PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
ESCOLA DE DIREITO, NEGÓCIOS E COMUNICAÇÃO
NÚCLEO DE PRÁTICA JURÍDICA
COORDENAÇÃO ADJUNTA DE TRABALHO DE CURSO
ARTIGO CIENTÍFICO

CRIMES CIBERNÉTICOS E SUAS IMPLICAÇÕES NA ECONOMIA E NA SOCIEDADE

ORIENTANDO (A) – NATÁLIA FERREIRA LOPES CIRQUEIRA
ORIENTADOR (A) - PROF. (A) CLAUDIA LUIZ LOURENÇO

GOIÂNIA-GO
2025

NATÁLIA FERREIRA LOPES CIRQUEIRA

CRIMES CIBERNÉTICOS E SUAS IMPLICAÇÕES NA ECONOMIA E NA SOCIEDADE

Artigo Científico (ou Monografia Jurídica) apresentado à disciplina Trabalho de Curso I, da Escola de Direito, Negócios e Comunicação da Pontifícia Universidade Católica de Goiás (PUCGOIÁS).
Prof. (a) Orientador (a) – Dra. Claudia Luiz Lourenço.

GOIÂNIA-GO

2025

NATÁLIA FERREIRA LOPES CIRQUEIRA

CRIMES CIBERNÉTICOS E SUAS IMPLICAÇÕES NA ECONOMIA E NA SOCIEDADE

Data da Defesa: 06 de junho de 2025

BANCA EXAMINADORA

_____

Orientador (a): Prof. (a) Dra. Claudia Luiz Lourenço Nota:

_____

Examinador (a) Prof. (a) Ms: Karla Beatriz Nascimento Pires Nota:

SUMÁRIO

CRIMES CIBERNÉTICOS E SUAS IMPLICAÇÕES NA ECONOMIA E NA SOCIEDADE

Natália Ferreira Lopes Cirqueira[1]

RESUMO

O presente trabalho tem como objetivo a apresentação da história nos bancos, como um todo, passando pela Idade Média, chegando até os dias atuais, sucedendo os relatos, por meio de notícias, sites e livros acerca do tema, da Internet, onde é possível observar como a Rede Mundial de Computadores ajudou a construir e facilitar as ações realizadas pelas pessoas, independente de onde estejam. Entretanto, neste caso também existem as dificuldades que envolvem esta tecnologia, chegando os crimes que permeiam o ambiente virtual. Por conseguinte a exposição da sociedade a essa nova tecnologia, apresentou um novo caminho para os autores seguirem, desenvolvendo as condutas tipificadas nos arts. 154-A, 155, §4º-B e 171, §2º-A, e posteriormente explanando as diferenças entre eles. A pesquisa é bibliográfica e seguiu o metodo histórico-dedutivo

Palavras-chave: Internet. Bancos. Crimes. Cibernético. Ambiente virtual

[1] Aluna do Curso de Direito na Pontifícia Universidade Católica de Goiás – e-mail:

INTRODUÇÃO

A presente pesquisa tem por objeto internet que é um tema muito recorrente tratado nas rodas de conversas e está fortemente ligado à criação e utilização da rede mundial de computadores em vários âmbitos da sociedade e, como esse uso impacta na vida das pessoas.

Todavia o entendimento da junção da internet e práticas nesse ambiente requer um breve apanhado histórico para apresentar um panorama do que vem acontecendo desde o seu advento. A primeira vez em que uma precursora do que identificamos, hoje, como internet, começou a ser desenvolvida no auge da Guerra Fria, sendo conhecida como Arpanet.

Para que a internet fosse aperfeiçoada, foram necessárias algumas alterações, dentre elas, a transição da Arpanet para TCP/IP. Neste contexto, o avanço da rede teve início com a aplicação de conhecimentos militares. Porém, essas informações não ficaram restritas apenas nessa área, evoluindo para outros ambientes, como na educação e comunicação.

Deste modo, com as atualizações acontecendo, e a possibilidade de mais áreas terem acesso a essa tecnologia, tornou-se viável que outros ambientes pudessem desfrutar dessa nova forma de comunicação. Desta maneira, vários “nichos” começaram a usufruir da conectividade e seus benefícios. No Brasil, a chegada desta tecnologia começou com o intuito educacional, fazendo contato com universidades mundiais, por meio de *e-mails*, via códigos.

Já no ano de 1994, a Embratel (Empresa Brasileira de Telecomunicações) desenvolveu uma espécie de internet comercial, em que um número limitado de pessoas conseguiria testar essa nova conexão. Então no ano de 1995, as empresas privadas começam a explorar o serviço, pois até essa data, apenas a Embratel tinha a concessão para ampliar a referida atividade. Em virtude de ter sido possível a mais empresas serem concessionárias desse serviço, os brasileiros começaram a usar a rede, com o padrão WWW *(World Wide Web*), com o lançamento de modelos de computadores mais acessíveis.

Com o lançamento e facilidade para acessar a internet, começaram a surgir vários sites, como o Canal Vip, sites de notícias, e bancos, além de ter sido criado o CGI.BR (Comite Gestor da Internet), órgão responsável por discutir diretrizes e

inovações relacionadas ao assunto. Com a finalidade de expandir os conhecimentos para determinado público, houve a exposição Internet Word, para apresentar a empresas, provedores e empresários. Deste modo, em 1997, o TSE (Tribunal Superior Eleitoral) divulga o resultado das eleições, o Imposto de Renda começa a poder ser declarado de forma online.

Ademais em 1999, surge o Mercado Livre para classificados, além do bate papo da UOL (Universo Online). Ao expor a criação de novos meios de comunicação, e publicação de notícias, foi inevitável que outros âmbitos da sociedade aderissem a essa nova ferramenta. Por conseguinte, os bancos também optaram por atualizar a sua forma de trabalho, trazendo inovações que pudessem auxiliar no uso de tais serviços.

Dentre as renovações, está a criação de aplicativos dos bancos, em que o usuário pode realizar transações bancárias em qualquer lugar, desde que tenha acesso a internet, além de ter configurado o aplicativo passando por todas as etapas de segurança para utilizar o produto. Nos aplicativos bancários, dentre várias camadas de proteção, estão o reconhecimento facial, a biometria e um código que é configurado em uma ação realizada em um caixa eletrônico de uma agência do seu banco.

Apesar de todo esse aparato tecnológico, ainda é possível perceber que essa modernização não veio apenas para o bem. Assim houve progresso dos que, atualmente, conhecemos como *hackers,* entretanto é um termo usado erroneamente, visto que na área da tecnologia existem dois grandes grupos que podem ser diferenciados, os *hackers* e os *crackers*. Para se referir a indivíduos que usam de seus conhecimentos envolvendo o Sistema de Informação (TI), com o intuito de invadir as camadas de segurança da internet, para obterem vantagens ilícitas, devem ser conhecidos como *crackers*. Já os *hackers* são indivíduos entusiastas da área da tecnologia que visam criar e otimizar sistemas e *softwares* de segurança para evitar invasões criminosas, ações estas cometidas por *crackers*. Todavia muitas pessoas utilizam dos serviços destes indivíduos para conseguirem dados pessoais de pessoas que estão fazendo compras em sites, ou até mesmo fazendo transferências bancárias, através dos aplicativos. Indivíduos estes que se aproveitam de um momento de distração das vítimas para concluir a prática dos crimes.

Assim como acontece em outras situações cotidianas, o uso da internet deve ser regulado pelas leis nacionais em conjunto com as internacionais, com o intuito do ambiente virtual não se tornar uma espécie de “terra sem lei” para que as pessoas possam fazer o que bem entender. E sabendo que a internet é resguardada por uma legislação específica torna-se mais fácil as investigações, caso seja necessária.

Apesar da criação do Comitê Gestor da Internet no Brasil, além de outras legislações para proteção do uso da internet, é possível observar que a tecnologia vem sendo usada, também, para facilitar as condutas delituosas. Uma parcela da sociedade acredita que a internet é uma “terra sem lei”, por pensarem que estão protegidos do alcance das autoridades. Entretanto, assim como um código de conduta em sociedade foi criado, as ações realizadas no ambiente virtual também têm suas obrigações a serem cumpridas. Deste modo, é possível observar que, no Brasil, foram criadas algumas legislações que pudessem auxiliar no controle contra a criminalidade no ambiente virtual.

