipos penais e acabou por perder a chance de criar um sistema de combate aos crimes virtuais. Adicionou apenas 4 (quatro) artigos, dentre eles o art. 154 A do CP, que criou o delito de invasão de dispositivo informático, 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.

Analisando a redação do artigo, percebe-se sua insuficiência, já que não configuraria crime se não violasse dispositivo de segurança. Outro fator negativo se referia à punição, que era extremamente branda, com detenção de 3 (três) meses a 1 (um) ano e multa, possibilitando os benefícios da Lei 9.099/95.

Posteriormente, o art. 154 A foi alterado pela recente lei 14.155, sancionada em 27 de maio deste ano, que promoveu alterações também nos artigos 155 e 171 do CP, tornando as punições mais gravosas, para os crimes de violação de dispositivo informático, furto e estelionato, cometidos pela internet ou por dispositivos eletrônicos. (BRASIL, 1940 [2021a]).

Na nova redação da lei desse artigo supramencionado, o ato de invasão é considerado crime, mesmo que não viole mecanismo de segurança, também deixou de exigir que o dispositivo informático seja de propriedade do usuário do dispositivo. (BRASIL, 1940 [2021a]). O art. 155 e 171 do CP tiveram suas penas majoradas, para algumas situações, como exemplo se o crime for cometido por servidor mantido fora do país e incluindo qualificadoras. Essas alterações são vistas positivamente, uma vez a legislação deve acompanhar as atualizações do mundo digital, e aplicação de penalidades mais severas tendem a ser mais eficazes, no combate aos crimes, mas ainda não se sabe se serão suficientes para combater o tipo penal, visto o pouco tempo de sua entrada em vigor. (BRASIL, 1940 [2021a]).

As legislações nacionais, como se percebe, são suficientes, para instauração de procedimentos investigatórios e punitivos dos delitos praticados por meio da internet. Já no âmbito internacional, faz-se necessário a adesão à Convenção de Budapeste, o que facilitaria a cooperação entre seus Estados membros, em caso de acesso a dados digitais, provas, formulação de estratégias conjuntas, para criação de leis penais para tipificar, prevenir e combater os crimes virtuais.

Os delitos envolvendo *Phishing*, tipos de fraudes em que se tentam obter informações pessoais e financeiras da vítima, seja por meio de técnicas ou de engenharia social (como por exemplo páginas falsas de Bancos e e-mail com links de acesso para atualização de dados falsos), segundo a Febraban, tornaram-se um dos mecanismos mais difundidos entre os criminosos, e durante a Pandemia os números elevaram-se ainda mais, ou seja, mais usuários circulando, mais potenciais vítimas.

Ademais, o presente trabalho visou contribuir e orientar os estudiosos para aprimorar os saberes não só no campo jurídico, fornecendo informações relevantes e atualizadas acerca do tema abordado.

Ressalta-se a extrema importância de trabalhar, na prevenção dos crimes virtuais, em que se faz necessário preparar os indivíduos nos ambientes escolares, e, futuramente, nos ambientes empresariais, e ensinar não somente a utilização dos recursos tecnológicos, como também a lidar com velocidade da informação e o estrago que ela pode causar, como bem lembra a autora Patrícia Peck Pinheiro (2021): “já não basta somente não abrir a porta para estranhos, mas não abrir *e-mails* de estranhos ou fonte duvidosas”.

Por fim, é importante redobrar a atenção, quando da utilização das facilidades oferecidas pelos meios digitais, como *e-mail, links*, propagandas, atualização de dados, entre outros, para que, conseguintemente, possa-se frear a incidência das fraudes no sistema virtual das Instituições Financeiras.

REFERÊNCIAS

ABREU, Jonas**.** *Phishing, smishing e vishing*, o que são esses golpes? **Nubanc**, 14 mar. 2020. Disponível em: https://blog.nubank.com.br/phishing-vishing-smishing-golpes/. Acesso em: 12 out. 2021.

AMEAÇAS emergentes. O que é *Smishing.* **NORTON.** [2021?]. Disponível em: https://br.norton.com/internetsecurity-emerging-threats-what-is-smishing.html. Acesso em: 12 out. 2021.

BANCOS reforçam conscientização contra crimes cibernéticos na pandemia. São Paulo.

NOOMIS Ciab **FEBRABAN.** 18 set. 2020. (Não paginado). Disponível em: https://noomis.febraban.org.br/temas/seguranca/bancos-reforcam-conscientizacao-contra-crimes-ciberneticos-na-pandemia. Acesso em 18 set. 2021.

BITTENCOURT, Luis Fernando. **Crimes no universo digital**. *E-book Kindle*, 2020. *E-book*. Acesso restrito via Amazon. Acesso em: 05 abr. 2021.

