CENTRO UNIVERSITÁRIO ALVES FARIA - UNIALFA
CURSO DE GRADUAÇÃO EM DIREITO

JULIANA CRISTHYNE FERREIRA SANTANA

CRIMES CIBERNÉTICOS E O DIREITO PENAL BRASILEIRO: As diferentes tipificações das condutas e suas consequências à luz do ordenamento jurídico-penalista

GOIÂNIA
JUNHO DE 2024

JULIANA CRISTHYNE FERREIRA SANTANA

CRIMES CIBERNÉTICOS E O DIREITO PENAL BRASILEIRO: As diferentes tipificações das condutas e suas consequências à luz do ordenamento jurídico-penalista

Trabalho monográfico apresentado ao Curso de Direito da Escola de Direito do Centro Universitário Alves Faria, sob orientação da Prof. Esp. Lucas Rocha Andrade, como requisito para a conclusão do Curso de Direito.

Prof. Esp. Lucas Rocha Andrade

GOIÂNIA

JUNHO DE 2024

JULIANA CRISTHYNE FERREIRA SANTANA

CRIMES CIBERNÉTICOS E O DIREITO PENAL BRASILEIRO: As diferentes tipificações das condutas e suas consequências à luz do ordenamento jurídico-penalista

Esta monografia foi analisada e julgada adequada para obtenção do título de Bacharel em Direito e aprovada em sua forma final pela Orientadora e Banca Examinadora designada pelo Curso de Direito do Centro Universitário Alves Faria.

_____

Prof. Esp. UNIALFA

Orientador

Aprovado em ____/____/_____.

BANCA EXAMINADORA:

_____

Profª. Me. UNIALFA

_____

Prof. Leitor – Instituição de origem

_____

Prof. Leitor – Instituição de origem

GOIÂNIA

JUNHO DE 2024

Dedico este trabalho a Deus, aos meus pais e a minha família.

AGRADECIMENTOS

Em primeiro lugar, agradeço a Deus, por toda força, amor e perseverança pela minha trajetória.

Agradeço, em especial, ao meu pai Jeferson de Deus Santana e à minha mãe Elayne Silva Ferreira Santana, que pese nunca deixar de me apoiar, incentivar, ajudar, amparar, fornecer o que me foi preciso. Vocês sempre acreditaram em mim, mesmo nos momentos mais difíceis, e me ensinaram o valor do esforço e da dedicação.

À toda a minha família, por ter me apoiado até aqui. Aos meus amigos pessoais, pela fraternidade inigualável.

Aos meus colegas de curso pela parceria, troca de conhecimentos e pelo apoio mútuo durante toda a jornada universitária. A amizade e companheirismo de vocês foram essenciais para tornar essa caminhada mais leve e prazerosa.

Ao meu orientador, Prof. Esp. Lucas Rocha Andrade, pela orientação durante o presente trabalho. Suas orientações precisas e críticas construtivas foram fundamentais para a elaboração deste trabalho.

A todo o corpo docente do Centro Universitário Alves Faria, pelo conhecimento dividido sabiamente com os discentes do Curso de Direito.

Por fim, agradeço a todos que, de alguma maneira, contribuíram para que este trab fosse concluído. A cada um de vocês, minha eterna gratidão.

RESUMO

SANTANA, Juliana Cristhyne Ferreira. **CRIMES CIBERNÉTICOS E O DIREITO PENAL BRASILEIRO: As diferentes tipificações das condutas e suas consequências à luz do ordenamento jurídico-penalista.** Monografia, 2024. 43 f. Curso de Graduação em Direito do Centro Universitário Alves Faria (UNIALFA). Goiânia, 2024.

Este Trabalho de Conclusão de Curso busca analisar as estimulações e avanços do direito, mais especificamente o direito penal. De acordo com as progressões da sociedade, cotidianamente utilizam-se os recursos do âmbito tecnológico para afazeres básicos do dia-a-dia, logo influencia no aumento dos crimes cibernéticos contra o patrimônio.
Desse modo, a vulnerabilidade da norma jurídica facilita a impunidade, assim, necessitando de um olhar crítico, buscando melhores soluções. O presente tema tem como objetivo geral a verificação das consequências do aumento de crimes cibernéticos para o direito brasileiro. Possuindo como problema de pesquisa o seguinte questionamento: hoje, o direito brasileiro está acompanhando a sociedade em relação aos crimes cibernéticos contra o patrimônio?
Portanto, com o objetivo de analisar as estimulações e avanços do ordenamento jurídico brasileiro. Após os avanços dos crimes cibernéticos no Brasil, utilizando-se a pesquisa básica em conjunto com o método dedutivo e a abordagem de pesquisa qualitativa, descritiva e bibliográfica.
Desse modo, é relevante a análise dos delitos: Invasão de dispositivo eletrônico - Art. 154-A; Furto mediante fraude eletrônica - Art. 155 §4-B; e Fraude eletrônica - Art. 171 §2-A. Tais delitos foram exemplos de aplicação do princípio da taxatividade.
Pois bem, com o objetivo concreto de verificar como essas normas acompanharam segurança jurídica para garantir o combate aos crimes. Igualmente, quais foram os obstáculos a serem superados para melhor efetivação.

PALAVRAS-CHAVE: Crimes cibernéticos. Direito penal. Crimes digitais contra o patrimônio.

.

ABSTRACT

SANTANA, Juliana Cristhyne Ferreira. **CYBER CRIMES AND BRAZILIAN CRIMINAL LAW: The different types of conduct and their consequences in the light of the criminal law system.** Monograph, 2024. 43 p. Undergraduate Course in Law at the Alves Faria University Center (UNIALFA). Goiania, 2024.

This thesis aims to analyze the stimulation and progress in law, especially in criminal law. According to the progress of society, technological resources are used on a daily basis for basic daily tasks, which therefore influences the increase of cybercrimes against property.
In this way, the vulnerability of the legal norm facilitates impunity, thus requiring a critical look in search of better solutions. The general objective of this topic is to verify the consequences of the increase of cybercrimes for Brazilian law. Having as a research problem the following question: Today, is Brazilian law following society in relation to cybercrimes against property?
Therefore, with the objective of analyzing the stimuli and advances of the Brazilian legal system. According to advances in cybercrime in Brazil, using basic research combined with the deductive method and the qualitative, descriptive and bibliographic research approach.
Therefore, it is relevant to analyze the following crimes: Invasion of an electronic device - Art. 154-A; Theft by electronic fraud - Art. 155 §4-B; and electronic fraud - Art. 171 §2-A. Such crimes were examples of the application of the principle of taxation.
Now, with the concrete objective of verifying how these standards accompanied legal security to guarantee the fight against crime. Likewise, what were the obstacles to be overcome for a better implementation.

KEYWORDS: Cybercrime. Criminal law. Digital crimes against property.

LISTA DE ABREVIATURAS E SIGLAS

ARPA - Advanced Research Projects Agency (Agência de Projetos de Pesquisa Avançada dos Estados Unidos)

ART - Artigo

CP - Código Penal

IBGE - Instituto Brasileiro de Geografia e Estatística

IP - Internet protocol (Protocolo da Internet)

MPF - Ministério Público Federal

TCP - Transmission Control Protocol (Protocolo de Controle de Transmissão)

SUMÁRIO

INTRODUÇÃO.....9

1. ANÁLISE INTRODUTÓRIA SOBRE A INTERNET E O CRIME CIBERNÉTICO11

1.1. Conceito de internet..... 11

1.2. A história da internet e seu desenvolvimento no mundo..... 11

1.3. O desenvolvimento da internet no Brasil.....13

1.4. Aspectos gerais do crime cibernético..... 15

2. CRIMES CONTRA O PATRIMÔNIO NA INTERNET..... 17

2.1. Art 154-A - Invasão de dispositivo informático.....18

2.1.1. Classificação doutrinária.....19

2.1.2. Figuras qualificadas e aumento de pena..... 22

2.2. Art. 155 §4-B, CP - furto mediante fraude eletrônica..... 23

2.2.1. Classificação doutrinária.....25

2.2.2. Causas de aumento de pena..... 26

2.3. Art. 171 §2-A - Fraude eletrônica.....27

2.3.1. A estrutura jurídica do crime de estelionato..... 27

2.3.2. Diferença entre furto mediante fraude eletrônica e estelionato eletrônico..... 30

3. DIFICULDADES E PERSPECTIVAS DA APLICAÇÃO DOS NOVOS DELITOS PENAIS.....30

3.1. Dificuldades na fase investigativa dos delitos cibernéticos.....30

3.2. Perspectivas na aplicação dos novos delitos penais.....34

4. CONSIDERAÇÕES FINAIS..... 36

REFERÊNCIAS.....39

INTRODUÇÃO

Este trabalho de conclusão de curso busca analisar as estimulações e avanços do direito, mais especificamente o direito penal. Conforme os dados revelados pela Pnad Contínua (Pesquisa Nacional por Amostra de Domicílios), coletada pelo IBGE, 84,4% da população a partir dos 10 anos de idade em 2021, possuíam celular para uso pessoal, utilizando os recursos digitais que essa tecnologia pode proporcionar. Conforme as progressões da sociedade, cada vez mais utiliza-se os recursos do meio digital no âmbito tecnológico para cometimento de crimes cibernéticos, especificamente contra o patrimônio. Desse modo, a vulnerabilidade do direito para com a aplicação da lei penal facilita a impunidade, assim, necessitando de um olhar crítico, buscando melhores soluções.

A evolução tecnológica impulsionou o cometimento de crimes cibernéticos, utilizando formas rápidas para a atuação de criminosos. A presente pesquisa busca analisar o comportamento do direito penal para com a modernização da sociedade, observando de uma maneira crítica, verificando os avanços de sua evolução. Assim, aderindo com o objetivo de combater de forma efetiva os crimes cibernéticos. Ao trazer a luz do direito sobre a importância de analisar tais crimes e sua inércia, vê-se o objetivo de aprimorar o direito brasileiro e auxiliar os seus avanços para com a sociedade.

Desse modo, questiona-se o âmbito histórico e os resultados na sociedade com aumento da utilização dos meios digitais. Portanto, interligando o início da internet para com a forma como a sociedade vive atualmente. A relevância do acompanhamento do direito, perante a sociedade, assegura os direitos fundamentais, presentes na carta magna. O fato de que o início do aprimoramento dos crimes cibernéticos desde o ano de 2020 impediu que o direito corretamente se adaptasse ao novo modo de cometer crimes.

Consoante a alta demanda pós-pandêmica do coronavírus, transgressões consideradas "novas" para o direito brasileiro foram sujeitas a ações de adiamento, logo, implementando leis para certos tipos de crimes efetuados através da internet. Dentre eles o crime de invasão de dispositivo informático (Art. 154-A, CP) já situado no código penal brasileiro desde 2012, pela lei nº 12.737/2012 (Lei Carolina Dieckmann). As novas disposições trazidas pela lei nº 14. 155 de 2021. O delito de furto mediante fraude eletrônica (art. 155 §4-B, CP) e o crime de estelionato mediante fraude eletrônica (Art. 171 §2-A, CP).