Em virtude de tudo isso, surgem as seguintes dúvidas a serem solucionadas no transcorrer da pesquisa a) A legislação vigente é suficiente para responsabilizar e condenar os praticantes desse tipo de conduta? b) Existe o aparato para investigação do crime cometido na internet? c) Qual a forma de evitar determinadas usurpações de dados? d) Como poderia ser melhorado ou encurtado o acesso a dados para uma melhor atuação da polícia?

Para tanto, poder-se-ia supor, respectivamente, o seguinte: Por ser um tema considerado novo, é possível observar a falta de doutrinas e entendimentos acerca dos crimes cibernéticos. Esta constatação é feita diante da comparação do Código penal vigente (1940) para receber uma “atualização” que abranja os crimes cibernéticos (Lei 14.155/2021). O conhecimento do tema pode ser considerado escasso, e assim não é possível ter uma tecnologia de ponta para que ocorra a investigação de forma efetiva e rápida.

Outrossim, é imprescindível uma melhoria para que exista uma forma de combater a invasão de dispositivos para a cometer o delito. Com apuração mais efetiva dessas ocupações se tornará mais fácil a participação da polícia e ajudará na forma de investigação, porque assim, a polícia terá um acesso direto e imediato a conduta criminosa, visto que estará resguardada e preparada para esse tipo de fato. Também é possível perceber que, com o conhecimento aprimorado do assunto, será

possível a criação de defesas eficazes e configurações mais seguras.

Utilizando-se uma metodologia eclética e de complementaridade, mediante a observância da dogmática jurídica, materializada em casos concretos; do método dedutivo-bibliográfico, cotejando-se normas e institutos processuais pertinentes ao tema; do processo metodológico-comparativo; e do estudo de casos.

Ter-se-á por objetivo principal analisar a legislação que cerca os crimes cometidos em ambiente virtual.

Como desdobramento deste, alia-se a pretensão de, primeiramente, na seção I, analisar os antecedentes históricos envolvendo as transações econômicas, seguida, na seção II, tratar da história da internet; e, na seção III, trazer o marco civil da internet, na seção IV, elencar os crimes cibernéticos e por fim, na seção V analisar alguns tipos penas específicos.

Nesse diapasão, em razão da dificuldade de sua compreensão e conseqüentes discussões a respeito dessas exceções, torna-se interessante, conveniente e viável analisar o assunto, visto que é uma temática considerada nova, a qual ainda não existe uma gama de legislações e doutrinas que possam auxiliar a polícia investigativa e os operadores do Direito.

A falta de incentivo as novas tecnologias para a polícia investigativa, juntamente com o apogeu do tema, aliada ao pouco conhecimento específico alcançado com escassos treinamentos, acaba “facilitando” a conduta delituosa dos criminosos.

Em especial este trabalho pretende desenvolver estudo voltado a alguns crimes cibernéticos, através especificamente da análise dos tipos penais criados com a finalidade de punir condutas como a de *hackers, crakers*, além dos mecanismos apontados como passíveis de identificar, reprimir e prevenir tais crimes e proteger, pelo menos, nesse aspecto os usuários.

1. ANTECEDENTES HISTÓRICOS ENVOLVENDO TRANSAÇÕES ECONÔMICAS

A História dos comércios mundiais e transações econômicas ocorrem desde muito antes do que conhecemos, atualmente como bancos. Trazendo um recorte histórico dos acontecimentos anteriores, é possível notar que uma das primeiras formas de “comércio” aconteceu quando a escrita começou a surgir. Um exemplo disso é o desenvolvimento de como as transações aconteciam na época dos Sumérios.

Os sumérios que viveram, onde hoje se tornou o Iraque e Kuait, na antiga Mesopotâmia, começaram a desenvolver uma forma de registrar os recebimentos, pagamentos e a circulação de produtos. Os mesopotâmicos realizavam atividades rurais como a agricultura e a pecuária e dessas práticas recolhiam os frutos como a cevada e o gergelim do âmbito agricultável. Quanto ao uso dos animais, dentre eles, bois, cabras, ovelhas e porcos, era possível adquirir gorduras, lã, carnes, e quando vivos, os bois auxiliavam no preparo da terra e os jumentos puxavam as carroças.

Enquanto isso, nas cidades, existiam artesãos que fabricavam tecidos, eram especialistas na cerâmica e esculpiam madeira e mármore. Todavia a forma que o povo das cidades obtinha os produtos rurais e vice-versa era em forma de trocas. Como as cidades-estados fenícias também ocorriam a troca de mercadorias, porém esse tipo de transação envolvia joias, cedro, tecidos de algodão, bem como produtos de outros povos. Tais interações aconteciam visto que os fenícios eram bons navegadores e cruzavam seu território chegando aonde hoje é conhecido como Inglaterra e a costa ocidental da África.

1.1 CRISTIANISMO E AS SOCIEDADES ANTIGAS

Desde os tempos antigos os estudos que se tem, demonstram que todas as civilizações eram politeístas, isto é, tinham religião que acreditavam em várias divindades superiores. Tal crença perdurou até o nascimento de Jesus. Vale ressaltar que Jesus tem grande impacto ainda hoje, visto que desde o que os historiadores acreditam que tenha sido o ano de seu nascimento, se transformou em uma “linha” para determinar fatos históricos, criando assim o calendário a.C. e d.C.

Tal curiosidade é acompanhada do entendimento que mostra que os cristãos (pessoas que seguiam os ensinamentos do cristianismo) foram perseguidos até o

final do ano de 313 d. C. A importunação que essa população sofria teve seu fim quando Constantino, Imperador de Roma, antes de sua morte, decidiu converter-se ao Cristianismo. Após a morte de Constantino, no ano de 380 o Imperador Teodósio transformou o cristianismo na religião oficial do Império Romano. A decisão de Teodósio acarretou um poder dado a esta forma adjunta de governo, o cristianismo. Essa forma de poder dada a Igreja corroborou para o futuro do que chamamos de feudalismo.

1.2 O FEUDALISMO

O Feudalismo é considerado um “sistema de organização econômica, social e política baseado nos lações de fidelidade e de dependência entre suserano e vassalo” (Alfredo Júnior Boulos, 2015). Tal forma de “gerenciamento” teve como ascendente os colonatos, que eram formas de trabalho desenvolvidas na Época Romana. Os colonatos foram se atualizando até chegarem à configuração de feudos.

Os feudos eram uma “troca” de pedaços de terra, ou o direito de cobrar pedágio em uma ponte, que o suserano “trocava” com outros homens em prol de fidelidade e dependência pessoal. Com a consolidação dessa forma de viver, as pessoas acabaram por ter o sistema de interações modificado, transformando-se em uma sociedade feudal. Como em toda sociedade existem as divisões, no feudalismo essas divisões eram conhecidas como: “os que oram (clero/igreja), “os que guerreiam (a nobreza)” e os que trabalham (servos, vilões e escravos).

O clero era considerado o grau de maior importância da população, deste modo as outras duas classes deviam respeito. A relação entre a Igreja e os demais consistia na realização de celebrações de batismos e casamentos, cobrando para tal. Além de possuírem propriedades, e nelas “abrigarem” camponeses, para que estes praticassem a agricultura e de lá a Igreja poderia tirar a sua sobrevivência.

Por sua vez, “os que guerreiam” eram o que conhecemos como nobres, e dentre eles estavam o rei, o duque, o conde e outros. Essa forma de “liderança” era independente a cada feudo, visto que um senhor feudal poderia ser vassalo de outro senhor feudal, ou seja, um senhor feudal poderia “usar” das terras de outro senhor feudal, desde que tivesse uma relação de fidelidade para com o seu suserano. Quanto aos guerreiros, que também estão inseridos na classe “dos que guerreiam” e

assim eram considerados nobres, ofertavam sua proteção em troca de ser sustentado pelos que trabalhavam nos feudos.

Em consonância com essa parte das pessoas, existiam “os que trabalham”, considerados “indignos” pelos nobres por realizarem serviços braçais. Os laboratores eram os servos, os vilões e os escravos, e trabalhavam com o plantio e cultivo, caça, pesca, tecer e construir casas. Com esse trabalho, os camponeses se reportavam ao senhor feudal, o administrador de determinado feudo. Assim, uma parcela do que os laboratores produziam eram repassados para o senhor feudal, para a nobreza e para o Clero.