BRANCO, Dácio Castelo. Sabe o que é Pharming? Conheça a ameaça e saiba como evitá-la. **Canaltech**, 10 set. 2021. (Não paginado). Disponível em: https://canaltech.com.br/seguranca/o-que-e-pharming-195474/. Acesso em 16 out. 2021.

BRASIL, **Lei nº 4.595, de 31 de dezembro de 1964**. Dispõe sobre a Política e as Instituições Monetárias, Bancárias e Creditícias, Cria o Conselho Monetário Nacional e dá outras providências. Brasília, DF: Presidência da República [1964]. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l4595.htm. Acesso em: 24 nov. 2021.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, [2020]. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 04 ago. 2021.

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990.** Dispõe sobre a proteção do consumidor e dá outras providências. Brasília, DF. Presidência da República [2017]. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 16 out. 2021.

BRASIL. **Súmula 48/STJ.** Supremo Tribunal de Justiça. Compete ao Juízo do local da obtenção da vantagem ilícita processar e julgar crime de estelionato cometido mediante falsificação de cheque. Diário de Justiça. Brasília, DF, 1992. Data da Publicação - DJ 25.08.1992 p. 13103.

BRASIL. **Lei nº 9.279, de 14 de maio de 1996**. Regula direitos e obrigações relativos à propriedade industrial. Brasília, DF. Presidência da República, 1996. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9279.htm. Acesso em: 10 nov. 2021.

BRASIL. **Lei nº 9.296, de 24 de julho de 1996**. Brasília, DF: Presidência da República, 1996a. Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9296.htm. Acesso em: 10 nov. 2021.

BRASIL. **Medida Provisória nº 2.200-2, de 24 de agosto de 2001**. Institui a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/mpv/antigas_2001/2200-2.htm. Acesso em: 30 out. 2021.

BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Brasília, DF. Presidência da República, 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/L10406compilada.htm. Acesso em: 30 out. 2021.

BRASIL. Supremo Tribunal de Justiça. **Agravo em Recurso Especial nº 1.418.119 – DF 2018/0333774-2**. 2007. AGRAVO NEGATIVO DE COMPETÊNCIA. PENAL PROCESSO PENAL. FRAUDE ELETRÔNICA NA INTERNET. TRANSFERÊNCIA DE NUMERÁRIO DE CONTA DA CAIXA ECONÔMICA FEDERAL. FURTO MEDIANTE FRAUDE QUE NÃO SE CONFUNDE COM ESTELIONATO. CONSUMAÇÃO. SUBTRAÇÃO DO BEM. APLICAÇÃO DO ART. 70 CPP. COMPETÊNCIA DA JUSTIÇA FEDERAL PARANAENSE. [...]. (STJ – CC: 6743 GO 2006/0166153-0, Relator: Ministra Laurita Vaz. Data de julgamento: 28/03/2007 – TERCEIRA SEÇÃO, Data de publicação: DJ: 11.12.2007 p. 170). Disponível em: https://stj.jusbrasil.com.br/jurisprudencia/5017/conflito-de-competencia-cc-67343-go-2006-0166153-0/inteiro-teor-100014363. Acesso em: 03 out. 2021.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Brasília, DF, 2012a. [2021]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 04 ago. 2021.

BRASIL. **Lei nº 12.735, de 30 de novembro de 2012**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências. Brasília, DF: Presidência da República, 2012b. [2021]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm. Acesso em: 04 ago. 2021.

BRASIL. Supremo Tribunal de Justiça. **Súmula 479** - As instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias. Brasília, DF, 2012c. Data da Publicação - DJ-e 1-8-2012.

BRASIL, **Lei nº 12.965, de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF. Presidência da República [2021]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 03 ago. 2021.

BRASIL. **Decreto nº 8.539, de 8 de outubro de 2015**. Dispõe sobre o uso do meio eletrônico para a realização do processo administrativo no âmbito dos órgãos e das entidades da

administração pública federal direta, autárquica e fundacional. Brasília, DF. Presidência da República 2015. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/decreto/d8539.htm. Acesso em: 03 ago. 2021.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF. Presidência da República [2019]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 29 out. 2021.

BRASIL. **Lei nº lei nº 13.979, de 6 de fevereiro de 2020**. Dispõe sobre as medidas para enfrentamento da emergência de saúde pública de importância internacional decorrente do coronavírus responsável pelo surto de 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/l13979.htm. Acesso em: 01 ago. 2021.

BRASIL. **Decreto 10.222, de 05 de fevereiro de 2020**. Aprova a Estratégia Nacional de Segurança Cibernética. Brasília, DF. Presidência da República, 2020a. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10222.htm. Acesso em: 02 nov. 2021.