Consequentemente, novas modalidades surgem, desse modo, dificultando o combate da polícia judiciária. Analisando de forma minuciosa, entende-se a relevância de trazer em pauta tal problemática no ordenamento jurídico.

A pergunta relevante ao trabalho é questionar se atualmente, o direito brasileiro está acompanhando a sociedade em relação aos crimes cibernéticos. Portanto, analisa-se que o direito brasileiro demonstra a efetividade no combate aos crimes no meio digital. Igualmente, quais as possíveis dificuldades na ação e as perspectivas do poder judiciário em relação ao enfrentamento. Logo, esclarecendo as possíveis soluções para a problemática em questão.

Assim, para avaliar as estimativas e progressos do sistema jurídico brasileiro após os avanços dos crimes cibernéticos, foi utilizada a pesquisa básica em conjunto com o método dedutivo, além da abordagem qualitativa, descritiva e bibliográfica. O propósito principal foi verificar se as normas estão adequadas para assegurar a segurança jurídica dos direitos fundamentais e combater os crimes.

O presente trabalho se dividirá em três capítulos. A primeira seção trata-se de uma análise introdutória sobre a internet e o crime cibernético. Portanto, observará a criação da internet, bem como a relação da sociedade com a internet, tanto no mundo como no Brasil. Será pontuado historicamente o início de um sistema, primeiramente, utilizado militarmente interno nos Estados Unidos, mas que posteriormente abrangeria para uma disponibilidade aprimorada mundialmente. Assim, foi analisada a influência da pandemia de 2020 para com as relações da humanidade com a internet, e como se tornou mais vulnerável aos crimes cibernéticos.

A segunda seção verifica a descrição dos crimes cibernéticos contra o patrimônio mais atuantes no Brasil, e analisa sua forma de atuação. A atenuando suas disposições no código brasileiro e suas penalidades. Sendo assim, descrevendo tais crimes: Invasão de dispositivo informático (Art. 154-A, CP), Furto mediante fraude eletrônica (Art. 155 §4-B, CP) e Estelionato mediante fraude eletrônica (Art. 171 §2-A, CP).

A terceira seção relaciona uma crítica acerca da atuação do normativo jurídico aos crimes cibernéticos, verificando casos concretos, entendimentos de jurisprudências, e os efeitos atuantes nos dispositivos. Semelhantemente, trazendo uma noção acerca do futuro de tais atuações e suas efetividades.

Os direitos fundamentais e humanos são garantidores que as normas, protegidas pela constituição, garantirão a dignidade de direitos humanos. Portanto, entendedores do direito possuem o dever de fiscalizar e analisar o ordenamento jurídico e seus efeitos objetivados.

1. ANÁLISE INTRODUTÓRIA SOBRE A INTERNET E O CRIME CIBERNÉTICO

1.1. Conceito de internet

Aparentemente um submundo ainda não totalmente explorado, aparentando uma infinitude de informação de dados. A internet é constituída por alguns milhões de computadores interconectados entre si a partir de uma linguagem comum. Permite a interconexão descentralizada de computadores através de um conjunto de protocolos denominado TCP/IP. Melhor dizendo, a internet é o que permite a transferência de dados e informações entre dispositivos em todo o mundo (Tescarollo, 2016).

Complementa Teixeira, que a permissão dessa transição torna a internet como "uma importante ferramenta para a comunicação entre as pessoas físicas ou jurídicas, pois oferece recursos aos seus usuários, como o acesso a informações, a transmissão de dados (via e-mail, por exemplo), a aquisição de produtos ou serviços etc." (Teixeira, 2022, p.44).

Por meio desta surge inúmeras possibilidades e recursos auxiliando o cotidiano dos usuários. Assim, relevante analisar os aspectos de sua criação, bem como sua trajetória até aquela que conhecemos hoje. Não retirando a importância de enfatizar as consequências de seu aceleramento, o qual estimulou a mudança repentina do direito brasileiro em seu âmbito digital.

1.2. A história da internet e seu desenvolvimento no mundo

Conforme Manuel Castells (2003) a internet se originou por meio da "Arpanet", uma rede de computadores criada pela *Advanced Research Projects Agency* (Agência de Projetos de Pesquisa Avançada dos Estados Unidos) - ARPA, um departamento de Defesa dos Estados Unidos com a missão de mobilizar recursos de pesquisa. Com a União Soviética, lançando o primeiro Sputnik em 1957, os Estados Unidos da América tinha como objetivo superar a tecnológica militar durante a guerra fria. Demonstrando uma estratégia dos Estados Unidos de estar à frente da guerra de demonstração de poderes.

A ARPANET facilitou uma comunicação e defesa, privando de possíveis ataques terroristas, usufruída para aqueles que trabalham na unidade da ARPA. Um grande cientista que atuou em conjunto para a criação desse equipamento, chamado "Licklider", descreveu a criação do computador como participante prioritário como parceiro para solucionar eventuais

problemas. Contudo, na década de 60 já havia os primeiros casos de delitos informáticos utilizando computadores, nos Estados Unidos (Rockembach; Pavão, 2024).

Contudo, foi utilizada no meio acadêmico e no científico, o protocolo de utilização passou a ser insuficiente para a comunicação. Por conseguinte, em 1974, foi aberto o ambiente de rede denominado o tão conhecido e utilizado nome “internet”. No final de 1980, a internet, com sua interface baseada em menus dos BBS (*Bulletin Board System*), trouxe de forma simples a utilização com aproximadamente 100 sites, expandindo até então. Historicamente, vários avanços ocorreram em simultâneo (Castells, 2003).

A partir do software Enquire, desenvolvido por Berners Lee, todos os sonhos foram transformados em realidade, pois, foi produzida a *World Wide Web*, a rede mundial. Ele construiu um programa navegador/editor em dezembro de 1990, e chamou esse sistema de hipertexto da “*World Wide Web*”. Introduzindo novas versões do software de navegação web, a Netscape Navigator, posteriormente a Microsoft lançou o Windows 95 com o Internet Explorer, um navegador para web.

A internet surgiu na metade da década de 1990 como um sistema de comunicação flexível e descentralizado. Essa arquitetura aberta proporcionou a cooperação dos usuários. Assim, a flexibilidade e a liberdade foram valores importantes para o desenvolvimento da Internet.

Conforme Carvalho (2007), analisando o contexto histórico da criação da internet considera que “Liberdade, solidariedade e cooperação são concepções que compõem a cultura de cientistas, engenheiros, estudantes de pós-graduação e dos primeiros usuários da rede que participaram conjuntamente da criação da Internet.”. Todos esses fatores conjuntamente avançaram o alcance da novidade tecnológica.

Com o avanço dos computadores e a possibilidade de realizar uma interconexão entre redes, “A partir de então, a Internet cresceu rapidamente como uma rede global de redes de computadores. O que tornou isso possível foi o projeto original da Arpanet, baseado numa arquitetura em múltiplas camadas, descentralizada, e protocolos de comunicação abertos.” (Castells, 2003).

Como relatado por Manuel Castells, não há caminhos a retornar à origem, caso os Estados Unidos não tivessem criado essa comunicação interna, outros países logo momento na história, assim, se direcionaria à modernização da sociedade.

O milênio, em sua concepção de transição, foi marcado e esperado um grande colapso no mundo. Porém, na época percebia um rápido aprimoramento na sociedade, marcada por

duas guerras mundiais (1ª guerra mundial, 1914, 2ª guerra mundial, 1939), as quais obrigaram o impulsionamento da tecnologia, finalizada pela guerra fria (1947).

Diante de tantos projetos e sonhos de pesquisadores para transformar a internet em um ambiente coletivo e mundial, Berners Lee foi um grande realizador deste projeto. A partir do software Enquire, foi produzida a *World Wide Web*, a rede mundial. Construiu um programa navegador/editor em dezembro de 1990, e chamou esse sistema de hipertexto de *World Wide Web*.

Castells (2003), afirma que:

> "Ele definiu e implementou o software que permitia obter e acrescentar informação de e para qualquer computador conectado através da Internet: HTTP, MTML e URI (mais tarde chamado URL)." (Manuel Castells, 2003).

Portanto, foi criado um sistema de comunicação flexível e descentralizado, proporcionando a cooperação dos usuários. Cooperou para cientistas, engenheiros, estudantes de pós-graduação e dos primeiros usuários da rede que participaram conjuntamente da criação da Internet.

Segundo relatos de Manuel Castells (2003):

> Consequentemente, assim que a world wide web se difundiu globalmente, e o acesso à Internet tornou-se relativamente acessível e de fácil operação, as redes comunitárias de computadores se diferenciaram segundo as linhas de seus componentes originais (Manuel Castells, 2003, p. 149).

Afinal, qual era o objetivo da criação da internet?

A resposta contorna dois lados da humanidade na época do acontecimento da guerra fria. Não haveria sucesso no avanço científico contra o oponente sem pesquisa e recursos. Igualmente, não haveria vantagens sobre o oponente sem a segurança da defesa. Os Estados Unidos unificaram suas necessidades com a fundação daquilo que se tornaria a internet.

O sistema de comunicação de computadores permitiu que pesquisas e estudos científicos fossem rapidamente unificados, contribuindo para o avanço da defesa do país. Própria defesa que possibilitou por meio desse sistema, uma segurança e rápida comunicação entre bases militares.

Os maiores beneficiários da criação da internet foram os universitários. A oportunidade de assegurar a interligação entre pesquisas trouxe vantagens irreais para a ciência, o qual também foi utilizada no ambiente militar. Entretanto, verifica-se o evidente verbo que significa a utilização dessa criação hoje, é o verbo "facilitar".

1.3. O desenvolvimento da internet no Brasil

Estava evidente que logo essa nova tecnologia espalharia para o mundo inteiro, tornando claro o que muitos esperavam, sendo o futuro da humanidade envolvendo algo agora concreto e possível.

No Brasil a internet teve seu surgimento no final dos anos 1980, especificamente 1988, por meio da Bitnet, uma rede de universidades ligada à Universidade de Nova York (CUNY) e à Universidade Yale, em Connecticut. Segundo o site Brasil Escola (20–), a rede conectava, por meio de um fio de cobre dentro de um cabo submarino, a Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP), juntamente com a UFRJ (Universidade Federal do Rio de Janeiro) e a LNCC (Laboratório Nacional de Computação Científica) ao Fermilab, laboratório de física especializado no estudo de partículas atômicas, que ficava em Illinois, nos Estados Unidos.