A economia feudal era baseada na agricultura e assim como os povos antigos obtinham outros tipos de mercadorias por meio do escambo (troca). Entretanto, em meados do século XI houve uma mudança gradativa, que acarretou uma quantidade maior de produção dos produtos. Com o aumento das mercadorias, e percebendo que não era necessária tanta mão de obra, os trabalhadores começaram a procurar outros locais para desenvolverem uma nova forma de viver. Desta forma começaram a surgir o que futuramente conheceríamos como cidades.

A eclosão das feiras medievais começou ainda no século XI, onde vários mercadores compareciam a estes lugares para realizarem as trocas de mercadorias. Entretanto, nessa época a troca não ocorria entre produtos e sim com o uso da moeda. Com o surgimento da moeda, cada povo possuía um tipo e cada uma com um valor diferente.

Por ser possível encontrar vários tipos de moedas diversas e de valores diferentes, existiam os cambistas, pessoas que trocavam o dinheiro para a moeda desejada, e como essa prática era feita em cima de bancos de madeira, que ficaram conhecidos como banqueiros. Outrossim, os banqueiros faziam as trocas de moedas e poderiam guardar, e até realizarem “empréstimos”. O que fazendo uma breve análise, se tornaria muito tempo depois o que se denominam hoje como bancários.

1.3 BANCOS NA IDADE MODERNA

Fazendo um salto na história, chegamos à criação da primeira instituição financeira de que se tem registro, sendo ela a *Casa di San Giorgio*, surgindo na cidade de Gênova, na Itália. Esta instituição foi criada com o intuito de administrar as dívidas que surgiram em decorrência de uma guerra que ocorria entre Gênova e

Veneza. Entretanto foi possível adicionar determinadas condutas dentro da *Casa*, como direito de realizar depósitos e atividades de crédito.

Já na Inglaterra, no século XVIII, época em que se desenrolava a 1ª Revolução Industrial era fundamental que houvesse modificações na forma de se realizar o trabalho afim de obter mais resultados e gerar mais lucros. Com a criação de máquinas que auxiliariam na produção de tecidos, e facilitaria o escoamento das mercadorias, foi necessário um incentivo econômico. E é neste momento em que as instituições financeiras começam a realizar operações para ajudarem na oferta de crédito para as empresas produzirem suas mercadorias, além de fornecerem dinheiro para que as pessoas possam comprar os produtos.

1.4 A HISTÓRIA DOS BANCOS NO BRASIL

Trazendo essas instituições para o continente americano, mais precisamente ao Brasil nota-se a forma como os bancos tiveram uma grande atualização desde a sua criação até os dias de hoje, onde existem bancos digitais, os quais nem possuem agências bancárias físicas.

As instituições bancárias chegaram junto com a Corte Portuguesa, em 1808, criando o primeiro banco brasileiro, o Banco do Brasil, que tinha como atribuição emitir as notas bancárias para circulação de dinheiro no país naquela época, além de auxiliar na comercialização de produtos, como o pau-brasil e os diamantes. Todavia, a forma como este Banco era comandada, tendo os “gerentes” sido escolhidos por proximidade real, começaram a ocorrer crises internas, o que acarretou o fechamento deste, e um tempo depois acabaria por existir outra casa financeira que pudesse realizar as atividades.

Com o declínio deste Banco, o Império visualizou que uma possível fusão entre dois grandes bancos da época, o Banco do Brasil criado pelo Barão de Mauá em 1851 e o Banco Comercial do Rio de Janeiro, conseguiria auxiliar na reforma financeira que estava sendo estudada e assim, a instituição financeira poderia ficar responsável apenas pela emissão de papel moeda. Entretanto, o que o imperador não contava é que, em 1864 o novo Banco do Brasil perderia sua exclusividade em realizar a operação de emissão do papel moeda, o que quase provocou a falência do Banco. A situação dos bancos públicos foi se agravando cada vez mais com a crise do café, o que favoreceu a idealização da criação dos bancos responsáveis

apenas pela emissão de moeda, além das instituições responsáveis por fornecer os empréstimos, os depósitos, atividades de crédito e demais operações bancárias.

Deste modo, houve a ascensão do que, posteriormente, viria a se tornar a Caixa Econômica Federal, onde era seu papel cuidar e regular os depósitos feitos por seus clientes, conceder “somente poderiam destinar seus depósitos à aquisição de apólices da dívida pública ou ao financiamento de despesas do Estado”. (Yttrio Corrêa da Costa, Neto, 2004). Já os Montes de Socorro ficaram responsáveis pelos empréstimos destinados aos populares. Outrossim, haveria um maior controle do Estado para com as transações bancárias, e desta maneira ocorreria a tentativa da não falência dos bancos existentes, como havia acontecido anteriormente. Destarte com a necessidade de produção da moeda e crescimento populacional, deu-se início a formação dos primeiros bancos privados.

1.4.1 Contemporaneidade bancária no Brasil

Com a evolução financeira que o país sofreu, houve a abertura da possibilidade para que bancos estrangeiros se instalassem no Brasil para poderem realizar as suas atividades. Entretanto, no mercado para pessoas físicas, onde as instituições estavam acostumadas a promover as atividades bancárias, como empréstimos, depósitos, emissões de folhas de cheque, não houve um grande interesse por parte do capital estrangeiro. E assim, deram-se início a criação dos bancos privados nacionais, tais como Itaú Unibanco (que atualmente havia sido uma fusão entre os bancos Itaú e Unibanco), Bradesco.

1.4.1.1 Origem do UNIBANCO e ITAÚ

O UNIBANCO começou em um pequeno estabelecimento de secos e molhados, a casa Moreira Sales, em 1924, recebeu a autorização para funcionar como seção bancária. Ao receber tal autorização ficou acordado que este comércio representaria os bancos privados e o Banco do Brasil para realizar algumas transações, como por exemplo, em casos de agricultores que precisavam comprar alguma coisa, sendo elas ferramentas, sementes ou máquinas, para auxiliar na colheita das sementes. No exemplo supramencionado, em casos que o agricultor não possuía dinheiro, recorria as seções bancárias para pegar o dinheiro emprestado, e quando a safra fosse colhida, pagaria o valor que havia pegado

emprestado acrescido de alguns juros.

Já em 1931, a casa Moreira Sales recebeu a aprovação para funcionar como uma casa bancária, sendo um estabelecimento autônomo, uma instituição bancária própria, a qual não dependia de outro banco para tal, podendo tomar as próprias decisões, o que diferia das seções bancárias que era uma “repartição”, que se submetia os bancos privados e Federais.

Com o passar dos anos, na década de 1940, a casa bancária se tornou o Banco Moreira Sales, começando sua expansão territorial, abrindo várias agencias, no Rio de Janeiro, São Paulo, Santos e posteriormente se expandindo para outras regiões.

Como o Banco Moreira Sales obteve algumas ampliações, seus responsáveis acreditaram que seria interessante, economicamente falando, se fundir a outros bancos, o que de fato aconteceu em 1967, com Banco Agrícola Mercantil, e assim essa função deu origem ao União de Bancos Brasileiros S.A. Entretanto, em meados de 1975, houve uma mudança no nome, visto que o antigo União de Bancos Brasileiros não gerava identificação aos consumidores, o que poderia trazer uma baixa nas contratações dos serviços, originando assim o UNIBANCO.

O que conhecíamos, até 2008, como Banco Itaú deu-se início com o nome Banco Central de Crédito, que surgiu em 1943, começando suas atividades em 1945. Todavia com a criação do Banco Central e algumas alterações do sistema bancário, tornou-se necessário que o Banco Central do Brasil modificasse seu nome, transformando-se em Banco Federal de Crédito S.A.

Com o passar das atividades desenvolvidas por eles, os dirigentes do Banco perceberam que seria viável uma fusão com outra instituição financeira para que pudessem realizar mais transações e atingirem uma maior quantidade de pessoas. Tal crescimento aconteceu via fusão do Banco Federal de Crédito S.A. com o Banco Itaú S.A. E em 1975 além do Banco Itaú foi criada a Itausa, uma *holding* para administração de todas as empresas do grupo Itaú.

Em 1980, o Banco Itaú começou a inserir em suas agências a modernização e investimentos em tecnologia. Outrossim, houve a aquisição de uma grande quantidade de computadores e equipamentos eletrônicos, o que posteriormente seria conhecido como banco eletrônico. Com essas novidades, o Banco Itaú continuou crescendo e oferecendo novos serviços e novas vantagens para os

clientes.