BRASIL. Câmara dos Deputados. Direito e Justiça. **Proposta insere no Código Penal o crime de estelionato virtual.** 20 ago. 2020b. Disponível em: https://www.camara.leg.br/noticias/680058-proposta-insere-no-codigo-penal-o-crime-de-estelionato-virtual/. Acesso em: 02 out. 2021.

BRASIL. **Lei nº 14.155, de 27 de maio de 2021**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato. Brasília, DF: Presidência da República, [2021a]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14155.htm. Acesso em: 25 out. 2021.

BRASIL. **Gov.br**. Governo do Brasil. Notícias. População brasileira chega a 213,3 milhões de habitantes, estima IBGE. Brasília: DF, 27 ago. 2021b.. Disponível em: https://www.gov.br/pt-br/noticias/financas-impostos-e-gestao-publica/2021/08/populacao-brasileira-chega-a-213-3-milhoes-de-habitantes-estima-ibge#:~:text=a%20popula%c3%a7%c3%a3o%20brasileira%20chegou%20a,1%c2%ba%20de%20julho%20de%202021. Acesso em: 28 ago. 2021.

BRASIL. Ministério Público Federal. Cidadão. **O que são dados pessoais? Segundo a LGPD.** Brasília: DF. Disponível em: http://www.mpf.mp.br/servicos/lgpd/cidadao. [2018?]a. Acesso em: 30 out. 2021.

BRASIL. Ministério Público Federal. **O que é a LGPD?** Brasília: DF. Disponível em: http://www.mpf.mp.br/servicos/lgpd/o-que-e-a-lgpd. [2018?]b. Acesso em: 30 out. 2021.

BRASIL. Ministério da Saúde. FIO CRUZ. Fundação Oswaldo Cruz. Rio de Janeiro. Notícias e artigos. **O que é uma pandemia**. 28 jul. 2021c. Disponível em:

https://www.bio.fiocruz.br/index.php/br/noticias/1763-o-que-e-uma-pandemia. Acesso em: 28 ago. 2021.

BRASIL. **Brasil é o país com maior número de vítimas de phishing na internet.** Agência Brasil. 04 mar. 2021d. Disponível em: https://agenciabrasil.ebc.com.br/geral/noticia/2021-03/brasil-e-o-pais-com-maior-numero-de-vitimas-de-phishing-na-internet. Acesso em: 10 nov. 2021.

BUDAPESTE. **Convenção sobre o cibercrime de Budapeste**, 23. XI. 2001. Disponível em: http://www.mpf.mp.br/atuacao-tematica/sci/normas-e-legislacao/legislacao/legislacoes-pertinentes-do-brasil/docs_legislacao/convencao_cibercrime.pdf. Acesso em 30 out. 2021.

CAPEZ, Fernando. **Curso de Processo Penal**. 23. ed. – São Paulo: Saraiva, 2016.

CAPEZ, F. **Curso de direito penal** v. 2 - parte especial arts. 121 a 212. São Paulo: Saraiva, 2020. 9788553619207. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788553619207/. (Acesso restrito). Acesso em: 23 set. 2021.

CARTILHA de segurança para internet. Fascículo *internet banking*. **Cert.br. nic.br. cgi.br** out. 2020. Disponível em: https://cartilha.cert.br/fasciculos/internet-banking/fasciculo-internet-banking.pdf. Acesso em: 13 out. 2021.

CARVALHO, Marcelo Sávio Revoredo Menezes de. **A trajetória da internet no Brasil**: do surgimento das redes de computadores à instituição dos mecanismos de governança. 2006. Dissertação (Mestrado em Ciências de engenharia de sistemas e computação). Universidade federal do Rio de Janeiro, Rio de Janeiro, 2006. Disponível em: https://www.cos.ufrj.br/uploadfile/1430748034.pdf. Acesso em: 06 nov. 2021.

CASSANTI, Moises de Oliveira. **Crimes virtuais, vítimas reais**. Rio de Janeiro: E-book Kindle, Brasport, 2014. E-Book: Acesso restrito via Amazon. Acesso em: 07 nov. 2021.

COELHO, Fábio Ulhôa**. Manual de Direito Comercial**. 23 ed. São Paulo: Saraiva, 2011.

COLAÇO, Hian Silva. Responsabilidade civil dos provedores de Internet: diálogo entre a jurisprudência e o marco civil da Internet. **Revista dos Tribunais**, São Paulo, vol. 957, Julho 2015. (Não paginado). Disponível em: http://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_servicos_produtos/bibli_boletim/bibli_bol_2006/RTrib_n.957.05.PDF. Acesso em: 30 out. 2021.

CONHEÇA as tentativas de golpes financeiros mais comuns na pandemia e saiba como evitá-los. **FEBRABAN**, 21 set. 2020. (Não paginado). Disponível em: https://portal.febraban.org.br/noticia/3522/pt-br/. Acesso em: 18 out. 2021.