Prossegue o site Brasil Escola (20–), que em 1989, a Rede Nacional de Pesquisas (RNP)foi criada pelo Ministério de Ciência e Tecnologia, uma instituição com objetivos de iniciar e coordenar a disponibilização de serviços de acesso à Internet no Brasil.

A utilização se alarmou a cada ano que passava. Esse processo histórico revolucionou o trabalho e a praticidade das pessoas. Contudo, o processo de democratização da internet foi demorado, pois, observava uma exclusividade com o direito ao acesso apenas para universidades, lugares os quais possuíam recursos para tal feito.

Mesmo com tantos impedimentos não havia negação de que a utilização da internet juntamente com a disponibilização da banda larga iria ampliar a democratização da tecnologia. Assim, a internet se popularizou permitindo uma ampla conexão. Contudo, há mudanças no mundo que possibilitam uma alteração significativa no comportamento de uma sociedade.

No final do ano de 2019 todo o mundo estava aguardando e se preparando para a chegada do vírus COVID-19 em seus países. Conforme o Ministério da saúde do Brasil, o Coronavírus, tal doença é transmitida por contato, gotículas ou aerossóis. Por conseguinte, em 11 de maio de 2020, houve a publicação da Recomendação N°036 do Conselho Nacional de Saúde recomendava a implementação de medidas de distanciamento social mais restritivo (lockdown) devido ao aumento de ocupação de vagas nos hospitais, de casos e de mortes. O isolamento transparece inúmeros conflitos, requerendo mais sobre a inovação tecnológica e a adaptação do direito brasileiro (Brasil, 2021).

Alguns trabalhos, as escolas e faculdades se adaptaram tecnologicamente para que não houvesse perdas e danos gravosos nos ambientes de trabalho e estudo. Contudo, com a escassez de interação social, as pessoas passaram a utilizar a tecnologia como forma de entretenimento, trabalho, estudo, durante o período. Também, ocorreu a realização de atividades comuns do dia a dia, como pedir comida, fazer compras, fazer transferências, onde todas as ações que deveriam ser feitas em instituições bancárias de forma presencial, naquele momento de isolamento foram feitas com apenas cliques.

Esse impulsionamento tecnológico devido às necessidades requeridas pela sociedade foi importante para evoluir a utilização da tecnologia e incentivar uma evolução que naquele momento deveria estar avançada. A internet possibilita uma interligação como uma única comunidade global. Agora, conseguimos nos conectar com quem nunca conseguiríamos ver pessoalmente (Pinheiro, 2021).

Observando a soma entre pessoas isoladas em suas casas, o aumento na utilização da tecnologia, a igualdade desses fatores resulta na criminalidade se evoluindo e se adaptando.

Após a pandemia, observou-se um aumento expressivo na incidência de golpes digitais em escala global. Os criminosos exploram novas oportunidades para cometer fraudes. O aumento no período de utilização de forma on-line possibilitou em alvos vulneráveis para golpes cibernéticos, como phishing, ransomware e fraudes online.

É de suma relevância a atuação do direito brasileiro, perante a rápida inovação tecnológica. Mesmo durante a pandemia do Coronavírus foi preciso analisar e rever os dispositivos, principalmente penais, para estarem alcançando todos os cidadãos brasileiros.

1.4. Aspectos gerais do crime cibernético

Diante da mudança social, um termo se popularizou e significou o tipo criminal que ocorre de forma recorrente hoje em dia. O termo “cibercrime” nada mais é que todo ato em que o computador ou meios de tecnologia de informação serve para atingir um ato criminoso ou em que o computador ou meios de tecnologia de informação é objeto de um crime.

Segundo Tarcísio Teixeira (2022), entre as diversas nomenclaturas doutrinárias, está o denominado “crime de informática”, que envolve: crime de computador, crime via internet, crime informático, crime praticado por meio da internet, crime praticado “por meio da informática, crime tecnológico, crime da internet, crime digital, *cybercrimes, infocrimes*, etc.”

O conceito de crime de informática engloba todo o sistema de informática, sendo a internet e sua utilização como meio de execução, sendo acessórios e perpetrados.

Observando uma sociedade conectada, há a preocupação em relação à violação de dados e informações. Para Rossini:

> O conceito de "delito informático" poderia ser talhado como aquela conduta típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, praticada por pessoa física ou jurídica, com o uso da informática, em ambiente de rede ou fora dele, e que ofenda, direta ou indiretamente, a segurança Informática, que tem por elementos a integridade, disponibilidade a confidencialidade (Rossini, 2004, p. 110.)

De acordo com Rossini, o delito virtual se interliga com o delito praticado da forma tradicional, a qual tem base em uma conduta ou prática ilícita e típica. Destaca-se que o cibercrime poderá ocorrer tanto online quanto offline. Offline, pois, há a possibilidade de transição de arquivos entre dois dispositivos sem conexão com a internet, ou utilizar mensagens de texto, ou ligações como meio de execução.

Após o crescimento das telecomunicações e informática na década de 1970, a sociedade apresentou novas condições para o processamento de informação. Assim, evidenciou a formalização da sociedade da informação e promoveu a inovação tecnológica. Foi por meio da modernização dessa sociedade, que o mundo atualmente enfrenta uma alta nos índices de vítimas de delitos virtuais (Lisboa, 2006).

O crime cibernético é cometido principalmente por hackers ou por indivíduos com amplo conhecimento em informática, que invadem ou prejudicam sistemas. Portanto, são agentes capazes de se adaptar à evolução tecnológica e desenvolver métodos de ataque. Os crimes cibernéticos têm como principal objetivo impactar computadores, dados ou sistemas informáticos.

Há uma diferenciação entre os crimes de informática e os crimes cibernéticos. O primeiro são todas as ações típicas, antijurídicas e culpáveis praticadas com a utilização de computadores e/ou de outros recursos da informática. Já o segundo, são aqueles cometidos utilizando a Internet. Desse modo, pode-se interpretar como o crime cibernético sendo uma espécie do crime de informática, uma vez que se utiliza de computadores para acessar a Internet (Costa; Silva, 2022).

O objetivo central do invasor é prejudicar o sistema informático da vítima, com o objetivo de afetar o dispositivo, colher informações ou dados, ou obter vantagem ilícita. No momento em que afeta o direito alheio foi preciso a ação da legislação penal para o devido combate à nova modalidade de crime.

Os crimes virtuais podem ser divididos em próprios ou puros, e impróprios ou impuros. Os crimes virtuais próprios são aqueles em que o agente precisa de um sistema informático para cometer a ação criminosa, utilizando o computador como meio para executar o crime.

Damásio (2003) afirma que crimes virtuais próprios “são aqueles em que o bem jurídico protegido pela norma penal é a inviolabilidade das informações automatizadas (dados)”. Melhor dizendo, está relacionado não somente com os dados em si, mas também suas finalidades. Ou seja, verifica-se a intenção da utilização desses dados (Viana, 2003 apud Carneiro, 2012).

Os crimes virtuais denominados impróprios são aqueles realizados com a utilização do computador, como instrumento para realização de condutas ilícitas. Agora utiliza-se o sistema de informática como meio para a realização do crime.

A diferença se dará que para a concretização do ato ilícito pode ser de outras formas e não necessariamente pela informática para chegar ao fim desejado como exemplo, o crime pedofilia.

Do mesmo modo afirma o jurista Damásio, que os crimes impróprios “(...) são aqueles em que o agente se vale do computador como meio para produzir resultado naturalístico, que ofenda o mundo físico ou o espaço "real", ameaçando ou lesando outros bens, não computacionais ou diversos da informática.” (Damásio, 2003 apud Carneiro, 2012).

Portanto, Alguns dos crimes mais comuns são: crimes de ódio, crimes contra honra, pedofilia, entre outros. A seguir, analisaremos em ênfase os principais crimes contra o patrimônio.

2. CRIMES CONTRA O PATRIMÔNIO NA INTERNET

Considerando o avanço da internet e sua evidente dependência na atualidade, paralelamente nota-se o crescimento dos crimes virtuais, in casu, crimes contra o patrimônio. A especificidade de condutas contribui para o combate aos delitos. A aplicação do princípio da taxatividade efetiva o acompanhamento com a sociedade.

De acordo com o entendimento de Fernando Capez, para ele o princípio da taxatividade envolve uma lei penal precisa e em perfeita correspondência. Assim, acrescenta o autor:

> A lei penal delimita uma conduta lesiva, apta a pôr em perigo um bem jurídico relevante, e prescreve-lhe uma consequência punitiva. Ao fazê-lo, não permite que o tratamento punitivo cominado possa ser estendido a uma conduta que se mostre aproximada ou assemelhada (CAPEZ, 2024, p. 43)

Portanto, analisa-se a busca do direito brasileito para aplicar esse princípio. Exemplificando, as alterações tragas pelas leis n° 12.737/2012 e n° 14.155/2021. Dessarte proporcionaram esperança de especificidade de dispositivos penais, para atuar positivamente frente a alta demanda.

2.1. Art. 154-A - Invasão de dispositivo informático

O crime de invasão de dispositivo informático, disposto no Art. 154-A, foi implementado pela lei n° 12.737/2012 conhecida como Lei Carolina Dieckmann. Essa foi a primeira lei criada para o combate de crimes ocorridos no meio virtual. Diante de um contexto histórico, no ano de 2012, a atriz Carolina Dieckmann teve seu computador pessoal invadido por hackers e suas fotos pessoais foram divulgadas (Brasil, 2012).

A repercussão do caso incentivou a criação de projetos de lei, sendo eles Projetos de Lei n. 35/2012 - originado pelo projeto n° 2.793/2011, com a proposta da l737ei modificativa Lei azevedo (projeto de lei n° 94/99) - o qual tornou-se a Lei n° 12.737/2012.

A urgência para com a criação dessa lei, tipificando novos delitos, foi com o objetivo de persuadir os hackers para serem dissuadidos de suas atividades, garantindo uma diminuição nessas ações criminais. No entanto, a urgência parece negligenciar certos aspectos técnicos cruciais para a configuração de crime, bem como a especificidade da ação penal.

A referida lei trouxe tipificações sobre os delitos normativos, sendo os principais presentes no código penal, o art 154-A do Código Penal Brasileiro.

Presente no Art. 154-A do código penal dispõe:

> 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. (Incluído pela Lei nº 12.737, de 2012)
> § 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)
> 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)
> § 5o Aumenta-se a pena de um terço à metade se o crime for praticado contra: (Incluído pela Lei nº 12.737, de 2012)
> I - Presidente da República, governadores e prefeitos; (Incluído pela Lei nº 12.737, de 2012)
> II - Presidente do Supremo Tribunal Federal; (Incluído pela Lei nº 12.737, de 2012)
> 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)
> IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal. (Incluído pela Lei nº 12.737, de 2012) (Brasil, 1940).