Até que, em 2008, O UNIBANCO e o Banco Itaú se fundiram, dando origem ao Itaú-Unibanco. Com essa união houve o crescimento do Itaú Unibanco, fazendo parcerias com a Porto Seguro, no ramo dos seguros de carro e de residências. E desde 2009 introduziu a internet em suas ações, devido a facilidade e rapidez que poderia ser proporcionada aos seus clientes, devido à nova realidade tecnológica que estava principiando.

1.4.1.2 Origem do banco BRADESCO

O Banco Bradesco tem origem em 1943, sendo criado por Amador Aguiar e alguns amigos, oriundo de uma casa bancária localizada em Marilia-SP, tendo como proposito, auxiliar uma gama da população, como lavradores, funcionários públicos, pequenos comerciantes e indivíduos com recurso limitados.

Deste modo o Bradesco incentivou algumas transações, como o uso do cheque e a criação da conta corrente popular e juvenil. E essas contas possibilitaram o pagamento de conta de luz, e postos para entrega da declaração do imposto de renda. Destarte, também investiu em projetos sociais, criando a Fundação Bradesco, instituição que oferece cursos e educação para a população.

Em relação ao aperfeiçoamento nos seus serviços, o Bradesco inseriu o primeiro computador de grande porte, possibilitando aos clientes o acesso aos extratos diários. Além da criação dos caixas executivos que facilitaria a vida do cliente, para que eles realizassem transações mais simples, como pagamentos e recebimentos. O Bradesco foi responsável por criar uma função para que os brasileiros pudessem sacar o dinheiro que estava em suas contas a qualquer hora, por conta dos SOS Bradesco (caixa eletrônicos). Em 1990, todas as agências do Bradesco abraçaram os sistemas online, marcando o autoatendimento por máquinas BradescoNet. E após essa inovação, deu-se início as melhorias e investimentos que futuramente seriam apresentados ao público.

Diante da melhoria nas transações bancárias e das inovações tecnológicas, foram-se criando ainda mais facilidades para o consumidor, como por exemplo a criação dos aplicativos bancários, os quais proporcionaram a resolução de problemas de forma virtual, além de fazer transferências bancárias e acessar alguns serviços dos bancos de forma remota. Contudo, para que essas ações pudessem

começar a serem realizadas, foi necessário a criação de um sistema seguro, para que as transações ocorressem sem o perigo de um “vírus” acessasse o sistema e “roubasse” os dados da pessoa que estaria realizando a ação.

Deste modo foi criada o *internet banking,* uma ferramenta oferecida pelos bancos tradicionais que possibilita as operações financeiras serem realizadas de forma online, e assim serem feitas pelo uso de aplicativo ou o site do banco. Dentre as finalidades da *internet banking* está a abertura de contas, consulta de extrato e saldo, pagamento de contas, contratação de empréstimos e transferências bancárias.

Embora algumas pessoas ainda desconfiem, o *internet banking* é uma ferramenta segura, em que as instituições financeiras utilizam vários programas de segurança avançados para proteger as informações financeiras dos consumidores. E em alguns casos, o usuário também deve fornecer informações adicionais para acessar a plataforma, como um código enviado por mensagem de texto, biometria e reconhecimento facial, por exemplo. Além disso, os bancos ainda costumam monitorar atividades suspeitas, como tentativas de login inválidas ou transações financeiras que o cliente não reconheça. (Serasa, 2020).

1.4.1.3 BANCOS DIGITAIS

Com o advento da internet, algumas funcionalidades do cotidiano de tornaram mais fáceis e rápidas, sejam elas as pesquisas para saber o significado das palavras, os sintomas que podem ser sentidos diante de uma doença, até a realização de atividades bancárias. Deste modo houve a criação dos bancos digitais, instituições ao redor de todo o mundo com o intuito de viabilizar as ações que se desenvolvem nos bancos tradicionais.

Os bancos digitais têm como finalidade a criação de contas correntes, contratação de empréstimos, transferências bancárias, dentre outras atividades são oferecidas pelos bancos que possuem uma agência presencial. Desta maneira, uma das diferenças gritantes entre esses bancos é a falta de agências físicas nos casos das instituições bancárias digitais, onde é possível a realização dos serviços de forma *online*, seja por computador ou aplicativo do celular.

Urge salientar que outra diferença que acompanha os bancos tradicionais, que oferecem serviços digitais, dos bancos digitais se dá pelo uso da *Internet*

Banking. Tal recurso está interligado aos bancos tradicionais, para que o usuário vá até uma agência física, pois já possui uma conta no estabelecimento, e assim possa realizar abertura de constas, desbloqueio de alguns serviços online e cadastro de senhas.

Por se tratar de bancos digitais, dentre outros benefícios, é possível que a instituição possibilidade a falta de anuidade nos cartões de crédito e débito, não possuir tarifas para alguns serviços no próprio sistema. É importante ficar atento, pois em transações entre bancos diferentes pode haver a cobrança de alguma taxa.

Os bancos digitais possuem autorização para funcionar, sendo monitorados pelo Banco Central, seguindo diretrizes bem estabelecidas, e assim, em meados de 2016 surgiram os primeiros bancos digitais brasileiros, dentre eles o Banco Inter, Neon, Original, e posteriormente em 2016 a criação da NUBANK.

a) ORIGEM DO BANCO INTER

O Banco Inter teve seu início como um banco tradicional, que antes era conhecido como Banco Intermedium, tendo origem com a ideia do principal responsável pela construtora MRV (Mario, Rubens e Veiga Engenharia) decidiu criar uma instituição financeira para que os clientes da MRV pudessem realizar operações de crédito para financiar os imóveis da empresa.

Devido à grande procura, o Banco Intermedium recebeu do Banco Central a autorização para começar a atuar como banco, oferecendo uma maior variedade de serviços para serem apresentados aos seus usuários. Já em 2014 criou-se a primeira conta digital brasileira, sem a cobrança de tarifas, além de oferecer serviços bancários como os bancos tradicionais. Com o aumento da procura por aqueles serviços da instituição ocorreu uma remodelação do nome do banco, assumindo o nome de Banco Inter.

b) ORIGEM DO NUBANK

O Nubank foi criado com o intuito de facilitar a abertura de contas, e resolver problemas financeiros. A primeira oferta aos clientes veio por meio de um cartão de crédito sem anuidade, mas não existia uma conta corrente acompanhada e era controlado pelo aplicativo no celular. Com o crescimento e procura por mais

atividades, o Nubank lançou sua conta corrente, que se destacou no cenário nacional devido ao rendimento automático do CDI.

2. HISTÓRIA DA INTERNET

Na década de 1950, durante o auge da Guerra Fria, era bem claro para todos que a informação representava poder. Em um conflito ideológico como aquele, qualquer nova ideia seria bem recebida, pois, em teoria, poderia representar uma maneira de encerrar essa disputa.

Desta forma, o governo dos EUA (Estados Unidos da América) concentrou alguns de seus estudiosos para aprimorar a forma como os computadores, que existiam, pudessem transmitir algumas informações para outros aparelhos, que estavam em outros lugares. Destarte começaram os desenvolvimentos do que viria a se chamar ARPANET, um mecanismo que seria usado pelos militares e cientistas para compartilhar inovações, em suas respectivas áreas.

Devido as melhorias que aconteciam nesse sistema, as Forças Armadas usufruírem deste mecanismo se tornou perigoso, devido à grande utilização por terceiros, dessa maneira, os militares migraram seus afazeres para uma outra rede, enquanto a Arpanet se tornou mais comercial, possibilitando que outras pessoas começassem a utilizar deste serviço.

Com o passar dos anos, e o desenvolvimento de novas tecnologias, os pesquisadores viram necessidade de melhorar a Arpanet, o que acarretou a criação do "World Wide Web" (que futuramente seria popularmente conhecido como WWW) uma espécie de programação que levaria as informações e documentos, que facilitou o acesso para a população e diversas áreas de atuação, sendo ela compartilhamento de notícias, bate papos *online*, compras e até transações financeiras.

2.1 A INTERNET NO BRASIL

Em meados de 1988, uma parceria entre a Fundação de Amparo à Pesquisa do Estado de São Paulo (Fapesp) e uma universidade estadunidense deu início ao acesso à internet. E ao mesmo tempo, a Universidade Federal do Rio de Janeiro

(UFRJ) entrou em contato com outras universidades estadunidenses para que fosse possível o ingresso na rede mundial de computadores.