CORRÊA, Gustavo Testa. **Aspectos Jurídicos da Internet.** 2. ed. rev. São Paulo: Saraiva 2002.

COSTA, Dionatan. A incidência dos crimes virtuais em tempos de isolamento social. **Revista Jus Navigandi**, Teresina, set. 2020. (Não paginado). Disponível em:

https://jus.com.br/artigos/85629/a-incidencia-dos-crimes-virtuais-em -tempos-de-isolamento-social. Acesso em: 13 ago. 2021.

CRESCIMENTO de crimes cibernéticos na pandemia: como não ser uma vítima. Disponível em: https://cryptoid.com.br/identidade-digital-destaques/crescimento-de-crimes-ciberneticos-na-pandemia-como-nao-ser-uma-vitima/. São Paulo. 28 abr. 2021. **CRYPTO ID**. (Não paginado). Acesso em 18 out. 2021.

CRESPO, Marcelo Xavier de Freitas. **Crimes digitais**. São Paulo: Saraiva, 2011.

CUNHA, Rogério Sanches. Lei 14155/21 e os crimes de fraude digital: primeiras impressões e reflexos no CP e CPP. 28 maio 2021. **MeuSiteJurídico.com**. São Paulo. (Não paginado). Disponível em https://meusitejuridico.editorajuspodivm.com.br/2021/05/28/lei-14-15521-e-os-crimes-de-fraude-digital-primeiras-impressoes-e-reflexos-no-cp-e-no-cpp/. Acesso em 27 out. 2021.

GIL, Antônio Carlos. **Métodos e técnicas de pesquisa social**. 6 ed. São Paulo: Atlas, 1995.

GIL, Antônio Loureiro. **Fraudes informatizadas**. 2 ed. São Paulo: Atlas, 1999.

GONÇALVES, Victor Eduardo Rios. **Direito penal esquematizado**: parte especial – 6. ed. – São Paulo: Saraiva, 2016.

GOLPES de Pix: quem é o responsável pelos prejuízos dos clientes? **Uol Economia**. 28 ago. 2021. (Não paginado). Disponível em: https://economia.uol.com.br/noticias/estadao-conteudo/2021/08/28/nao-ha-consenso-sobre-quem-deve-arcar-com-o-prejuizo.htm?cmpid=copiaecola. Acesso em 17 out. 2021.

GUEIROS, Guilherme; NUNES, Elaine. Lei dos "crimes cibernéticos" altera competência em caso de estelionato. **Consultor Jurídico**, São Paulo, 04 jun. 2021. (Não paginado). Disponível em https://www.conjur.com.br/2021-jun-04/opiniao-lei-crimes-ciberneticos-altera-competencia-estelionato. Acesso em 27 set. 2021.

GUGELMIN, Felipe. Tentativas de fraudes contra serviços financeiros cresceram 612% no Brasil. **Canaltech**. 29 jul. 2021. (Não paginado). Disponível em: https://canaltech.com.br/seguranca/tentativas-de-fraudes-contra-servicos-financeiros-cresceram-612-no-brasil-188587/. Acesso em: 29 ago. 2021.

GUIZZO, Erico Marui. **Internet**: o que é? O que oferece? Como conectar-se. São Paulo: Ática, 2002.

HARÁN, Juan Manuel. Campanhas de phishing continuam apresentando crescimento no Brasil. **Welivesecurity.com**. Eslováquia, 03 set. 2019. (Não paginado). Disponível em: https://www.welivesecurity.com/br/2019/09/03/campanhas-de-phishing-continuam-apresentando-crescimento-no-brasil/. Acesso em: 10 nov. 2021.

INTERNET no Brasil. **Brasil escola**. Uol. [2020?]. (Não paginado). Disponível em: https://brasilescola.uol.com.br/informatica/internet-no-brasil.htm. Acesso em:

JESUS, Damásio de; MILAGRE, José Antônio. **Manual de crimes informáticos**. São Paulo: Saraiva, 2016.

LEITÃO, Joaquim Júnior. Atribuição para investigar e competência para processar o crime virtual de estelionato (fraudes bancárias) praticado com uso de bancos digitais. **Revista Jus Navigandi**, Teresina, ano 25, n. 6343, 12 nov. 2020. (Não paginado). Disponível em: https://jus.com.br/artigos/86340/atribuicao-para-investigar-e-competencia-para-processar-o-crime-virtual-de-estelionato-fraudes-bancarias-praticado-com-uso-de-bancos-digitais. Acesso em: 25 set. 2021.

LEONEL, Vilson; MARCOMIM, Ivana. **Projetos de Pesquisa Social**. Livro didático. Palhoça: Unisul Virtual, 2015.