O Art. 154-A tipifica a conduta de invadir o dispositivo móvel violando o mecanismo de segurança, assim, remetendo a instalações de vírus com o objetivo de obter, adulterar ou destruir dados alheios, sem autorização.

2.1.1. Classificação doutrinária

O crime disposto trata-se de crime comum, sendo aquele que não exige nenhuma qualidade específica do sujeito ativo para sua prática, ou seja, pode ser praticado por qualquer pessoa. Também considerado plurissubsistente, é aquele cuja prática exige mais de uma conduta para sua configuração. Em outras palavras, a conduta do agente pode ser fracionada, possibilitando a interrupção da execução.

É uma conduta comissiva, pois há uma ação direta do agente: "invadir, instalar". De forma vinculada, tendo modos específicos para a execução descritas no tipo penal ou de forma, onde não prevê uma forma específica.

Aplicado a classificação de crime formal, que se consuma sem a produção do resultado naturalístico, embora ele possa ocorrer. Desse modo, instantâneo, onde a consumação não se prolonga no tempo.

Por fim, monossubjetivo podendo ser praticado por um único agente. E, simplesmente atingindo um único bem jurídico, a inviolabilidade da intimidade e da vida privada da vítima (Maggio, 2013).

Há uma especificidade sobre a caracterização de ação pública no delito em questão. Assim considera Maggio,

> A ação penal, em regra, é condicionada à 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, hipóteses em que a ação será pública incondicionada (CP, art. 154-B) (Maggio, 2013).

O bem jurídico do crime de invasão de dispositivo informático é a inviolabilidade da intimidade e da vida privada.

Entende-se um diferente conceito, pois, a inviolabilidade da intimidade concentra-se no direito do indivíduo ter a oportunidade de manter a sua vida privada, sendo respeitada e protegida. Já a vida privada contorna o repositório de segredos e particularidades do âmbito íntimo (Taballi, 2016).

Trata-se de um direito fundamental constitucionalmente assegurado. Presente no artigo 5°, inciso X da Constituição Federal, nestes termos:

> Art. 5° são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurando o direito de indenização pelo dano material ou moral decorrente de sua violação.
> (...)
> 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).

Os termos obter, adulterar ou destruir dados ou informações significam tudo aquilo que é considerado íntimo e privado da vítima. Assim, arquivos situados no dispositivo.

O sujeito ativo da ação poderá ser qualquer pessoa, consoante a classificação de crime comum. Por ser um crime de alta complexidade, popularmente, são os chamados “hackers”, que realizam este tipo de ação.

Sujeito passivo é a pessoa que pode sofrer dano decorrente da ação de invasão indevida em seu dispositivo informático, com a ação de obter, adulterar ou destruir dados e informações, ou proceder à instalação de vulnerabilidades para obter vantagem ilícita, seja para si ou para outrem.

O núcleo do tipo penal está representado pelos verbos invadir e instalar, tendo como objeto material os dados e informações armazenadas, bem como o próprio dispositivo informático da vítima que sofre a invasão ou a instalação de vulnerabilidades.

De acordo com Maggio (2024), o tipo penal “trata-se de tipo misto alternativo, onde o agente responde por crime único se, no mesmo contexto fático, praticar uma das duas condutas típicas (invadir e instalar).”. O cerne do crime é delineado pelos atos de invadir e

instalar, visando os dados e informações guardadas, assim como o próprio dispositivo informático da vítima, sujeito à invasão ou à inserção de vulnerabilidades.

Na primeira conduta, invadir dispositivo informático o crime é de forma vinculada, de acordo com Damásio (1997):

> Os crimes de forma livre são os que podem ser cometidos por meio de qualquer comportamento que cause um determinado resultado. Os crimes de forma vinculada são aqueles em que a lei descreve a atividade de modo particularizado (Jesus, 1997).

Desse modo, somente pode ser praticado mediante violação indevida de mecanismo de segurança.

Na segunda conduta (instalar) vulnerabilidades o crime é de forma livre, sendo cometido por qualquer meio de execução. Ao fato de que a proteção postergada no delito é dos dados e das informações dele retirados, interpreta-se que a conduta tipificada para instalar, não necessariamente ocorrerá no próprio dispositivo informático. Atualmente há formas tecnológicas que o meio será totalmente digital. Portanto, caso haja a instalação, com a intenção de obter a vantagem ilícita configura o crime disposto (Maggio, 2013).

O elemento tipificado na conduta é o dolo, consistente na vontade livre e consciente de invadir dispositivo informático alheio, mediante violação indevida de mecanismo de segurança ou de instalar no mesmo vulnerabilidades, tornando-o desprotegido, facilmente sujeito a violações (Maggio, 2013).

Exigem-se, ainda, os elementos subjetivos específicos. Como, por exemplo a especificidade da intenção do agente, o qual necessita de uma vontade especial, que segundo Pablos (2010), “pode ser expressa (CP, art. 158[10], v.g) ou implícita (crimes contra a honra)” (Oliveira 2014, apud, Pablos, 2010).

No delito em questão pode ser atribuída pelas expressões "com o fim de obter, adulterar ou destruir dados ou informações" e "para obter vantagem ilícita". Portanto, conclui-se que esse elemento subjetivo específico precisa ser executado na ação, não havendo, não configurará o delito, ou seja, torna o fato atípico. Consequentemente, o tipo penal não admite a modalidade culposa (Maggio, 2013).

Sendo caracterizado como crime formal, que se consuma sem a produção do resultado naturalístico, na invasão de dispositivo informático, a obtenção, adulteração ou destruição de dados ou informações da vítima, constitui no simples exaurimento do crime.

Analisando o Art. 154-A da lei n° 12.737/2012 verifica-se o artigo fonte para a conduta, sendo “invadir”, o verbo propõe uma conduta dolosa. A consumação ocorre com a

imediata invasão do dispositivo eletrônico, mesmo que tenha ou não coletado informações de dados. Trata-se de crime instantâneo (Azevedo, 2017).

Já a tentativa é possível por ser considerado crime plurissubsistente.(Maggio, 2013)

Incorrerá na mesma pena logo no §1 do mesmo artigo a produção, oferecimento, distribuição, venda ou difusão dispositivo ou programa de computador com o intuito de permitir a prática da conduta. Percebe-se que independe do conteúdo coletado, salvo especificidades em lei.

Tal figura típica equipara-se ao delito com a ação voltada para o objeto dispositivo ou programa de computador com o intuito de permitir a invasão de dispositivo informático alheio e praticar as mesmas condutas. Mas, apresentando novos verbos: produzir (fabricar, originar, fazer aparecer), oferecer (expor, exibir ou propor para que seja aceito), distribuir (dar, entregar, transmitir), vender (alienar, dispor ou ceder por certo preço) e difundir (transmitir, espalhar, propagar).

2.1.2. Figuras qualificadas e aumento de pena

O § 3º, do Art. 154-A, do Código Penal, define o crime de invasão de dispositivo informático qualificado.

Assim, ao contrário da figura simples ou equiparada tem pena de detenção, de três meses a um ano, e multa, as figuras qualificadas em razão das circunstâncias específicas têm pena de reclusão, de seis meses a dois anos, e multa.

“Se da invasão resultar a obtenção de conteúdo de comunicações”, as comunicações envolvem todos os meios que se pode enviar ou receber mensagens de texto, imagens, vídeos e clipes de áudio, etc.

Ao citar “privadas, segredos comerciais ou industriais, informações sigilosas”, assim, uma tipificação envolvendo a segurança digital para instituições. Assim, prosseguindo “ou se da invasão resultar o controle remoto não autorizado do dispositivo”, com a evolução tecnológica, não é preciso o controle do dispositivo direto no mesmo, mas sim à longa distância, sendo feita por outro computador ou celular.

A invasão de dispositivos se tornou o meio mais comum para as práticas dos crimes cibernéticos. A exemplo, a lei 12.737/2012, inicialmente aborda o delito de invadir, contudo há o resultado de prejuízo econômico disposto no art 154-A §2 Aumentando-se a pena de 1/3 (um terço) a 2/3 (dois terços).

O Art. 154-A §4 descreve uma condição legal em que, caso haja divulgação, comercialização ou transmissão a terceiros dos dados ou informações obtidos de maneira ilegal, a pena é aumentada de um a dois terços.

Já o §5 aborda um aumento de pena de um terço até a metade atribuída a cargos importantes, sendo eles: I - Presidente da República, governadores e prefeitos; Presidente do Supremo Tribunal Federal; Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal (Brasil, 1940).

A lei "Carolina Dieckmann" trouxe disposições interessantes no âmbito dos crimes digitais, pois há a necessidade de segurança privada dos dados e dispositivos. Contudo, alguns doutrinadores analisam que o texto torna-se vago, e desnecessariamente repetitivo.

Todavia, o ilustre prof. Dr. Rogério Greco, entende:

> Não é incomum que pessoas evitem colocar senhas de acesso, por exemplo, em seu computadores, permitindo, assim, que qualquer pessoa que a eles tenha acesso, possam conhecer o seu conteúdo. No entanto, mesmo sem a existência de senha de acesso, a ninguém é dado invadir computador alheio, a não ser que ocorra a permissão expressa ou tácita de seu proprietário. No entanto, para fins de configuração típica, tendo em vista a exigência contida no tipo penal em análise, somente haverá a infração penal se houver, por parte do agente invasor, uma violação indevida do mecanismo de segurança. (Greco, 2013)

Logo, a expressão "sem autorização" presente no caput do Art 154-A, não necessariamente corresponde a um pleonasmo no texto, mas sim uma segurança extra para que não ocorra interpretações em casos específicos de forma errada. Havendo a autorização, a conduta se tornará fato atípico (Greco, 2013).

2.2. Art. 155 §4-B, CP - Furto mediante fraude eletrônica

O crime de furto mediante fraude, disposto no Art. 155 §4-B, CP, onde foi implementado pela lei n° 14.155/2021 conhecida como Pacote Anti-crime. A lei buscou aperfeiçoar alguns dispositivos presentes no código penal e no processo penal.

O pacote Anticrime foi bastante debatido e gerou opiniões divergentes. Alguns debutantes enxergavam essa lei como uma medida necessária para o combate à criminalidade. O fato de que a sociedade evolui o direito brasileiro deve evoluir conjuntamente. Outros críticos argumentam que poderiam violar direitos fundamentais e não resolveriam os

problemas estruturais do sistema de justiça criminal brasileiro. Contudo, foi aprovado e sancionado em dezembro de 2019.

A referida lei trouxe a inclusão de uma nova tipificação penal, o Art. 155 §4-B do Código Penal Brasileiro.