Quando o Governo Federal notou as implicações desse tipo de tecnologia no cotidiano, decidiu manifestar seu interesse em regular e tomar conta desta área, e assim a Embratel estava disposta a se responsabilizar por este ramo, pois já era de sua responsabilidade cuidar dos serviços interurbanos e internacionais. Contudo, naquele período, o Brasil sofreu uma mudança em relação as empresas estatais (dentre elas, a Embratel), ou seja, a ideia do Governo e da Embratel de serem as únicas provedoras de internet no território nacional foram freadas, uma vez que a iniciativa privada começava a alçar voos em território nacional. Mas para que as decisões fossem tomadas em consenso, e no intuito de viabilizar o uso desta, para toda a população, o governo criou o Comitê Gestor de Internet (Cgi.br), órgão responsável pela tomada de decisões acerca deste assunto. Esta entidade formada por 21 membros, sendo eles 12 pessoas da Sociedade Civil e 9 do governo, e por isso são responsáveis pela tomada de algumas decisões que envolvem os serviços de internet no país.

2.1.1 Primeiras legislações sobre a internet

Para que a internet fosse utilizada no Brasil era necessário que existisse uma norma que regulasse este serviço. Entretanto, uma redação que se tratasse apenas deste assunto só veio a ser redigida com o primeiro grande escândalo em volta deste tema, sendo ele a exposição de fotografias intimas da atriz brasileira Carolina Dieckman. Naquela época, por não haver nenhum dispositivo que pudesse julgar os responsáveis pela divulgação das fotos, os autores não foram punidos de forma correta. Com a repercussão do fato, um ano depois, a Lei 12.737/2012 foi sancionada, modificando os artigos 154-A e 154-B do Código Penal Brasileiro (CP), trazendo a pena de 6 meses a 2 anos para o infrator que cometesse crimes virtuais e delitos informáticos, como a invasão de dispositivos informáticos com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do proprietário. E que posteriormente, no ano de 2021 voltaria a sofrer uma nova alteração, por meio da Lei 14.155/2021, onde a pena novamente seria alterada.

3. Lei do marco civil da internet – Lei 12.965/2014

Seguindo o artigo 1º da Lei 12.965/2014, mais comumente conhecida como Lei do Marco Civil da Internet, 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.

Também é possível encontrar quais os objetivos do uso da internet no Brasil, como o direito de acesso à internet, do acesso à informação, ao conhecimento, outro ponto que cabe salientar é que existe no artigo 5º a explicação de alguns termos para a legislação brasileira, tendo como explicação termos como a internet, terminal, endereço de protocolo de internet (endereço IP), e outros mais.

Ao analisar a referida lei, em seu capítulo II, onde trata dos direitos e garantias dos usuários, nota-se que o internauta é assegurado por lei a manter sua privacidade em relação aos seus dados de acesso, sua vida privada e suas comunicações, salvo por ordem judicial na forma da lei. Tais ordens judiciais serão pedidas apenas se necessário, em casos de investigação.

Outro ponto descrito em seus artigos se trata da confirmação de que os indivíduos são amparados por lei em relação a ter informações claras e completas sobre o regime de proteção de suas conexões, assim como bem diz o artigo 7º, VI e seguintes.

Em seu capítulo III, a legislação traz o conteúdo que envolve a provisão de conexão e de aplicações de internet, e nesta parte é possível observar a subdivisão do texto em seções, para que cada tema seja abordado de forma clara. Em sua seção I, a Lei trata da neutralidade de rede, isto é, os provedores e responsáveis pela rede tem a obrigação de tratar todos sem nenhuma distinção, seguindo o princípio da isonomia. Quando a seção II expõe o que é assegurado ao usuário em relação a proteção aos Registros, aos Dados Pessoais e às comunicações privadas, proporcionando a segurança de que o que for pesquisado e os dados colocados em determinados locais da internet, serão sigilosos, salvo questões judiciais, que serão citadas em outra seção. E esta seção, acaba por se subdividir, carregando a subseção I, tratando da Guarda de Registros de Conexão. Já na subseção II nota-se o texto sobre Guarda de Registros de Acesso a Aplicações de Internet na Provisão

de Conexão, enquanto a subseção III explicita a Guarda de Registros de Acesso a Aplicações de Internet na Provisão de Aplicações.

De forma geral a subseção I trata da neutralidade da rede, garantindo que a internet não seja bloqueada ou restringida para diferentes tipos de conteúdo. Já a subseção II esclarece que a proteção aos registros, dados pessoais e comunicações privadas, possui regras para a coleta, tratamento e uso de dados pessoais. Enquanto a subseção III elucida a demanda envolvendo a responsabilidade por danos decorrentes de conteúdo gerado por terceiros, definindo como a responsabilidade é distribuída quando alguém é prejudicado por conteúdo publicado na internet. A seção III explana a responsabilidade por danos decorrentes de conteúdo gerado por terceiros.

A seção IV ilustra as condições para que ocorra a requisição judicial de registros, sendo este medido com o propósito de formar conjunto probatório, como descreve o artigo 22, com a aceitação do juiz é necessário garantir que os dados requisitados, mantenha-se em sigilo para resguardar a intimidade da parte. E em seu capítulo IV, o texto expressa os direitos, deveres e limites para a atuação do Poder Público, sendo ele a União, os Estados, Distrito Federal (DF) e municípios. E por fim, o capítulo V aborda as disposições gerais da Lei.

3.1. Lei 13.709/2018 – Lei Geral de Proteção de Dados (LGPD)

A Lei Geral de Proteção de Dados (LGPD) foi sancionada para proteger os dados pessoais em todos os ambientes, sejam eles no mundo virtual ou não. Tanto é que em seu 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, explicando assim que a LGPD garante a proteção dos dados pessoais, independente do ambiente a ser usado.

Em seu artigo 5º a redação esclarece o que considera dado pessoal, dado pessoal sensível, dado anonimizado, banco de dados, dentre outros conceitos que serão citados na referida lei, para que assim não ocorra dificuldade no entendimento

da matéria. Em seu inciso VIII ao clarificar o que é considerado encarregado, verifica-se que existe a Autoridade Nacional de Proteção de Dados (ANPD).

Já em seu artigo 6º, os legisladores optaram por especificar os princípios e a boa-fé que será utilizada no uso destes. No desenvolvimento do texto, o capítulo II amparará o que estiver relacionado ao tratamento de dados pessoais, sendo eles os Requisitos para o Tratamento de Dados Pessoais (seção I), as hipóteses em relação ao Tratamento de Dados Pessoais Sensíveis (seção II). Para melhor compreensão da LGPD os dados pessoais são as informações relacionadas a pessoa natural, enquanto os Dados Pessoais Sensíveis envolvem a origem racial, convicção religiosa, opinião política, dentre outros, assim como está descrito em seu artigo 5º, inciso I e II. Também, de forma específica, expõe sobre o Tratamento de Dados Pessoais de Crianças e de Adolescentes, desde que seja para o melhor interesse dos supramencionados e seguindo legislação pertinente (seção III), do término do tratamento de Dados (seção IV).

No capítulo III, são apresentados os direitos do titular, que é a pessoa proprietária dos dados pessoais que podem ser acessados. Esses direitos garantem, entre outras coisas, a confirmação da existência de tratamento dos dados, o acesso a essas informações e o direito de solicitar a eliminação dos dados pessoais. Já no capítulo IV, é feita uma explicação sobre como o Poder Público realiza o Tratamento de Dados Pessoais. Vale ressaltar que no capítulo IV, existe a seção II, a qual trata de um possível uso dos dados pessoais dos indivíduos, ou quando houver uma infração ou abuso de autoridade quanto a LGPD, por parte dos órgãos públicos.

A Lei 13.709 expressa como decorre a transferência internacional dos dados protegidos por esta legislação oriundos do território nacional, para países ou organismos internacionais, identificando os casos que serão aceitos e como estes deverão proceder para solicitar as informações. No capítulo VI os agentes de tratamento de dados pessoais serão o foco desta parte do texto, visto que existirão subseções como Do Controlador e do Operador (seção I), Do Encarregado pelo Tratamento de Dados Pessoais (seção II) e Da Responsabilidade e do Ressarcimento de Danos (Seção III). Em seu capítulo VII o assunto a ser tratado será Da Segurança e das Boas Práticas o que acarretará a discriminação Da Segurança e do Sigilo de Dados (seção I) e Das Boas Práticas e da Governança (seção II).