LEONARDI, Marcel. **Fundamentos do Direito Digital**. São Paulo: Thomson Reuters Brasil Revista dos Tribunais, 2019.

LIMA, Glaydson de Farias. **Manual de Direito Digital:** Fundamentos, Legislação e Jurisprudência**.** Curitiba: Appris, 2016.

LUBECK, Luis. Brasil é o segundo país da América Latina com mais detecções de ataques de engenharia social. **Welivesecurity.com.** Eslováquia, 07 jan. 2021. (Não paginado).Disponível em: https://www.welivesecurity.com/br/2021/01/07/brasil-e-o-segundo-pais-da-america-latina-com-mais-deteccoes-de-ataques-de-engenharia-social/. Acesso em: 10 nov. 2021.

MARINHO, Simone Barbosa de Aquino. Proteção de dados e o Impacto da LGPD nas Instituições Financeiras. **Conteúdo Jurídico**, São Paulo, 08 jun. 2021. (Não paginado). Disponível em: https://conteudojuridico.com.br/consulta/artigos/56684/proteo-de-dados-e-o-impacto-da-lgpd-nas-instituies-financeiras. Acesso em: 30 out. 2021.

MARTINS, Pedro Batista. **Comentários ao Código de Processo Civil**, v. 2. São Paulo: Forense, v. 2, 2011.

MAZIERO, Carlos. O serviço DNS. **Prof. Carlos Maziero**. [2021?]. (Não paginado). Disponível em: http://wiki.inf.ufpr.br/maziero/doku.php?id=espec:servico_dns. Acesso em: 17 out. 2021.

MEDEIROS, Diego. Crimes Virtuais. **Revista Jus Navigandi**. São Paulo, set. 2015. (Não paginado). Disponível em: https://jus.com.br/artigos/42734/crimes-virtuais. Acesso em: 22 nov. 2021.

MEDEIROS, Gutembergue Silva Medeiros. **Âmbito Jurídico**, Rio Grande/RS**,** nº 200, 11 set. 2020**.** (Não paginado). Disponível em: https://ambitojuridico.com.br/cadernos/direito-penal/crimes-ciberneticos-consideracoes-sobre-a-criminalidade-na-internet/amp/. Acesso em: 02 out 2021.

MINAS GERAIS. Tribunal de Justiça do Estado de Minas Gerais. **Agravo de Instrumento-Cv1.0000.21.030411-9/001**. Relatora: Des. Lílian Maciel. AGRAVO DE INSTRUMENTO - AÇÃO DE DECLARAÇÃO DE INEXISTÊNCIA DE DÉBITO - TUTELA DE URGÊNCIA - ABSTENÇÃO DE COBRANÇA DE VALORES E DE INSCRIÇÃO DO AGRAVANTE NO ROL DE DEVEDORES - GOLPE "PHISHING" - FRAUDE BANCÁRIA -

REQUISITOS PREENCHIDOS -- RECURSO A QUE SE DÁ PROVIMENTO. - Como é cediço, a concessão da tutela de urgência depende do preenchimento dos requisitos previstos no art. 300 do CPC, especificamente a probabilidade do direito alegado e o perigo da demora. Como fornecedor na relação de consumo, a instituição financeira responde objetivamente pelos danos ocasionados aos consumidores pela ocorrência de falha na prestação dos serviços. Configura falha na prestação dos serviços por parte da instituição financeira a ocorrência de fraude bancária pela aplicação do golpe denominado "phishing", sobretudo quando há comprovação de que o agente financeiro, ciente da existência do golpe, não adotou todas as medidas que estava ao seu alcance para cientificar os consumidores e, principalmente, minimizar a incidência da fraude por meio de eficiente sistema de segurança que detecta operações financeiras estranhas ao perfil do cliente. Considerando que no presente caso a parte recorrente demonstrou nessa fase sumária, a ocorrência de falha na prestação de serviço, impõe-se o provimento do recurso. (TJMG - Agravo de Instrumento-Cv1.0000.21.030411-9/001, Relator(a): Des.(a) Lílian Maciel, 20ª CÂMARA CÍVEL, julgamento em 22/09/2021, publicação da súmula em 23/09/2021). Disponível em: https://tj-mg.jusbrasil.com.br/jurisprudencia/1286186940/agravo-de-instrumento-cv-ai-10000210304119001-mg/inteiro-teor-1286187013. Acesso em: 03 out. 2021.

NEVES, José Roberto de Castro. **O mundo pós-pandemia**. Rio de Janeiro: Nova Fronteira, 2020.

NUCCI, Guilherme de Souza, **Direito penal: Partes geral e especial**. .6 ed. Rio de Janeiro: Método 2019 1 recurso on line (Esquemas & Sistemas) ISBN 9788530986483. Disponível em: https://ambitojuridico.com.br/cadernos/direito-penal/crimes-de-internet-da-competencia-e-da-dificuldade-de-obtencao-de-provas-no-meio-eletronico. Acesso em: 25 ago. 21.