Presente no Art. 155 §4-B do código penal dispõe:

> Furto
> Art. 155 - Subtrair, para si ou para outrem, coisa alheia móvel:
> Pena - reclusão, de um a quatro anos, e multa.
> § 1º - A pena aumenta-se de um terço, se o crime é praticado durante o repouso noturno.
> § 2º - Se o criminoso é primário, e é de pequeno valor a coisa furtada, o juiz pode substituir a pena de reclusão pela de detenção, diminuí-la de um a dois terços, ou aplicar somente a pena de multa.
> § 3º - Equipara-se à coisa móvel a energia elétrica ou qualquer outra que tenha valor econômico.
> 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) (Brasil, 1940)

O Art. 155 §4-B, CP tipifica a conduta de praticar o furto mediante fraude. Mas, a fraude é cometida por meio de dispositivo eletrônico ou informático, que poderá estar conectado ou não à internet, pode ou não violar o mecanismo de segurança ou utilizar vírus maliciosos ou outros meios análogos.

Conforme Greco (2023), o meio utilizado “dispositivo eletrônico” conceitua-se como todo aquele aparelho capaz de receber e armazenar dados e informações, tratá-los, bem como transmitir os resultados, a exemplo do que ocorre com os computadores, smartphones, tablets etc.”

De forma esclarecedora no momento em que o legislador relata “conectado ou não à internet”, referência a possibilidade de haver a atuação de um conjunto de dois ou mais computadores autônomos e outros dispositivos. Assim, estando interligados com a finalidade de compartilhar informações, por exemplo, dados, impressoras, mensagens, bluetooth, cabos que interligam dispositivos, atualmente a transição de informação por meio de *QR Code*. Logo, há variações para a prática penal, importante detalhe evidenciado pelos legisladores (Greco, 2023).

Por mecanismos de segurança está relacionado com meios que asseguram que somente o proprietário daquele dispositivo terá acesso, por exemplo, senhas, modos de autenticação. Há a presença de programa malicioso (popularmente conhecido como vírus) ou qualquer

outro meio análogo, não implicando brechas na lei, restando somente a interpretação por meio do poder judiciário para considerar os outros meios fraudulentos análogos.

Caso o objetivo seja induzir a vítima a se distrair para facilitar a subtração, aplica-se ao delito. O presente trata-se de um meio de execução do cometimento de fraude, situado no Art. 155 §4º, II.

2.2.1. Classificação doutrinária

O crime possui algumas classificações específicas criminais. Trata-se de crime comum, onde não há exigência a quem praticar o furto. Também considerado unissubsistente, onde apenas a ação de "subtrair" relaciona-se com a prática exigida. Portanto, igualmente, comissivo devendo o agente "subtrair" o bem de forma direita.

Desse modo, instantâneo, no momento em que o agente toma posse do objeto. No delito em questão, considera-se monossubjetivo podendo ser praticado por um único agente.

Analisa-se que o furto é caracterizado como ação pública incondicionada. Tendo como o bem jurídico tutelado sendo o patrimônio, sob forma específica inclui a posse e a propriedade. No furto mediante fraude eletrônica o núcleo do tipo penal é a subtração, ou seja, pegar escondido sem o consentimento da vítima (Barbagalo, 2022).

O bem jurídico do crime de furto mediante fraude eletrônica é o patrimônio, mas especificamente a propriedade do objeto, no caso as informações, dados, capazes de afetar o patrimônio da vítima (Greco, 2023).

A pessoa que comete a ação também será considerada o sujeito ativo, dependendo da classificação do crime comum.

O crime somente pode ser praticado dolosamente, o delito necessita da finalidade de ter a coisa alheia móvel para si ou para outrem, tendo também a presença do animus furandi (intenção de furtar) na ação. A conduta prevista no tipo é de natureza comissiva. Entretanto, poderá o delito de furto ser praticado por omissão, desde que o agente goze do status de garantidor.

O status de garantidor está relacionado com o crime omissivo impróprio (comissivo por omissão), consiste na omissão ou não execução de uma atividade predeterminada e juridicamente exigida do agente, é o resultado que poderia ser evitado.

Consoante a consumação do crime há várias teorias as quais analisa-se o crime de furto no código penal brasileiro.

A teoria do *contrectatio* entende que se consuma o furto quando é retirada da esfera de posse e disponibilidade da vítima, ingressando, consequentemente, na do agente. Na segunda corrente, descreve que na troca de posse, sendo tranquila, é obrigatório exercer, por curto espaço de tempo. Esta última, possuindo vários entendimentos no tribunais. Assim, não tendo tempo suficiente para dispor da coisa, estaria aplicada a tentativa (Greco, 2023).

2.2.2. Causas de aumento de pena

O § 4º-C também foi inserido ao Art. 155 do Código Penal por meio da Lei nº 14.155, de 27 de maio 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).

O referido do § 4º-B do Art. 155 do Código Penal, assevera que 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.

Assim, consoante a dificuldade de estipular uma investigação fora do país, a referida pena de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, será aumentada de 1/3 (um terço) a 2/3 (dois terços), se o crime for praticado mediante a utilização de servidor mantido fora do território nacional (Greco, 2023).

Posteriormente, se o crime for praticado contra pessoa idosa ou vulnerável, haverá um aumento de 1/3 (um terço) ao dobro. Segundo o Art. 1º da Lei nº 10.741/2003, uma pessoa é considerada idosa quando tiver idade igual ou superior a 60 (sessenta) anos. É considerada vulnerável, os elencados pelo Art. 217-A do diploma repressivo, sendo o menor de 14 (quatorze) anos, vulnerável por enfermidade ou deficiência mental, ou seja, aquele que não têm o necessário discernimento para a prática do ato (Greco, 2023).

A falta de conhecimento e o constante surgimento de inovações dificultam a exclusão de classes sociais de determinadas oportunidades educacionais. Isso também afeta pessoas em

situação de vulnerabilidade, que podem se tornar alvos de golpistas, como idosos, pessoas com deficiência intelectual, analfabetos e outros grupos vulneráveis.

Como forma exemplificativa, segundo o site de notícias G1, sob informação do Disque 100 do governo federal, houve um aumento significativo nas denúncias de crimes financeiros contra idosos. Portanto, foi analisado esse fator nos primeiros cinco meses de 2023 em comparação com o mesmo período de 2022, o qual destaca-se a maior vulnerabilidade dos idosos diante dos avanços tecnológicos.

Dessa forma, analisa-se que não somente idosos tornaram-se alvos dos golpistas, mas também pessoas com deficiência. Assim, no momento em que desenvolvem iscas voltadas para benefícios sociais, indenizações, supostas facilidades, entre outros. Os indivíduos por trás das propostas irresistíveis conseguem organizar nichos específicos e buscar meios para garantir o interesse desses grupos específicos.

Assim, de forma exemplificativa, uma notícia publicada pelo Correio Braziliense destaca uma quadrilha especializada em aplicar golpes em idosos e pessoas com deficiência foi alvo de uma operação desencadeada pela 18ª Delegacia de Polícia (Brazlândia). Primeiramente, obtém a confiança das vítimas, logo, enviam links para cadastro onde garantam seus dados. Utilizavam os dados para acesso às contas bancárias realizando empréstimos, comprometendo as futuras condições financeiras e benefícios, como comprometer o recebimento da aposentadoria.

2.3. Art. 171 §2-A - Fraude eletrônica

2.3.1. A estrutura jurídica do crime de estelionato

O delito de estelionato mediante fraude eletrônica, disposto no art. 171 §2-A, CP, semelhante, foi implementado pela lei n° 14.155/2021 conhecida como Pacote Anti-crime. No âmbito jurídico o estelionato, de acordo com Greco (2023), é regido pelo binômio vantagem ilícita/prejuízo alheio.

O mesmo dispõe o conceito da seguinte forma:

> Ilícita é a vantagem que não encontra amparo no ordenamento jurídico, sendo, na verdade, contrária a ele. Se a vantagem perseguida pelo agente fosse ilícita, o fato poderia ser desclassificado para outra infração penal.A doutrina majoritária posiciona-se no sentido de que a expressão vantagem ilícita abrange qualquer tipo de vantagem, tenha ou não natureza económica.A utilização da fraude pelo agente visa a induzir ou a manter a vítima em erro. Erro significa a concepção equivocada da

> realidade, é um conhecimento falso do que ocorre no mundo real.Qualquer meio fraudulento utilizado pelo agente, seja mediante dissimulações, seja até mesmo uma reticencia maliciosa, que faça a vitima incorrer em erro, já será suficiente para o raciocinio relativo ao delito de estelionato (GRECO, 2023, P. 356).

Na linguagem jurídica em um contexto histórico, desde o direito romano até o código penal republicano resume-se em usar artifícios para surpreender a boa-fé, ou seja, a fraude. Essa que induz a vítima ao erro, com a finalidade obter vantagem patrimonial (Bittencourt, 2024).

O bem jurídico protegido como os demais delitos expostos é a inviolabilidade do patrimônio, mas especificamente voltada para a ação praticada mediante fraude eletrônica. A ação tipificada é obter vantagem ilícita (para si ou para outrem), em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil ou qualquer outro meio fraudulento (Bittencourt, 2024).

O crime de estelionato possui como elemento subjetivo o dolo, não possuindo a modalidade culposa. Cuida-se do *animus rem sibi habendi* ou *do animus lucri faciendi* (Estefam, 2024).

Complementa o ilustre Dr. prof. Bitencourt (2024):

> O dolo, na primeira figura, "induzir em erro", deve anteceder o emprego do meio fraudulento e a produção dos resultados "vantagem ilícita" e "prejuízo alheio". Na segunda figura, "manter em erro", o dolo é concomitante ao referido erro: constatada a existência do erro, o dolo consiste exatamente em sua manutenção (Bitencourt, 2023, p. 163).

Sujeito ativo do crime de estelionato pode ser qualquer pessoa, sem qualquer condição especial (crime comum). O concurso eventual de pessoas, na forma de coautoria e participação. Destacado pelo legislador "para si ou para outrem", essa poderá se enquadrar em coautor ou partícipe do crime, sendo alcançada pelo concurso de pessoas (Art. 29 do CP). Mas, também poderá ser um terceiro não consciente do delito ocorrido, não se enquadrando no concurso de pessoas (Estefam, 2024).

O sujeito passivo é aquele que teve o seu patrimônio lesado, sendo induzido ao erro do sujeito ativo, que pode não ser a mesma pessoa. É preciso que seja "pessoa(s) determinada(s)". Tratando-se de pessoas indeterminadas, pode configurar-se crime contra a economia popular ou contra as relações de consumo, sendo um crime comum, material, doloso, instantâneo, de forma livre, comissivo, de dano, unissubjetivo, plurissubsistente (Bittencourt, 2024).

A consumação ocorre no momento e no lugar da ação de obter o proveito econômico que causou o prejuízo alheio. Não basta a existência do erro mediante fraude, mas necessita da vantagem indevida (Bittencourt, 2024).