Esta regulamentação exterioriza como se dá a fiscalização da forma errônea que os dados foram usados, sejam eles por seus Agentes de tratamento, que sofrerão Sanções Administrativas (seção I). No penúltimo capítulo, a Lei aborda a Autoridade Nacional de Proteção de Dados (ANPD) e o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, dedicando uma seção específica para cada um deles (I e II). Por fim, no capítulo X, são apresentadas as Disposições Finais e Transitórias.

4. CRIMES CIBERNETICOS

Os crimes cibernéticos visam punir os autores dos delitos cometidos por meio da internet. Dentre estes crimes, podemos citar, desde os crimes contra a honra, sendo eles a calúnia, difamação e injúria, passando por crimes como xenofobia, homofobia, pornografia infantil, chegando aos crimes que envolvem a invasão dos dispositivos privados, clonagem de dados e até transferências bancárias de forma ilícita.

Para que a internet funcione é necessário que exista alguns códigos e programas para que possa ocorrer o acesso as diversas funcionalidades que a rede mundial de computadores pode oferecer, esses códigos e programas são conhecidos como software, e alguns desses códigos tem como objetivo o uso de sistemas operacionais, programas de aplicativos e navegadores de web.

Quanto ao uso destes, é fundamental que o usuário procure sites respeitáveis, seguros e livres de malware para adquirir os serviços dos códigos procurados, a fim de assegurarem contra-ataques de crimes cibernéticos, como a invasão dos dispositivos, ou uso de senhas para obter vantagens como entrar em contas de bancos.

Um dos tipos mais comuns de ataques cibernéticos se dá pelo uso dos *malwares* (*malicious software* ou *software* malicioso), que pode ser entendido como uma categoria de códigos maliciosos para prejudicar ou explorar qualquer dispositivo, serviço ou rede programável, por conseguinte existem vários tipos de *malwares* para facilitar o ataque as camadas de segurança dos aparelhos ligados a *WEB.*

Assim, como em diversas áreas, há pessoas que se destacam como especialistas em certos conhecimentos. No campo da internet, por exemplo, temos

os *hackers*, que, de uma forma geral podem ser definidos como pessoas com um conhecimento profundo de computação e informática, que trabalham desenvolvendo e modificando *softwares e hardwares* de computadores, não necessariamente para cometer algum crime.

No entanto, como foi mencionado ao longo deste texto, há pessoas que têm conhecimento especializado na área e utilizam esse conhecimento para cometerem fatos ilícitos. E com a criação da denominação dos *hackers*, fez-se necessário a subdivisão do termo *hacker* para que não houvesse discriminação para com todos aqueles que dispõe de entendimento da rede mundial de computadores. Assim sendo, as tipificações presentes são:

- *White Hat*: é o mesmo que o "*hacker* ético", um profissional de segurança dedicado apenas a proteger sistemas; trabalham de forma ética, auxiliando na proteção de sistemas e redes, ajudando empresas e governos a identificarem vulnerabilidades antes que sejam exploradas.

- *Grey Hat*: é a pessoa que vai mexer em sistemas que estão no ar, que operam em uma área cinzenta, às vezes invadindo sistemas sem autorização. Mas ao descobrir uma falha, vai reportar aos responsáveis ou fazer algo que comprove a falha, mas sem efeito nocivo

- *Black Hat*: é o criminoso, a pessoa que vai abusar de sistemas para benefício próprio. Estes são os *hackers* mal-intencionados, também conhecidos como *craker's* que realizam ataques cibernéticos para roubo de dados, extorsão ou sabotagem.

4.1 TIPOS DE *MALWARE*

a) VIRUS

"Vírus é um código malicioso que "sequestra" um *software* legítimo para causar danos e espalhar cópias de si mesmo. Os vírus não podem agir sozinhos. Em vez disso, ocultam trechos do código em outros programas executáveis. Quando um usuário inicia o programa, o vírus também começa a ser executado. Os vírus geralmente são projetados para excluir dados importantes, interromper as operações normais e espalhar cópias de si mesmos para outros programas no computador

infectado. Um vírus geralmente vem como um anexo em um e-mail que contém uma carga de vírus, ou parte do malware que executa a ação maliciosa. Depois que a vítima abre o arquivo, o dispositivo está infectado.”

b) SPYWARE

O *spyware* se esconde em um computador infectado, coletando secretamente informações confidenciais e transmitindo-as de volta ao invasor. Um tipo comum de *spyware*, chamado *keylogger,* registra todas as teclas digitadas pelo usuário, permitindo que os hackers coletem os nomes de usuário, senhas, números das contas bancárias e de cartão de crédito, números da segurança social e outros dados confidenciais.

4.2 TIPOS DE ATAQUES AOS DISPOSITIVOS

a) FORÇA BRUTA

Esta forma de conseguir diferentes informações contidas no aparelho se dá por tentativa e erro, ou seja, o indivíduo ficará tentando por diversas vezes conseguir acessar o que é de interesse dos *crakres*. Além disso, esse tipo de invasão também pode ocorrer pessoalmente, se a pessoa que quer obter as informações tiver acesso ao aparelho.

b) FALSIFICAÇÃO DE E-MAIL (E-MAIL *SPOOFING)*

Falsificação de e-mail (E-mail *spoofing*): é uma técnica que consiste em alterar campos do cabeçalho de um e-mail de forma que pareça que ele foi enviado de um determinado remetente, quando na verdade, foi enviado de outro.

c) HACKEAMENTO

Segundo o delegado de polícia Augusto César que atua no estado de Sergipe o hackeamento trata-se de uma invasão e obtenção de dados sensíveis da vítima, ou seja, quando o criminoso consegue acesso tanto ao dispositivo, quanto às contas de redes sociais ou bancárias da vítima

d) *PHISHING*

Esse tipo de golpe consiste em tentativas de fraude para obter ilegalmente informações como número da identidade, senhas bancárias, número de cartão de crédito, entre outras, por meio de e-mail com conteúdo duvidoso.

Há uma série de técnicas que os cibercriminosos utilizam para subtrair informações, as duas mais comuns são:

- E-mail/Spam: consiste em mensagens falsas relacionadas a bancos ou instituições, que levam o destinatário a fornecer seus dados pessoais. O mesmo e-mail é enviado para milhares de pessoas.

- *Malware*: após o usuário clicar em um link disponível no e-mail, o programa malicioso começa a funcionar na máquina coletando informações. Também pode ser anexado em arquivos para download.

- Para conseguir *hackear* os dispositivos eletrônicos e as contas das vítimas, os criminosos utilizam técnicas que envolvem o envio de links em mensagens pelo celular ou ainda por e-mail. “Esses links contêm vírus que, evidentemente, depois de instalados nos celulares capturam dados sensíveis, a exemplo de senhas”, explicou o delegado Augusto César, integrante da 1ª DM.

Além de enviar links com vírus, os criminosos também utilizam a técnica de clonagem do chip da linha telefônica, assim como detalhou o delegado Augusto César. “O chip identificador dá acesso à linha telefônica e, quando a vítima perde o acesso a esse chip, o criminoso acaba obtendo acesso aos links e códigos de verificação de segurança que são encaminhados por SMS”, relatou.

Um link malicioso é um URL que, quando acessado, direciona a pessoa para um site ou página da web projetado por criminosos para causar danos aos dispositivos ou roubar informações.

Esses links são frequentemente usados e conhecidos por todos como ataques de phishing, onde os criminosos tentam enganar suas vítimas para que eles forneçam dados, como senhas, informações financeiras ou detalhes pessoais.

No caso de empresas, quando um colaborador clica nesse link fornece informações confidenciais que, caso caiam em mãos erradas, impactam negativamente a organização.

Esses links podem vir por diversos canais, como:

- E-mail;
- SMS;
- Redes sociais;
- Aplicativos de conversa.

5. TIPOS PENAIS ESPECÍFICOS

5.1 Análise do Art. 154-A do CPB

O primeiro artigo a ser analisado, artigo 154-A, está inserido na parte especial do CPB (Código Penal Brasileiro), nota-se que existe um bem jurídico especifico a ser protegido, e como o crime de invasão de dispositivo informático está inserido no Título I que expõe os crimes cometidos contra a pessoa, e no Capítulo VI, dos crimes contra a liberdade individual e presente na seção IV, dos crimes contra a inviolabilidade dos segredos, o bem jurídico tutelado é a privacidade de quem está usando o equipamento físico (*hadware)*. E assim vale salientar ainda que a vítima do crime pode ou não ser dona do aparelho, desde que tenha sua privacidade prejudicada.

Em sua redação, o art. 154-A, trata da conduta do sujeito ativo de praticar a invasão do dispositivo informático, com o fim de ter acesso ao aparelho como um todo, e após conseguir a conexão com o dispositivo poderá alterar os dados e informações que estejam salvos no celular ou periférico. Uma outra conduta que está descrita se refere ao fato de, caso o autor conseguir realizar a invasão, conseguir inserir algum programa que facilite a instalação de vulnerabilidades no sistema. Tal conduta é penalizada com reclusão de 1 (um) a 4 (quatro) anos, além de multa.

No §1º do mesmo artigo também incorre quem vende, produz ou distribui os programas que viabilizam a execução do ato ilícito especificado no caput. Já no §2º ao minuciar um prejuízo que pode acontecer devido a prática delitiva, ocorre o aumento da pena. O §3º explicita um outro resultado que pode acontecer devido a ação da invasão, o que está assegurado neste parágrafo está envolvido a obtenção dos dados pertencentes a empresas, tendo uma outra pena, e logo após, em seu

próximo § explana uma nova sanção a qual se refere na divulgação das informações obtidas. Enquanto o §5º esclarece as punições a quem comete as ações descritos no caput contra algumas entidades especificas do Brasil.

5.2 Análise do Art. 155, §4º-A do CPB

O art. 155, §4ºA a ser examinado está exposto na parte especial do Código Penal Brasileiro, nota-se que existe um bem jurídico específico a ser protegido, e como o crime de furto qualificado está inserido no Título II que expõe os crimes cometidos contra o patrimônio, e no capítulo I, do furto, o bem jurídico tutelado é o patrimônio de quem tem a posse ou propriedade da coisa.

O artigo 155, caput descreve que ao subtrair para si ou para outrem coisa alheia móvel é considerado como furto, e logo após esta redação, acontecem algumas especificações que poderão majorar a penalidade, dentre elas a conduta de o furto acontecer mediante uma fraude, e essa fraude ocorrer por meio de dispositivo eletrônico.

A redação do artigo explica que, o bem jurídico protegido é a coisa alheia móvel, ou seja, alguma coisa que possa ser considerada propriedade, ou possibilitar a posse ou detenção legítima e que propicie o transporte de um lugar para outro.

O texto apresentado no art. 155, §4º B tem a seguinte redação

> 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.

e ao observar, percebe-se que ocorre a especificação da majorante que acompanha esta conduta. Em relação a situação qualificada a ser aprofundada, o crime pode ser explicado que a conduta independe de estar conectado ou não à rede de computadores, haver ou não violação de mecanismo de segurança (ex.: hackear senha), haver ou não utilização de programa malicioso (ex.: instalar programa que capta senha do usuário).

Um exemplo que pode ser usado para que fique mais claro a situação é, se o agente invade o computador da vítima, lá instala um malware (programa malicioso), descobre sua senha e subtrai valores de sua conta bancária.

5.3 Análise do Art. 171, §2º A do CPB

O terceiro artigo a ser estudado (art. 171, §2º A) está exposto na parte especial do Código Penal Brasileiro, percebe-se que existe um bem jurídico específico a ser protegido, e como o crime de fraude eletrônico está inserida no Título II que expõe os crimes cometidos contra o patrimônio, e no capítulo VI, do estelionato e outras fraudes, o bem jurídico tutelado é o patrimônio de quem tem a posse ou propriedade da coisa.

Para entender o §2º A do artigo 171, é necessário que o próprio caput seja exposto, tendo a seguinte redação:

> 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:

Ou seja, para ser considerado o estelionato é necessário que ao praticar a conduta, o autor obterá uma vantagem ilícita e ter um prejuízo alheio, além de ser um crime praticado contra o patrimônio. Deste modo a vantagem de ilícita pode significar que a pessoa adquiri bens, serviços ou dinheiro, ou algo que cause prejuízo a outra pessoa, prejuízo este sendo patrimonial ou financeiro, dentre outros.

Ao ler o caput do artigo, e ao esmiuçar o núcleo do tipo, é possível ter a compreensão de que o a redação pode ser entendida da seguinte forma:

Induzir a pessoa (o próprio agente que gera na vítima a falsa percepção da realidade) ou manter a vítima em erro (a vítima já está enganada e o agente se aproveita disso – fica em silêncio),

Mediante as seguintes situações: artifício (documento falso, falso bilhete premiado, falso uniforme), ardil (conversa enganosa) ou qualquer outro meio fraudulento (inclusive por omissão).

Assim, ao investigar a fraude eletrônica, nos é apresentado o seguinte texto:

> § 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

O que difere o estelionato comum da fraude eletrônica acontece pelo meio o qual acontece, no caso do §2º A essa vantagem ilícita foi ganha por intermédio das redes sociais (aplicativos de mensagens como WhatsApp e Telegram, Instagram e Facebook), contatos telefônicos (onde autores se passam por gerentes de bancos, operadoras de cartão de crédito, dentre outros), além de envio de correio eletrônico fraudulento (e-mail avisando que sua compra foi retida na Alfandega, ou disponibilização de algum link para que a vítima possa acessar um *malware*).

5.4 Diferença entre os artigos

Invasão de Dispositivo Informático (art. 154-A): acontece quando o autor se aproveita de seus conhecimentos na área para conseguir entrar no sistema operacional para conseguir dados pessoais de quem estiver usando o aparelho celular ou computador.

Furto Mediante Fraude (art. 155, §4º-B do CP): ocorre quando o agente utiliza artifício (fraude material – ex.: falso uniforme de garçom do local para subtrair pertences da mesa de clientes) ou ardil (fraude intelectual – conversa enganosa) para enganar a vítima e subtrair seus bens.

Fraude Eletrônica (art. 171, §2º-A do CP): neste artigo a fraude é empregada para ludibriar a vítima, para que ela própria entregue livremente seu bem ao agente (ex.: falso assistente técnico de tv – a vítima entrega para consertar e o agente foge com ele), enquanto no furto, a fraude é para facilitar a subtração.

CONCLUSÃO

Após esclarecer a origem das relações de transações entre as pessoas, foi possível observar que as transferências pecuniárias foram evoluindo de acordo com as relações interpessoais e a necessidade dos indivíduos de coexistirem no mesmo ambiente, e poderem auxiliar na sua subsistência sem que lhe faltasse algo que, para eles, seria de suma importância. Ao analisar as obras que retratam os períodos históricos da humanidade é factível examinar que sempre houve pessoas com uma "visão" diferenciada, onde conseguiram perceber a necessidade de uma troca entre as coisas que já possuíam, ou que seria necessário que houvesse o empréstimo daquilo que já dispunham, para outros que viam necessidade de usufruir de tal objeto, ou mercadoria que lhe era oferecido.

Assim, com o passar do tempo, com o surgimento das civilizações e interações sociais, a forma como essas pessoas trocavam e usavam as coisas que tinham a seu dispor foi sendo atualizada para que se desse uma boa convivência.

Deste modo com a invasão do território, que mais tarde seria conhecido como Brasil, houve a necessidade de a Coroa Portuguesa intervir nas formas das pessoas que aqui viviam, para que começasse a ocorrer um mercado, e para tal foi necessário a implantação das seções bancárias, que posteriormente seriam conhecidas como casas bancárias. E com a criação das casas bancárias ocorreu a evolução destes estabelecimentos, se transformando nos bancos privados e federais que conhecemos hoje, como o Banco Bradesco, Itaú Unibanco, Caixa Econômica Federal e Banco do Brasil.

Já com a invenção da Rede Mundial de Computadores adveio da necessidade dos potenciais mundiais de aprimorar os conhecimentos que já detinham, para possíveis ataques bélicos de outras nações. E como na época que começaram os estudos acerca deste tema, as superpotências que estavam em evidência, eram os Estados Unidos da América (EUA) e a União Soviética, em decorrência da Guerra Fria, sucederam vários episódios em que o EUA não mediu esforços para que as Forças Armadas pudessem ter alguma vantagem, caso acontecesse algum ataque armado. Entretanto, como a notícia dessa nova tecnologia foi se espalhando, vários estudiosos concentraram suas pesquisas nesta área, onde foi possível que a WEB se tornasse perigosa para o exército

estadunidense, e assim, se tornou mais viável que a população tivesse acesso a internet e que as Forças Armadas desenvolvessem um sistema próprio.