NÚMERO de usuários de Internet no mundo chega aos 4,66 bilhões. **Isto é Dinheiro**. 03 fev. 2021. (Não paginado). Disponível em: https://www.istoedinheiro.com.br/numero-de-usuarios-de-internet-no-mundo-chega-aos-466-bilhoes/. Acesso em: 10 nov. 2021.

O QUE É SPAM? **techtudo**. 25 jul. 2016. Disponível em: https://www.techtudo.com.br/noticias/noticia/2016/07/o-que-e-spam.html. Acesso em: 12 out. 2021.

OS INFLUENCIADORES que promovem golpes nas redes sociais. **Negócios**. (2021). (Não paginado). Disponível em: https://epocanegocios.globo.com/Tecnologia/noticia/2021/08/os-influenciadores-que promovem-golpes-nas-redes-sociais.html. Acesso em: 12 set. 2021.

PHARMING. **AVAST** Academy. [2016?]. (Não paginado). Disponível em: https://www.avast.com/pt-br/c-pharming#gref. Acesso em: 12 set. 2021.

PINHEIRO, Patricia Peck. **Direito Digital**. 7 ed. São Paulo: Saraiva Educação, 2021.

POLIDO, Fabrício Bertini Pasquot. Porque o Brasil deve urgentemente aderir à Convenção de Budapeste. **Consultor Jurídico**, São Paulo, 05 jul. 2021. (Não paginado). Disponível em https://www.conjur.com.br/2021-jul-05/polido-brasil-urgentemente-aderir-convencao-budapeste. Acesso em 31 out. 2021.

PORFÍRIO, Francisco. Isolamento social. **Mundo Educação**. Uol. [2019?]. (Não paginado). Disponível em: https://mundoeducacao.uol.com.br/sociologia/isolamento-social.htm. Acesso em: 29 ago. 2021.

PRADO, Luiz Regis. **Bem Jurídico Penal e Constituição**. 5 ed. São Paulo: Revista dos Tribunais, 2011.

ROHR, Altieres. Como identificar se um boleto é verdadeiro ou falso? **G1** Economia. 10 dez. 2020. (Não paginado). Disponível em https://g1.globo.com/economia/tecnologia/blog/altieres-rohr/post/2020/12/10/como-identificar-se-um-boleto-e-verdadeiro-ou-falso-qual-o-meio-mais-seguro-para-pagar-um-boleto.ghtml. Acesso em 16 out. 2021.

ROHR, Altieres. Golpes pela internet têm penas ampliadas para até 8 anos de prisão; entenda a nova lei. **G1** Economia. 28 maio 2021. (Não paginado). Disponível em: https://g1.globo.com/economia/tecnologia/blog/altieres-rohr/post/2021/05/28/golpes-pela-internet-tem-penas-ampliadas-para-ate-8-anos-de-prisao-entenda-a-nova-lei.ghtml. Acesso em: 11 set. 2021.

ROSA, Fabrízio, **Crimes de Informática**, 2 ed. Campinas: Bookseller, 2006.

SANTA CATARINA. **Delegacia de Polícia Virtual**. Governo de Santa Catarina, Florianópolis, 2002. Disponível em: https://delegaciavirtual.sc.gov.br/inicio.aspx. Acesso em: 27 out. 2021.