Tratando-se de crime material, que é uma ação que depende de fracionamento, é admissível a tentativa. Para sua consumação depende da ocorrência do resultado naturalístico, ou seja, da obtenção da vantagem ilícita e do efetivo prejuízo alheio. Neste delito requer a cooperação da vítima, para a efetividade do delito. Há hipóteses para a configuração da tentativa. A primeira o agente não consegue enganar a vítima. A segunda hipótese é que o agente não consegue obter vantagem ilícita. Na última hipótese o ofendido não tem prejuízo sofrido (Estefam, 2024).

A pena do estelionato será de quatro a oito anos de reclusão, 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 (Facebook, Instagram, Twitter, TikTok), contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo.

Dispõe no Art. 171 §2-A do código penal o delito fraude eletrônica:

> 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 1 (um) a 5 (cinco) anos, e multa.
> (...)
> § 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.
> Lei 14.155, de 27/05/2021, art. 1º (acrescenta o § 2º-A).
> § 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).

A figura qualificadora foi inserida no código penal pela Lei n. 14.155 de 2021. Ela apresenta uma nova modalidade de estelionato, muito comum nos últimos anos, mais especificamente cresceu durante a pandemia de Covid-19.

A verdadeira vítima é aquela que, devido às informações obtidas pelo agente fraudulento, é levada ao erro, permitindo que o agente obtenha uma vantagem ilegal à sua custa. O agente ludibria a vítima induzindo-a a cair em armadilhas a levanto ao erro. Por exemplo, quem possui a conta do aplicativo “WhatsApp” clonada, não é vítima desse delito.

Quem é considerado vítima são as pessoas em que os autores contataram se passando pelo perfil clonado, induzindo-as a pedidos envolvendo prejuízos econômicos (Estefam, 2024).

O Art. 171 §2-B implica que a fraude eletrônica realizada usando um servidor localizado fora do país, a pena será aumentada de um a dois terços. Porque, o agente pode realizar essa ação com servidores mantidos em território estrangeiro com o objetivo de ocultar sua localização e dificultar sua identificação.

Tal conduta tende a complicar as investigações, já que o servidor pode estar sujeito à jurisdição de um país diferente, e, pode não acatar as ordens emitidas pela justiça brasileira (Estefam, 2024).

2.3.2. Diferença entre furto mediante fraude eletrônica e estelionato eletrônico

Apesar dos dois delitos envolverem fraude eletrônica, o furto mediante fraude, o meio fraudulento é utilizado como meio para facilitar a consumação do furto, ou seja, a fraude é a distração da vítima para a facilitação. A vítima não tem vontade e nem entrega o bem de forma espontânea.

De modo exemplificativo, Tavares (2021) relata que no momento em que a vítima é enganada por sujeitos com falsos uniformes da empresa de telefone/internet, permitindo a entrada deles, enquanto um distrai a vítima, os outros subtraem bens do imóvel, pode se enquadrar no delito.

Tavares (2021) relata que no crime de Estelionato, a vítima é iludida pelo agente pela fraude praticada, onde ela entrega o objeto de livre e espontânea vontade. Assim, a vontade provém de ambos os lados, o que resulta no devido fracionamento da ação, presente a vantagem ilícita e o prejuízo alheio. Por exemplo, sites de compras falsificados, com o objetivo de obter dados de cartões financeiros.

3. DIFICULDADES E PERSPECTIVAS DA APLICAÇÃO DOS NOVOS DELITOS PENAIS

3.1. Dificuldades na fase investigativa dos delitos cibernéticos

Para o direito processual penal, a prova é o momento mais importante para o convencimento do juiz. Não bastam as alegações das partes do processo, é preciso a comprovação da materialidade criminal. Sendo assim, a fase instrutória é o momento cabível.

Segundo a Dra. Jardene Braz (2022), é “o momento processual onde as partes poderão produzir provas para demonstrar a veracidade das alegações, é o momento que a parte tem para provar sua razão acerca dos fatos”.

Como qualquer outro crime, os delitos cibernéticos necessitam de uma maior capacidade na fase investigatória. Quem possui esse poder é a polícia judiciária, logo, capacitada para buscar a materialidade do crime. Contudo, há circunstâncias que atrapalham uma verdadeira prova concreta do crime digital.

Atualmente, a dificuldade probatória gira em torno de buscar evidências que comprovem a atividade criminosa. Dentre os inúmeros meios de prova, a perícia é a mais utilizada, pois analisa o ato criminoso e o autor do crime.

O maior obstáculo é o anonimato, pois, a facilidade de criar outras identidades ou perfis atrapalham a encontrar o verdadeiro agente de determinado delito. Nos crimes digitais contra o patrimônio é comum a utilização de inteligência artificial, como, por exemplo, criar rostos para colocar nas fotos de perfis, vozes automáticas de ligações, o envio de mensagens e códigos automáticos nos e-mails e mensagens de celular, entre outras inúmeras possibilidades (Dorigon; Soares, 2018).

Uma utilização comum são os servidores “proxies”. Para Dorigon e Soares (2018), no artigo científico - Crimes cibernéticos: dificuldades investigativas na obtenção de indícios da autoria e prova da materialidade, publicado em 2018, dispõem o contexto desses servidores, relatando o seguinte:

> Os proxies são servidores que agem como um intermediário para requisições de seus clientes, solicitando recursos ou serviços de outros servidores, ou seja, agem como uma ponte entre o usuário e o conteúdo acessado por este na internet. Deste modo, constará que o endereço IP do servidor proxy foi o que acessou aquele conteúdo disponibilizado na internet e não o do usuário que o efetivamente acessou (Dorigon, Soares, 2018).

O também chamado proxy anônimo aprimora o acesso à internet favorecendo o usuário, ao proteger as suas informações pessoais ocultando o endereço IP que o identificaria, assim previne que haja a publicidade das informações, mas também favorece para livrar-se de eventuais investigações.

A perícia do delito virtual funciona da seguinte forma: o perito nomeado técnico em informática irá acessar um dispositivo eletrônico e verificará os eventuais vestígios do delito. Por conseguinte, poderá contribuir para uma eventual prova no processo, até mesmo identificar a localidade, ou podendo chegar aos dados de fato do agente do crime.

Em um roteiro de atuação sobre os crimes cibernéticos, o Ministério Público Federal (2016) dispõe de recomendações e procedimentos de coleta dessas provas. Assim, deve-se atentar às seguintes características: Admissível, Autêntica, Completa, Confiável e Convincente (MPF, 2016).

Logo mais, o MPF dispõem o seguinte acerca dos vestígios digitais:

> No contexto da investigação de crimes computacionais, onde notadamente o objeto sensível é quase sempre representado pelo intangível, têm-se que o vestígio é majoritariamente apresentado como um registro digital que existe em decorrência de uma prévia intervenção humana, tratada aqui como agente motivador direto ou indireto daquele evento (MPF, 2016, p. 168).

Entretanto, nem todos os casos permitirão uma concreta aplicação sobre um roteiro pré estabelecido condizente em conseguir os devidos resultados. O anonimato é o fator em que mais segura as investigações dos delitos. De modo exemplificativo, o uso de wifi gratuito burla a identificação do usuário (Dorigon; Soares, 2018).

Contudo, a polícia possui alternativas para conseguir identificar a localidade do criminoso. Para utilizar a internet é necessário um provedor, ou seja, aquele que disponibilizará o acesso. Assim, a autoridade competente irá solicitar a identificação do computador para o provedor, o qual é obrigado a fornecer (Teixeira, 2022).

Outro fator é o flagrante delito, uma vez que é quase impossível de acontecer, pois, em respeito aos princípios da intimidade e da privacidade, a polícia judiciária não monitora dispositivos eletrônicos. Ainda que utilizasse “isca” para o acompanhamento de um delito, é preciso a identificação do autor do crime. Semelhantemente, nos delitos virtuais a execução inicia em um lapso de tempo longo para que a consumação ocorra (Teixeira, 2022).

O estabelecido “BOOM” dos delitos virtuais ocorreu repentinamente após a pandemia do COVID-19 não criou possibilidades para capacitar os policiais a respeito dessas novas modalidades criminosas. Somente a criação de novas legislações não apresentaram efeitos concretos para o requisito (Lourenço; Santos; Almeida; Castro, 2023).

Uma pesquisa sobre o uso das Tecnologias de Informação e Comunicação nos domicílios brasileiros foi realizada pelo Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br). O estudo, denominado TIC Domicílios 2020, constatou um aumento no uso de tecnologias no Brasil a partir do ano de 2019 comparando com o ano de 2020, durante a pandemia do Coronavírus.

Foi constatado que o uso de tecnologias digitais no Brasil foram intensificados, conforme as seguintes informações, sendo no ano de 2019 cerca de 71% dos domicílios

brasileiros tinham acesso à internet, porém em 2020 a porcentagem aumentou para 83% dos domicílios brasileiros.

O direito evolui constantemente, logo os órgãos que trabalham para protegê-lo deveriam evoluir conjuntamente. A justiça brasileira criou novas leis concretas acerca de cada nova modalidade que surgiu. Contudo, percebe-se que não possui efeito em sua concretização. É preciso uma capacitação constante, de modo que esteja presente a atenção e o acompanhamento acerca do mundo digital. Assim, complementa Emerson Wendt e Higor Jorge (2021):

> Os integrantes desses órgãos devem ser estimulados por políticas internas a participar destas capacitações. Ademais, políticas públicas nacionais, voltadas aos órgãos de segurança pública, são bem-vindas e motivarão os estados a investir na qualificação de seus quadros (Wendt; Jorge, 2021, p. 246).

Há outro fator que dificulta o combate a esses delitos. Não há um consenso ou uma coordenação entre os órgãos responsáveis pela investigação de crimes online, mesmo pertencentes a um mesmo órgão. Isso resulta num déficit de conhecimento e comunicação padronizada. Ao concentrar a persecução penal em um único órgão facilita a compreensão e a metodologia a ser aplicada a esses encargos ou futuros delitos.

Boa parte dos criminosos da área da informática, possuem conhecimentos e, a cada dia, buscam novos modos de aprimorar os meios de consumar os delitos. À vista disso, verifica-se a necessidade de buscar novas alternativas para aumentar a segurança na rede, logo, confrontando frente as atualidades dos criminosos (Teixeira, 2022).

Diante disso, acrescenta Tarcísio Teixeira (2022), “o procedimento investigatório não se apresenta vestido de provas irrefutáveis e contundentes do crime cometido.”. Sendo assim, condiz com a falta de preparo de alguns agentes de investigação e da estrutura disponível, ou seja, elementos como capacitação e material informático.

Consoante ao aumento dessa modalidade, Wendt E Jorge (2021) apresenta uma estratégia plausível, sendo “a da formatação de um laboratório de inteligência cibernética nos estados, capaz de auxiliar e procedimentalizar os demais órgãos estaduais.”. Consoante a alta demanda, apenas alguns estados possuem órgãos específicos para essa modalidade de crime.