Com a “decisão” tomada pela comunicante cientifica dos Estados Unidos, deu-se a liberdade para as universidades tentarem fazer contato entre si, para que pudessem ter a noção de onde o ciberespaço chegaria, e quais seriam as suas funções, inovações e onde poderiam ser usadas. Como a Rede Mundial de Computadores deu certo, abriu-se possibilidades de que outras instituições e populares conseguissem a oportunidade de usar a nova tecnologia. Deste modo, cientistas brasileiros em contato com universidades do EUA, desenvolveram formas de que a internet chegasse ao Estado, e assim lucrassem com a descoberta e aplicassem ao cotidiano.

Com a criação da WEB, foi possível a introdução deste serviço em diversas áreas, sendo elas os estudos, facilitação cotidiana, além de introduzir a internet nos sistemas bancários, favorecendo o serviço prestado pelas instituições financeiras, podendo auxiliar na criação dos caixas eletrônicos, e posteriormente na criação dos aplicativos bancários.

Todavia, com o lançamento destes aplicativos, e essas inovações os criminosos também não ficaram para trás, deste modo começaram a aplicar diversos golpes em pessoas que não fruíam de determinados conhecimentos, e acreditando estarem falando com os prestadores de serviço, ou parentes, a depender do delito cometido, realizam o que é pedido.

Destarte, a presente dissertação trouxe a explicação e diferenciação dos 3 crimes que visam o prejuízo financeiro, divulgação de informações das vítimas, que tem como meio de praticar o delito, a internet.

REFERENCIAS BIBLIOGRAFICAS

ANDRADE, Antônio *et al*. Hacker: Hacker ou Cracker? Entenda a Diferença e os Cuidados em um Mundo Digital. **APDADOS,** 2024. Disponível em: Hacker ou Cracker? Entenda a Diferença e os Cuidados em um Mundo Digital. Acesso em: 29 abr. 2025.

ANDRADE, Walmart *et al*. Marco Civil da Internet: tudo o que você precisa saber sobre a lei fundamental da Internet. **Walmart Andrade,** 2020. Disponível em: https://walmarandrade.com.br/marco-civil-da-internet/. Acesso em: 29 abr. 2025.

BOULOS, Alfredo Júnior. **360ª história sociedade e cidadania**. São Paulo: FTD, 2015.

BRASIL. Código Penal. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Rio de Janeiro: Imprensa Nacional, 1940

BRASIL, IBM *et al*. O que é Malware. **IBM,** 2024. Disponível em: https://www.ibm.com/br-pt/topics/malware. Acesso em: 29 abr. 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2024. Lei Geral de Proteção de Dados. Planalto.gov.br, Brasília, 14 de agosto de 2018

BRASIL, Lenovo *et al*. O que é Software. **LENOVO,** 2024. Disponível em: https://www.lenovo.com/br/pt/glossary/what-is-software/?srsltid=AfmBOoqAel7VsfwOmSbZg07FeEQN42sVbXo24iS_MJcYsvkT4gD4rfCr. Acesso em: 29 abr. 2025.

CARREIRAS POLICIAIS, Dedicação Delta. **Preparação pré-edital**: Delegado. 1. ed. Goiás: Dedicação Delta, 2021.

CESAR, Augusto. Estratégias dos hackers. **Polícia Civil do Estado de Sergipe,** 2021. Disponível em: https://policiacivil.se.gov.br/policia-civil-faz-alerta-para-cuidados-com-links-falsos-que-viabilizam-praticas-criminosas-envolvendo-hackeamento-de-celulares-e-golpes-na-internet/#:~:text=Estrat%C3%A9gias%20dos%20hackers,encaminhados%20por%20SMS%E2%80%9D. Acesso em: 14 maio 2025.

CONTENT, Redator Rock *et al*. Conheça a história da Internet, sua finalidade e qual o cenário atual. **Rock Content,** 2020. Disponível em: https://brasilescola.uol.com.br/informatica/internet.htm. Acesso em: 29 abr. 2025.

DEFENSORIA PUBLICA DO ESTADO DO CEARÁ. Lei Carolina Dieckmann: 10 anos da lei que protege a privacidade dos brasileiros no ambiente virtual. Publicado em 2 de dezembro de 2022. Disponível em: https://www.defensoria.ce.def.br/noticia/lei-carolina-dieckmann-10-anos-da-lei-que-protege-a-privacidade-dos-brasileiros-no-ambiente-virtual/. Acesso em: 22/04/2025.

FEDERAL, Governo *et al*. Crimes Digitais. **Ministério da Justiça e Segurança Pública,** 2024. Disponível em: https://www.gov.br/mj/pt-br/assuntos/sua-protecao/sedigi/crimes-digitais. Acesso em: 29 abr. 2025.

Figueiredo, Rudá. **Crimes eletrônicos e Lei 14.155/2021.** 2021. Faculdade Baiana de Direito

HELDER, Darlan *et al*. Hacker: Entenda o que é um 'hacker' e a diferença para 'cracker'. **G1,** 2023. Disponível em: https://g1.globo.com/tecnologia/noticia/2023/08/18/entenda-o-que-e-um-hacker-e-a-diferenca-para-cracker.ghtml. Acesso em: 29 abr. 2025.

LFTM MARKETING. História de Valor #003: a história dos bancos desde os Templários até a Revolução Industrial. 9 de abril de 2024. Disponível em: https://lftm.com.br/blog/historia-de-valor/a-historia-dos-bancos/#:~:text=Os%20primeiros%20bancos&text=Os%20bancos%20como%20conhecemos%20surgem,tendo%20sido%20fundada%20em%201406. Acesso em 02 de abril de 2025.

NICBrvideos. Sobre o CGI.br. Youtube, 10 de julho de 2012. 4min7s. Disponível em: https://www.youtube.com/watch?v=F38J9R5wugo. Acesso em: 29 de abril de 2025

PROTEÇÃO DE DADOS, Autoridade Nacional De *et al*. Institucional: tudo o que você precisa saber sobre a lei fundamental da Internet. **Ministério da Justiça e Segurança Pública,** 2024. Disponível em: https://www.gov.br/anpd/pt-br/acesso-a-informacao/institucional#:~:text=A%20ANPD%20%C3%A9%2C%20portanto%2C%20o,seus%20dados%20pessoais%20devidamente%20protegidos. Acesso em: 29 abr. 2025.

SANTA CATARINA, Tribunal De Justiça. Entenda como funcionam os ataques de hackers na Internet. **Poder Judiciário de SC,** 2024. Disponível em: https://www.tjsc.jus.br/web/servidor/dicas-de-ti/-/asset_publisher/0rjJEBzj2Oes/content/entenda-como-funcionam-os-ataques-de-hackers-na-internet. Acesso em: 29 abr. 2025.

SILVA, Daniel Neves. "História da internet"; *Brasil Escola*. Disponível em: https://brasilescola.uol.com.br/informatica/internet.htm. Acesso em 29 de abril de 2025.

SOUZA, Thiago. História da Internet: quem criou e quando surgiu. **Toda Matéria**, *[s.d.]*. Disponível em: https://www.todamateria.com.br/historia-da-internet/. Acesso em: 29 abr. 2025

TECNOLOGIA DA INFORMAÇÃO, Prodest. Entenda o que é phishing: e adote medidas para evitá-lo. **Governo do Estado do Espírito Santo,** 2024. Disponível em: https://prodest.es.gov.br/entenda-o-que-e-phishing-e-adote-medidas-para-evita-lo#:~:text=Ele%20consiste%20em%20tentativas%20de,e%2Dmail%20com%20conte

%C3%BAdo%20duvidoso. Acesso em: 29 abr. 2025.

TELEFONIA, Vivo. Você sabe qual é a diferença entre hacker e cracker, e como se proteger? **Vivo,** 2024. Disponível em: https://vivo.com.br/para-voce/por-que-vivo/vivo-explica/para-descomplicar/diferencas-entre-hacker-e-cracker#:~:text=Resumindo%3A%20ambos%20t%C3%AAm%20as%20mesmas,obter%20vantagem%20ou%20causar%20dano. Acesso em: 29 abr. 2025.

VIEIRA, Eduardo *et al*. **Os Bastidores da Internet: a história de quem criou os primeiros negócios digitais do Brasil**. Ebook: Manole, 2003.
FRAGA, Renê *et al*. **A História da Internet**. Kindle: Amazon, 2023.