SANTA CATARINA. Tribunal de Justiça de Santa Catarina. **Apelação n. 5001582-92.2019.8.24.0016.** Relator:. Saul Steil, Terceira Câmara de Direito Civil. j. 27-10-2020. APELAÇÃO CÍVEL. AÇÃO DECLARATÓRIA DE INEXISTÊNCIA DE DÉBITO C/C COMPENSATÓRIA DE DANOS MORAIS. AUTORA QUE, ALMEJANDO REEMITIR BOLETO PARA PAGAMENTO DE PARCELA DE FINANCIAMENTO CONTRATADO JUNTO À RÉ, TERIA SIDO DIRECIONADA, AO ACESSAR O SITE DA INSTITUIÇÃO FINANCEIRA, A CONTATO COM ESTELIONATÁRIO VIA APLICATIVO "WHATSAPP" E A PAGAR A ELE O VALOR DA PRESTAÇÃO, RESULTANDO EM INSCRIÇÃO DE SEU NOME NO CADASTRO DO SERASA. SENTENÇA DE IMPROCEDÊNCIA. INSURGÊNCIA DA AUTORA.
INSISTÊNCIA NA ILICITUDE DO APONTAMENTO. INSUBSISTÊNCIA. INVERSÃO DO ÔNUS DA PROVA (ART. 6º, INC. VIII, CDC) QUE NÃO AFASTA O ÔNUS DA PARTE AUTORA DE DEMONSTRAR, AINDA QUE MINIMAMENTE, OS FATOS CONSTITUTIVOS DO SEU DIREITO (ART. 373, I, CPC). ACERVO PROBATÓRIO A INDICAR TER A CONSUMIDORA SIDO VÍTIMA DE "PHISHING", POIS ACESSOU SITE FALSO EM QUE DIRECIONADA A FAZER CONTATO COM O FALSÁRIO NO APLICATIVO DE MENSAGENS REFERIDO. SEQUÊNCIA DE EVENTOS CUJA RESPONSABILIDADE NÃO PODE SER IMPUTADA À INSTITUIÇÃO FINANCEIRA, MAS SIM À FALTA DE CAUTELA DA PRÓPRIA AUTORA. FORTUITO EXTERNO. INAPLICABILIDADE DA SÚMULA 479 DO STJ. PRECEDENTES DESTA CORTE. IMPROCEDÊNCIA DA PRETENSÃO INAUGURAL MANTIDA. PLEITO PELA CONDENAÇÃO DA RÉ ÀS PENALIDADES DECORRENTES DE PRÁTICA DE ATO ATENTATÓRIO À DIGNIDADE DA JUSTIÇA E DE LITIGÂNCIA DE MÁ-FÉ POR CONTA DE SUPOSTO DESCUMPRIMENTO À TUTELA DE URGÊNCIA ANTERIORMENTE CONCEDIDA. AUSÊNCIA DE PROVAS, CONTUDO, DE INOBSERVÂNCIA À ORDEM JUDICIAL. RECURSO CONHECIDO E DESPROVIDO.

(TJSC, Apelação n. 5001582-92.2019.8.24.0016, do Tribunal de Justiça de Santa Catarina, rel. Saul Steil, Terceira Câmara de Direito Civil, j. 27-10-2020).

SANTA CATARINA. Tribunal de Justiça de Santa Catarina. **Apelação n. 5001582-92.2019.8.24.0016.** Relator: Saul Steil, Terceira Câmara de Direito Civil. j. 19-08-2021. APELAÇÃO CÍVEL. AÇÃO CONDENATÓRIA. FRAUDE NA EMISSÃO DE BOLETO BANCÁRIO. SENTENÇA DE PROCEDÊNCIA. INSURGÊNCIA DA REQUERIDA. PRELIMINAR. PEDIDO DE DENUNCIAÇÃO À LIDE. INSUBSISTÊNCIA. RELAÇÃO DE CONSUMO. INTELIGÊNCIA DA SÚMULA 83 DO STJ. "É vedada a denunciação da lide nas relações de consumo, nos termos do art. 88 do CDC" (AgRg no REsp 1288943/SP, Rel. Ministro JOÃO OTÁVIO DE NORONHA, TERCEIRA TURMA, julgado em 15/9/2015, DJe 21/9/2015). ALEGADA INEXISTÊNCIA DE ATO ILÍCITO, SOB O ARGUMENTO DE QUE A FRAUDE SE CONSUMOU POR AUSÊNCIA DE CAUTELA DA PRÓPRIA PARTE AUTORA. ACOLHIMENTO. FRAUDE EM BOLETOS DE QUITAÇÃO DE DÍVIDA EMITIDO PELA EMPRESA CREDORA. AUSÊNCIA DE COMPROVAÇÃO DA PARTICIPAÇÃO DA REQUERIDA OU DE SEUS PREPOSTOS NA PERPETRAÇÃO DA FRAUDE OU FALHA NA PRESTAÇÃO DE SERVIÇOS. EMISSÃO DE BOLETO QUE FOI REALIZADA FORA DOS CANAIS OFICIAIS DA INSTITUIÇÃO BANCÁRIA. REMESSA POR MENSAGEM ELETRÔNICA (E-MAIL) PELA EMPRESA CREDORA E INTERCEPTADA POR TERCEIRO. ADULTERAÇÃO DO CÓDIGO DE BARRA E DA EMPRESA BENEFICIÁRIA. RESPONSABILIDADE OBJETIVA AFASTADA. CULPA EXCLUSIVA DA VÍTIMA QUE NÃO AGIU COM AS CAUTELAS NECESSÁRIAS EM SE CERTIFICAR DA VERACIDADE DO DOCUMENTO, MESMO DIANTE DE TANTOS INDICIOS DE QUE SE TRATAVA DE ATO FRAUDULENTO. NEXO DE CAUSALIDADE INEXISTENTE. AUSENTE O DEVER DE INDENIZAR. INTELIGÊNCIA DO ARTIGO 14, § 3º, II DO CDC. SENTENÇA REFORMADA. INVERSÃO DOS ÔNUS SUCUMBENCIAIS. HONORÁRIOS RECURSAIS. INVIABILIDADE RECURSO DA REQUERIDA CONHECIDO E PROVIDO. (j. 19-08-2021).