Outro grande desafio é equilibrar a segurança pública e os direitos individuais à privacidade garantidos constitucionalmente. Logo, dispõe o Art. 5° da Constituição Federal:

> 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).

De forma clara o uso da tecnologia poderia facilitar o trabalho nas investigações. Muitas das tecnologias já são utilizadas na aplicação da lei, como câmeras de vigilância, sistemas de reconhecimento facial e monitoramento de comunicações. Bem como, o uso de algoritmos e inteligência artificial na análise de dados e tomada de decisões policiais. Contudo, podem representar uma ameaça à privacidade dos cidadãos se não forem devidamente regulamentadas e controladas.

Há um direito a ser preservado. Por mais que a rápida evolução tecnológica supera a capacidade das leis existentes de acompanhá-las, criando lacunas regulatórias e incertezas legais, não pode ultrapassar os direitos já estabelecidos constitucionalmente, mesmo que seja em caso de delitos cibernéticos. Uma vez que, comprova-se com uma profunda investigação que envolve dados e informações privadas (Mozetic; Babiero, 2024).

Há uma importância da previsibilidade das leis na proteção dos direitos fundamentais. Por mais que as lacunas da regulação legal possam ser complementadas pela interpretação do aplicador do direito, tais interpretações não podem suprir a necessidade de uma *lex stricta y lex praevia* (a lei penal deve ser interpretada restritivamente e presente na lei penal. Assim, ressaltando a necessidade de uma legislação precisa e prévia (Martinez, 2019).

Portanto, é necessário atualizar e fortalecer as leis e regulamentos para garantir que o uso da tecnologia pela polícia seja realizado de acordo com os mais altos padrões éticos e legais.

3.2. Perspectivas na aplicação dos novos delitos penais

Acrescentando outro aspecto, verifica-se a necessidade de uma maior participação do Brasil nas convenções internacionais. No contexto da crescente digitalização da sociedade moderna, a busca pela cooperação internacional e marcos legais robustos para lidar com os desafios emergentes tornou-se cada vez mais evidente.

Conjuntamente, as ameaças passaram a ser globalizadas, o qual possibilita o autor de um crime morar no país estrangeiro, ou até mesmo concurso de agentes que estejam

localizados em diferentes países, com a utilização dos recursos tecnológicos para a preparação e execução de seus crimes (Dorigon; Soares, 2018).

O estabelecimento das convenções internacionais sobre o direito digital trouxe uma harmonia entre as leis acerca de tecnologia ao nível global. Logo, Vanzetta atribui sentido instruído por Leite e Lemos, no seguinte sentido:

> A cooperação internacional e a harmonização das legislações penais dos países despontam como saídas eficazes no combate à criminalidade informática, na medida em que permitem mais agilidade e eficácia nas investigações e punições (Leite; Lemos, 2014, p.63 apud Vanzetta, 2019, p. 24).

Essas convenções, elaboradas e adotadas por organizações internacionais - como as Nações Unidas (ONU), o Conselho da Europa e outras entidades regionais - promovem cooperação transfronteiriça relacionadas ao direito digital. O Brasil tem participação ativa nessas convenções se comprometendo a contribuir para o desenvolvimento do arcabouço jurídico global sobre questões digitais.

Inicia-se com a participação do Brasil na Convenção de Budapeste sobre Crimes Cibernéticos. Ocorreu em 2001 pelo Conselho da Europa, sendo o primeiro tratado internacional que abordou questões relacionadas à segurança cibernética.

A participação do Brasil demonstra um reconhecimento sobre a importância de combater ameaças digitais transnacionais e promover a cooperação internacional neste domínio, mesmo estando apenas como observador (Dorigon; Soares, 2018).

A Convenção de Budapeste traz como objetivo a harmonização das leis nacionais em relação a crimes cibernéticos, assim, criando procedimentos eficazes para investigação e aplicação da lei nesses casos (Vanzetta, 2019).

No entanto, a participação do Brasil oferece oportunidades significativas. Isso inclui o acesso a recursos e conhecimentos compartilhados pela comunidade internacional, podendo estabelecer parcerias e colaborações bilaterais e multilaterais para enfrentar desafios comuns no campo do direito digital, bem como trazer investimentos em tecnologia e inovação, demonstrando um compromisso com a proteção dos direitos digitais e a promoção de um ambiente digital seguro e confiável (Dorigon, Soares, 2018).

Conduto, mesmo participando e adquirindo conhecimentos nas convenções, a aplicação desses tratados no Brasil trouxe desafios. Um dos principais desafios enfrentados pelo Brasil na implementação das convenções internacionais é a necessidade de adequar sua legislação nacional aos padrões estabelecidos nos tratados. Por muitas vezes requer ajustes

significativos nas leis existentes, com necessidade de criação de novas políticas e regulamentações relacionadas ao direito digital. Além disso, o Brasil não tem uma base fortalecedora com instituições responsáveis pela aplicação da lei.

Em relação a perspectivas futuras, a sociedade avançará com o passar dos anos, e o Brasil necessita estar atento consoante ao tratamento internacional acerca da segurança digital. Uma das perspectivas futuras para o Brasil é a continuação do seu engajamento ativo em fóruns e negociações internacionais sobre direito digital.

Outra perspectiva importante é o fortalecimento das capacidades nacionais do Brasil na legislação, ou seja, melhorar a aplicação da lei e infraestrutura tecnológica para lidar com os desafios do mundo digital. Isso requer investimentos significativos em recursos humanos e tecnológicos, bem como a adoção de novas políticas e regulamentações atualizadas que reflitam as melhores práticas internacionais.

4. CONSIDERAÇÕES FINAIS

A análise empreendida neste Trabalho de Conclusão de curso foi a ressaltada profunda conexão entre o avanço tecnológico e os desafios jurídicos, especialmente no domínio do direito penal.

Em suma, a internet revolucionou a vivência e comunicação, possibilitando a conexão de milhões de pessoas globalmente. No entanto, com essa crescente surgem os desafios dos crimes cibernéticos, afetando indivíduos, empresas e governos. A criação das novas tipificações como Invasão de dispositivo eletrônico - Art. 154-A; Furto mediante fraude eletrônica - Art. 155 §4-B; e Fraude eletrônica - Art. 171 §2-A, demonstra o esforço do Brasil para adaptar o direito com a sociedade e preencher lacunas deixadas na legislação. Entretanto, há obstáculos significativos a serem enfrentados.

A internet surgiu como forma de aprimoramento da comunicação militar, mas que rapidamente foi descoberta para diversas utilidades, como, por exemplo, estudo por meio das universidades americanas. A rápida proliferação do uso de dispositivos digitais na sociedade contemporânea, aprimorada pelo isolamento social, cria uma via para possibilidades de delitos adaptáveis às novidades na sociedade. Pois, antes havia o receio de sofrer um roubo nas ruas, mas hoje o receio é ser vítima de uma fraude eletrônica.

Verificou-se a imposição de adaptação do ordenamento jurídico diante das transformações tecnológicas e sociais. O qual justifica os inúmeros conceitos, antes nunca

vistos nem imaginados, mas agora extremamente importantes para conhecimento tanto para o mundo jurídico quanto para o cidadão que providenciará forma de se prevenir de tais delitos.

As alterações e surgimentos dos principais crimes cibernéticos contra o patrimônio no Brasil, antes eram realizados em outros modos de execução, os quais não envolviam dispositivo eletrônico. Contudo, com a correta disposição legal, as modalidades delitivas contribuíram para a abordagem da polícia judiciária consoante ao combate. Desse modo, a aplicação da lei vem se adequando à realidade digital.

Posteriormente, verificou-se a eficácia do ordenamento jurídico no enfrentamento dos crimes cibernéticos, com base em medidas atuantes na investigação, especificamente na comprovação dos delitos virtuais. Observou-se a atuação internacional adotada pelo Brasil e projeções futuras.

Diante do exposto, fica claro que a análise dos avanços e desafios do direito penal diante dos crimes cibernéticos é de extrema relevância para o desenvolvimento de estratégias eficazes de prevenção e combate a essas práticas.

Destaca-se a importância dos órgãos competentes para trabalhar com o direito digital, logo, unificar o modo de operação para a investigação. O rápido aprimoramento não possibilitou um preparo e adequação das autoridades competentes, para que efetivamente combater tais crimes. Conclui-se que necessita de capacitação dos atuais agentes, mas também necessita de profissionais especialistas em tecnologia da informação para que compõem a prevenção.

Para que se atue de forma efetiva, mas respeitados os direitos fundamentais respaldados na Constituição Federal do Brasil de 1988. A cooperação do Brasil para com os tratados internacionais, desempenha um papel crucial na prevenção desses crimes e nas inovações para prevenção de tais, o qual aumenta a conscientização sobre os riscos cibernéticos e a segurança na internet.

A legislação brasileira conseguiu avançar na busca de antecipar os desafios e oportunidades decorrentes da crescente digitalização da sociedade. Contudo, é preciso buscar a atenção em relação a futuros ritmos das mudanças tecnológicas, os quais poderão deixar lacunas na regulamentação e na aplicação da lei.

Entretanto, há possíveis tendências criminológicas que, mesmo inscritas em tipos penais conhecidos, necessitam de possuir suas tipificações próprias, como ocorreu com o furto mediante fraude eletrônica e a fraude eletrônica. Tais condutas passaram pelo princípio da taxatividade, que exige que as normas sejam claras, precisas e específicas.

De modo exemplificativo, assunção de identidade de terceiros, sequestro de contas bancárias, transferência de títulos de débitos para outrem. Portanto, é crucial que o sistema jurídico brasileiro se modernize e se adapte às futuras tendências criminológicas, incorporando novas abordagens, legislação atualizada e políticas públicas eficazes para garantir a segurança e a justiça para todos os cidadãos.

Desse modo, os crimes cibernéticos são novos e complexos. A criatividade em ludibriar a população criando novos meios de praticar delitos, traz um considerável desafio em várias frentes. Assim, centralizar a capacitação de profissionais responsáveis para o combate, bem como, apresentar inovações na legislação são elementos fundamentais para a efetiva aplicação dos direitos fundamentais estabelecidos na Constituição Federal de 1988.

REFERÊNCIAS

AZEVEDO, Flavio Olímpio de. **Artigo 154-A.** Disponível em: https://www.direitocom.com/codigo-penal/codigo-penal/artigo-154-a. Acesso em: 17 abr. 2024.

BARBAGALO, Juiz Fernando Brandini. **O novo crime de fraude eletrônica e o princípio da legalidade.** 2022. Disponível em: https://www.tjdft.jus.br/institucional/imprensa/campanhas-e-produtos/artigos-discursos-e-entrevistas/artigos/2022/o-novo-crime-de-fraude-eletronica-e-o-principio-da-legalidade. Acesso em: 26 abr. 2024.

BARATTA, Alessandro. **Criminologia crítica e crítica do direito penal introdução à sociologia do direito penal.** 3. ed. Rio de Janeiro: Revan, 2002.

BENAKOUCHE, TAMARA. **REDES TÉCNICAS/REDES SOCIAIS:** PRÉ-HISTÓRIA DA INTERNET NO BRASIL. Revista USP, São Paulo, Brasil, n. 35, p. 124–133, 1997. DOI: 10.11606/issn.2316-9036.v0i35p124-133. Disponível em: https://www.revistas.usp.br/revusp/article/view/26923.. Acesso em: 17 maio. 2024.

BRASIL. **Código Penal (Decreto-Lei nº 2.848, de 7 de dezembro de 1940)**. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 04 abr 2024.

BRASIL. **Constituição da República Federativa do Brasil de 1988.** Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 20 abr 2024.

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. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 14 mar. 2014

BRASIL, **Lei nº 14.155, de 27 de maio de 2021**. http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14155.htm. Acesso em 16 de abr de 2024.

BRASIL. Ministério da saúde. Presidente do conselho. R**ECOMENDAÇÃO Nº 036, DE 11 DE MAIO DE 2020.** Disponível em: https://conselho.saude.gov.br/recomendacoes-cns/1163-recomendac-a-o-n-036-de-11-de-maio-de-2020. Acesso em: 25 jan. 2024.

BRASIL. Ministério Público Federal. Câmara de Coordenação e Revisão, 2. **Roteiro de atuação:** crimes cibernéticos / 2. Câmara de coordenação e revisão. – 3.ed. rev. e ampl. – Brasília: MPF, 2016.

BRAZ, Jardene. **Crime Cibernético:** da identificação do usuário para efetividade da pena. da identificação do usuário para efetividade da pena. 2022. Disponível em: https://www.jusbrasil.com.br/artigos/crime-cibernetico-da-identificacao-do-usuario-para-efeti

vidade-da-pena/1664917013#:~:text=No%20direito%20penal%2C%20a%20fase,sua%20raz%C3%A3o%20acerca%20dos%20fatos.. Acesso em: 16 mar. 2024.

CAPEZ, Fernando. **Curso de direito penal:** parte geral: arts. 1º a 120. v.1. [Digite o Local da Editora]: SRV Editora LTDA, 2024. E-book. ISBN 9788553622696. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788553622696/. Acesso em: 17 mai. 2024.

CARNEIRO, Adeneele Garcia. **Crimes virtuais:** elementos para uma reflexão sobre o problema na tipificação. elementos para uma reflexão sobre o problema na tipificação. 2012. Disponível em: https://ambitojuridico.com.br/edicoes/revista-99/crimes-virtuais-elementos-para-uma-reflexao-sobre-o-problema-na-tipificacao/. Acesso em: 25 fev. 2024.

CARVALHO, Guilherme Paiva de. **Uma reflexão sobre a rede mundial de computadores**. 2007. Disponível em: https://www.scielo.br/j/se/a/BVCWK5hLdhLLt43JRLMWBMM/. Acesso em: 20 dez. 2023.

CASTELLS, Manuel. **A galáxia da internet**. Rio de Janeiro: Jorge Zahar. 2003, 243 pgs.

CONCEITO.DE., Equipe Editorial de. **Internet:** o que é, conceito e definição. O que é, conceito e definição. 2021. Disponível em: https://conceito.de/internet. Acesso em: 13 dez. 2023.

COSTA, Emanuely Silva; SILVA, Raíla da Cunha. **Crimes cibernéticos e investigação policial.** Revista Eletrônica do Ministério Público do Estado do Piauí, Teresina, v. 1, n. 2, p. 180-196, 2021. Semestral. Disponível em: https://www.mppi.mp.br/internet/revista/editais-de-chamada-de-trabalhos/revista-eletronica-do-ministerio-publico-do-estado-do-piaui/revista-eletronica-do-ministerio-publico-do-estado-do-piaui-3/. Acesso em: 08 maio 2024.

DORIGON, Alessandro; SOARES, Renan Vinicius Oliveira. **Crimes cibernéticos:** dificuldades investigativas na obtenção de indícios da autoria e prova da materialidade. Revista Jus Navigandi, ISSN 1518-4862, Teresina, ano 23, n. 5342, 15 fev. 2018. Disponível em: https://jus.com.br/artigos/63549. Acesso em: 5 mai. 2024.

ESCOLA, Brasil. **Internet no Brasil**; Brasil Escola. Disponível em: https://brasilescola.uol.com.br/informatica/internet-no-brasil.htm. Acesso em 29 de fev de 2024.

GRECO, Rogério. **Direito Penal Estruturado.** MÉTODO: Grupo GEN, 2023. E-book. ISBN 9786559647651. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786559647651/. Acesso em: 26 abr. 2024.

GRECO, Rogério. **Invasão de dispositivo informático - art. 154-a do código penal.** 2013. Disponível em: https://www.jusbrasil.com.br/artigos/invasao-de-dispositivo-informatico-art-154-a-do-codigo-penal/121819872. Acesso em: 14 mar. 2024.

JESUS, Damásio E. de. **Direito Penal – Parte Geral.** 20 ed. São Paulo: Saraiva, 1997. v. 1.

LISBOA, Roberto Senise et al. **Direito na sociedade da informação**. Revista dos Tribunais, ano, v. 95, p. 106, 2006.

LOURENÇO, A. C. G.; SANTOS, C. E. P. dos; ALMEIDA, G. H. de; CASTRO, B. V. de. **O aumento dos crimes cibernéticos durante a pandemia da Covid-19 e as dificuldades para combatê-los.** LIBERTAS DIREITO, [S. l.], v. 4, n. 1, 2023. Disponível em: https://www.periodicos.famig.edu.br/index.php/direito/article/view/387. Acesso em: 09 maio. 2024.

MAGGIO, Vicente de Paula Rodrigues. **Novo crime:** invasão de dispositivo informático - cp, art. 154-a. invasão de dispositivo informático - CP, Art. 154-A. 2013. Disponível em: https://www.jusbrasil.com.br/artigos/novo-crime-invasao-de-dispositivo-informatico-cp-art-154-a/121942478. Acesso em: 08 mar. 2024.

MARTINEZ, Thiago Hartmann. **OS DIREITOS FUNDAMENTAIS X SEGURANÇA PÚBLICA:** a admissibilidade de métodos ocultos de investigação criminal em ambiente digital. 2019. Disponível em: https://repositorio.ul.pt/handle/10451/40795. Acesso em: 04 maio 2024.

MOZETIC, Vinícius Almada; BARBIERO, Diego Roberto. **SURVEILLANCE E A TEORIA DA PONDERAÇÃO:** o conflito entre direito a privacidade e segurança pública no brasil. 2022. Disponível em: http://ojs.unimar.br/index.php/revistaargumentum/article/view/1268%20-%2010.05.2024. Acesso em: 05 maio 2024.

NÚMERO DE GOLPES CONTRA PESSOAS IDOSAS CRESCE MAIS DE 70% EM 2023. Jornal Nacional, 2023. Disponível em: https://g1.globo.com/jornal-nacional/noticia/2023/07/03/numero-de-golpes-contra-pessoas-idosas-cresce-mais-de-70percent-em-2023.ghtml. Acesso em: 05 maio 2024.

OLIVEIRA, Flávio Emanoel Rangel de. **Breves considerações sobre o tipo penal:** do causalismo à teoria constitucionalista. Do causalismo à teoria constitucionalista. 2014. Disponível em: https://jus.com.br/artigos/31002/breves-consideracoes-sobre-o-tipo-penal. Acesso em: 04 abr. 2024.

PINHEIRO, Patrícia P. **Direito Digital.** Editora Saraiva, 2021. E-book. ISBN 9786555598438. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786555598438/. Acesso em: 14 mar. 2024.

ROCKEMBACH, Moisés; PAVÃO, Caterina Groposo. **Arquivamento da web e preservação digital**. São Paulo: Pimenta Cultural, 2024. 282 p. Disponível em: https://www.academia.edu/113743875/Arquivamento_da_web_e_preserva%C3%A7%C3%A3o_digital?auto=download. Acesso em: 04 fev. 2024.

ROSSINI. Augusto. **Informática Telemática e Direito Penal.** 2004 Memoria Jurídica: 2004, Colombo.

TAVARES, Iury. **Distinção entre o Furto mediante Fraude e Estelionato.** 2021. Disponível em: https://www.jusbrasil.com.br/artigos/distincao-entre-o-furto-mediante-fraude-e-estelionato/1198496201. Acesso em: 11 maio 2024.

TRABALLI, Arthur. **A inviolabilidade à intimidade, à vida privada, à honra, à imagem:** dano material, moral ou à imagem. dano material, moral ou à imagem. 2016. Disponível em: https://www.jusbrasil.com.br/artigos/a-inviolabilidade-a-intimidade-a-vida-privada-a-honra-a-

imagem-dano-material-moral-ou-a-imagem/337428559#:~:text=A%20vida%20privada%20%C3%A9%20aquela,do%20indiv%C3%ADduo%E2%80%9D%20(3).. Acesso em: 23 abr. 2024.

TEIXEIRA, Tarcísio; GUERREIRO, Ruth M. **Lei Geral de Proteção de Dados Pessoais (LGPD)**: Comentada Artigo por Artigo. [Digite o Local da Editora]: Editora Saraiva, 2022. E-book. ISBN 9786555599015. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786555599015/. Acesso em: 29 mar. 2024.

TESCAROLLO, Camila Berto. **A Internet e seus conceitos básicos.** 2016. Disponível em: https://www.programaria.org/internet-e-seus-conceitos-basicos/. Acesso em: 13 dez. 2023.

UOL. **Estudo mostra que pandemia intensificou uso das tecnologias digitais**. 2021. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2021/11/25/estudo-mostra-que-pandemia-intensificou-uso-das-tecnologias-digitais.htm#:~:text=A%20pandemia%20de%20covid-19%2C%20declarada%20pela%20Organiza%C3%A7%C3%A3o%20Mundial,domic%C3%ADlios%20com%20algum%20tipo%20de%20conex%C3%A3o%20%C3%A0%20rede.. Acesso em: 14 jan. 2024.

VANZETTA, Karoline. **DIREITO DIGITAL**: a importância da especificidade de leis e dos tratados internacionais frente aos avanços tecnológicos. 2019. 40 f. TCC (Graduação) - Curso de Direito, Universidade Regional Integrada do Alto Uruguai e das Missões, Erechim, 2019. Disponível em: https://www.uricer.edu.br/cursos/arq_trabalhos_usuario/4626.pdf. Acesso em: 19 maio 2024.

WENDT, Emerson; JORGE, Higor Vinicius Nogueira. **Crimes cibernéticos:** ameaças e procedimentos de investigação. 3ª Ed. Rio de Janeiro: Brasport, 2021.