SILVA, Francisco José Albino Faria Castro. **Classificação Taxonómica dos ataques de engenharia social.** 2013. Dissertação (Mestrado em Segurança da informação), Universidade Católica Portuguesa Faculdade de Engenharia, 2013.

SILVA, Iury Pereira. **Engenharia social como ameaça ao setor bancário: uso do phishing para coletar informações dos correntistas e a necessidade de estratégias de segurança.** Ortiz, 2019. Trabalho de Conclusão de Curso (Engenharia de Software), Universidade Federal do Ceará, Quixadá, 2019.

SILVA, Thiago. Mundo digital não é terra sem lei e nova legislação endurece penas. **FEBRABAN News.** 10 jun. 2021. (Não paginado). Disponível em: https://portal.febraban.org.br/noticia/3638/pt-br/. Acesso em: 03 out. 2021.

SOUZA, Ramon. Engenharia social: o que é e como não ser vítima? **Canaltech**, 15 out. 2020. Disponível em https://canaltech.com.br/seguranca/o-que-e-engenharia-social-como-nao-ser-vitima-171899/.Acesso em 02 out. 2021.

SYDOW, Spencer Toth. **Curso de Direito Penal Informático**. 2. ed. rev. atual. Salvador: JusPODIVM, 2021.

VILLAR, Alice Saldanha. A responsabilidade civil dos bancos por fraudes e delitos praticados por terceiros em operações bancárias. São Paulo. **Jusbrasil**. 2015. Disponível em: https://alice.jusbrasil.com.br/artigos/241116662/a-responsabilidade-civil-dos-bancos-por-fraudes-e-delitos-praticados-por-terceiros-em-operacoes-bancarias. Acesso em: 03 out. 2021.

ANEXO

ANEXO A – TIPOS DE *PHISHING*

Tabela: Exemplos de tópicos e temas de mensagens de *phishing.*

Tópico	**Tema da mensagem**
Álbuns de fotos e vídeos	pessoa supostamente conhecida, celebridades algum fato noticiado em jornais, revistas ou televisão, traição, nudez ou pornografia, serviço de acompanhantes
Antivírus	atualização de vacinas, eliminação de vírus, lançamento de nova versão ou de novas funcionalidades
Associações assistenciais	AACD Teleton, Click Fome, Criança Esperança
Avisos judiciais	intimação para participação em audiência ˆ comunicado de protesto, ordem de despejo
Cartões de crédito	programa de fidelidade, promoção
Cartões virtuais	UOL, Voxcards, Yahoo! Cartões, O Carteiro, Emotioncard
Comercio eletrônico	cobrança de débitos, confirmação de compra, atualização de cadastro, devolução de produtos, oferta em site de compras coletivas
Companhias aéreas	promoção, programa de milhagem
Eleições	título eleitoral cancelado, convocação para mesário
Empregos	cadastro e atualização de currículos, processo seletivo em aberto
Imposto de renda	nova versão ou correção de programa, consulta de restituição, problema nos dados da declaração
Internet Banking	unificação de bancos e contas, suspensão de acesso, atualização de cadastro e de cartão de senhas, lançamento ou atualização de módulo de segurança, comprovante de transferência e depósito, cadastramento de computador
Multas e infrações de trânsito	aviso de recebimento, recurso, transferência de pontos
Músicas	canção dedicada por amigos
Notícias e boatos	fato amplamente noticiado, ataque terrorista, tragédia natural
Prêmios	loteria, instituição financeira
Programas em geral	lançamento de nova versão ou de novas funcionalidades
Promoções	vale-compra, assinatura de jornal e revista desconto elevado, preço muito reduzido, distribuição gratuita
Propagandas	produto, curso, treinamento, concurso
Reality shows	Big Brother Brasil, A Fazenda, Ídolos
Redes sociais	notificação pendente, convite para participação, aviso sobre foto marcada, permissão para divulgação de foto
Serviços de Correios	recebimento de telegrama online
Serviços de e-mail	recadastramento, caixa postal lotada, atualização de banco de dados
Serviços de proteção de crédito	regularização de débitos, restrição ou pendência financeira
Serviços de telefonia	recebimento de mensagem, pendência de débito, bloqueio de serviços, detalhamento de fatura, créditos gratuitos

Sites com dicas de segurança	aviso de conta de e-mail sendo usada para envio de spam (Antispam.br) cartilha de segurança (CERT.br, FEBRABAN, Abranet etc.)
Solicitações	orçamento, documento, relatório, cotação de preços, lista de produtos

Fonte: https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf