PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
PRO-REITORIA DE GRADUAÇÃO
ESCOLA DE DIREITO, NEGÓCIOS E COMUNICAÇÃO
CURSO DE DIREITO
NÚCLEO DE PRÁTICA JURÍDICA
COORDENAÇÃO ADJUNTA DE TRABALHO DE CURSO II

ANÁLISE JURÍDICA DO CRIME DE ESTELIONATO VIRTUAL

ORIENTANDO: TEODORO MACIEL FERREIRA

ORIENTADOR: PROF. Me. JOSÉ CARLOS DE OLIVEIRA

GOIÂNIA-GO
2023

TEODORO MACIEL FERREIRA

ANÁLISE JURÍDICA DO CRIME DE ESTELIONATO VIRTUAL

Artigo Científico apresentado à disciplina Trabalho de Curso I, da Escola de Direito, Negócios e Comunicação da Pontifícia Universidade Católica de Goiás (PUCGOIÁS).
Prof. Me. Orientador: José Carlos de Oliveira

GOIÂNIA-GO
2023

RESUMO

ANÁLISE JURÍDICA DO CRIME DE ESTELIONATO VIRTUAL

As tecnologias, principalmente, a Internet, têm exercido expressivas transformações na sociedade global e, o Brasil, a cada dia, tem adentrado neste universo em um caminho que direciona sempre para a inovação em todos os setores. No entanto, embora o mundo ciber seja incontestavelmente relevante, trazendo inúmeros benefícios, gera também novas formas de crimes. Os crimes cibernéticos estão se tornando cada vez mais frequentes e sofisticados, difíceis de se combater. O estelionato virtual consiste em um destes crimes cibernéticos que mais tem afetado a sociedade brasileira atualmente. Portanto, este estudo se propôs investigar as implicações jurídicas do crime de estelionato virtual no Brasil e, esta investigação se configurou no principal objetivo deste trabalho. Buscou também conceituar os crimes cibernéticos, especialmente, o crime de estelionato virtual, bem como, o perfil de criminosos e sua forma de atuação e vítimas; analisar a legislação pertinente aos crimes cibernéticos e sua aplicação no Brasil e; investigar as medidas de prevenção e punição do crime de estelionato virtual de acordo com a legislação brasileira. Para alcançar tais objetivos, optou-se pelo artigo científico que teve como método a pesquisa de natureza exploratória descritiva com abordagem qualitative. Concluiu-se que a Lei 14.155/21 trouxe alterações relevantes com maior endurecimento das penas e tipificando novos crimes como o estelionato contra vulnerável e idoso, o estelionato sentimental e a fraude eletrônica. A nova norma prevê penas mais severas que podem ser aumentadas de reclusão, além de multa. Embora fossem observados avanços, o caminho para a prevenção e combate ao crime de estelionato virtual ou qualquer outro que se utiliza dos dispositivos de informática para a sua consumação ainda é longo.

Palavras-Chave: Crimes Cibernéticos. Estelionato Virtual. Lei 14.155/21.

ABSTRACT

LEGAL ANALYSIS OF THE CRIME OF VIRTUAL STEAM

Technologies, mainly the Internet, have brought about significant transformations in global society and, every day, Brazil has entered this universe on a path that always leads towards innovation in all sectors. However, although the cyber world is undeniably relevant, bringing countless benefits, it also generates new forms of crimes. Cybercrimes are becoming increasingly frequent and sophisticated, difficult to combat. Virtual fraud is one of the cybercrimes that has most affected Brazilian society today. Therefore, this study set out to investigate the legal implications of the crime of virtual embezzlement in Brazil and this investigation was the main objective of this work. It also sought to conceptualize cybercrimes, especially the crime of virtual embezzlement, as well as the profile of criminals and their way of acting and victims; analyze the legislation relevant to cybercrimes and its application in Brazil and; investigate prevention and punishment measures for the crime of virtual embezzlement in accordance with Brazilian legislation. To achieve these objectives, we opted for a scientific article whose method was exploratory, descriptive research with a qualitative approach. It was concluded that Law 14,155/21 brought relevant changes with greater harshness of penalties and typifying new crimes such as embezzlement against vulnerable and elderly people, sentimental embezzlement and electronic fraud. The new rule provides for more severe penalties that can be increased by imprisonment, in addition to a fine. Although progress has been made, the path to preventing and combating the crime of virtual fraud or any other crime that uses computer devices for its consummation is still long.

Keywords: Cybercrimes. Virtual Swindle. Law 14,155/21.

SUMÁRIO

INTRODUÇÃO

Este trabalho trata-se de um artigo científico acerca do crime de estelionato virtual que tem crescido de maneira expressiva no Brasil e utiliza como ferramenta a Internet e as inovações tecnológicas a seu favor. O uso das tecnologias tem como principal alicerce a rapidez e eficiencia que as ferramentas tecnológicas possuem.

As tecnologias, especialmente, a Internet, têm transformado de modo significativo a sociedade. Isso traz inúmeros benefícios, mas, também, gerando novas formas de crimes. Os crimes cibernéticos têm se tornado cada vez mais frequentes e o estelionato virtual, em especial, tem afetado diversos grupos de pessoas no Brasil.

O estelionato virtual consiste em um tipo de crime que ocorre por meio de fraudes e enganações, no qual o criminoso se passa por uma pessoa ou empresa confiável e induz a vítima a fornecer dados pessoais, bancários ou a realizar transferências de dinheiro. Em muitos casos, os alvos preferenciais são os idosos que são menos familiarizados com a tecnologia e, portanto, mais suscetíveis a cair em golpes virtuais.

O estelionato consiste em um delito no qual o agente obtem vantagm ilícita para si ou para terceiros e decorre da indução ou manutenção de uma pessoa em erro. É um tipo de crime que mexe com a mente da vítima fazendo-a crer em situações que poderiam beneficiá-la caso fossem reais. Desse modo, o criminoso conduz a vítima ao erro enganando e iludindo, tudo isso com a finalidade de obter vantagem ilícita. O estelionato virtual tem como instrumento o ambiente virtual que tem sido cada vez mais eficaz e modernizado. (ANDREUCCI, 2014)

Este estudo teve como proposta principal investigar as implicações jurídicas do crime de estelionato virtual no Brasil. Buscou também conceiturar crimes cibernéticos, especialmente, o crime de estelionato virtual, bem como o perfil de criminosos e sua forma de atuação e vítimas; analisar a legislação pertinente aos

crimes cibernéticos e sua aplicação no Brasil e; investigar as medidas de prevenção e punição do crime de estelionato virtual de acordo com a legislação brasileira.

As questões problemas que permearam este artigo consistiram em análises acerca do crescimento dos crimes cibernéticos no mundo e no Brasil, inclusive entre as pessoas concebidas como intelectualmente avançadas que ainda se tornam vítimas deste tipo de crime, além de muitas outras que não possuem conhecimento mais aprofundado do que sejam crimes cibernéticos. Vale destacar a relevância da identificação dos tipos de crimes cibernéticos mais praticados, as características dos criminosos e perfis de vítimas mais buscados por eles.

Outra questão que se considera importante destacar é a de que a percepção de crescimento dos crimes cibernéticos exige maior engajamento da legislação brasileira no sentido de prevenir e combater tais práticas. Portanto, é de grande relevância analisar como a legislação brasileira tem se posicionado mediante esse tipo de crime. Muitas pessoas que praticam crimes cibernéticos não têm conhecimento acerca das implicações jurídicas no que concerne ao tema e outras confiam plenamento na impunidade, portanto, vale apresentar tais implicações.

As hipóteses elencadas neste estudo foram as de que a falta de informações, conhecimento e negligência dos usuários da Internet em relação à segurança de suas informações pessoais são fatores que contribuem para o aumento do estelionato virtual praticado contra grupos de pessoas no Brasil. Também a pouca eficiência da legislação, assim como, das autoridades responsáveis pela investigação desses crimes também são fatores que dificultam a prevenção e punição dos crimes cibernéticos, especialmente, o estelionato virtual.

Este trabalho se justifica na medida em que se propõe refletir sobre o fenômeno do estelionato virtual praticado contra usuários da Internet para que, dessa forma, se possa identificar as principais características dos criminosos e das vítimas, bem como, os meios utilizados para a prática do crime, as consequências jurídicas e sociais do delito e as medidas preventivas e repressivas existentes para combater esse tipo de crime.

Para alcançar os objetivos propostos, optou-se pelo artigo científico que teve como método a pesquisa de natureza exploratória descritiva com abordagem qualitativa. A pesquisa qualitativa foi realizada por meio da análise de literaturas já publicadas acerca do tema, bem como, documentos normativos acerca do estelionato virtual praticado no Brasil com a finalidade de compreender melhor as formas de atuação dos criminosos e as características das vítimas.

1 DOS CRIMES CIBERNÉTICOS

Nesta seção referenciam-se as definições relevantes para melhor entendimento do que vem a ser esse tipo de crime, os tipos de crimes cibernéticos e o perfil de criminosos e vítimas do estelionato virtual.

1.1 DEFINIÇÕES DE CRIMES CIBERNÉTICOS E ESTELIONATO VIRTUAL

A Internet se configura como uma grande rede de dispositivos de vários tipos. Os equipamentos se conectam uns aos outros de diferentes formas, seja por meio de linhas de comunicação particular, seja por cabos telefônicos e por satélites. Computadores e celulares se conectam de qualquer lugar se integram a Internet. A Internet funciona como um caminho pelo qual a informação, através de sons, textos e imagens é disponibilizada, trafegando entre qualquer dispositivo que acessa a rede em uma enorme velocidade. (ESTRELA, 2003)

Os crimes digitais ou eletrônicos estão entre os diversos acontecimentos que tem sua origem no mundo virtual. Estes crimes estão em crescimento acelerado e se constituem como sendo crimes comuns, mas que são praticados com o uso da Internet, portanto, não são crimes novos, apenas usam novos caminhos para sua prática. O meio digital tem sido muito utilizado em razão da sua facilidade e o fato de proporcionar ao criminoso a efetivação de sua conduta ilícita com menor potencial de riscos. (DINIZ; CARDOSO; PUGLIA, 2022)

O crime eletrônico não consiste, por natureza, em um crime de fim, mas sim, de meio, pois utiliza-se de um meio virtual para ser praticado. Isto é, um crime de fim seria aquele cuja modalidade somente aconteceria em um ambiente virtual, exceto

os crimes praticados por hackers que não podem de maneira alguma ser enquadrados na categoria de falsidade ideológica, fraude, estelionato, extorsão e outros. Isso significa que, o meio no qual se materializa a conduta criminosa pode ser virtual, mas, o crime, em determinados casos não. (PINHEIRO, 2013)

Por crimes digitais ou cibernéticos entende-se como sendo atos delituosos, condutas ilícitas praticadas no ambiente virtual e tem como principal ferramenta a informática como um todo. São tipos de crimes praticados, especificamente, no ambiente virtual utilizando algum tipo de dispositivo tecnológico. (ROSA, 2002; ROCHA, 2017)
Os crimes digitais consistem em conduta que fere o estado natural dos dados e recursos fornecidos por um sistema de processamento de dados. Tanto pode ser pelo armazenamento, transmissão de dados ou pela compilação. Ofende o estado natural dos dados na sua forma entedida pelos elementos componentes de um sistema de armazenamento, transmissão e tratamento de dados, bem como, na forma mais rudimentar. Consiste ainda em todo procedimento que atenta contra dados e pressupõe dois elementos que não se dissociam, ou seja, contra dados destinados para as operações do computador e também por meio do mesmo. Neste caso, se utilizam softwares e hardwares com o fim de perpetrá-los. (ROSA 2002)

No caso do estelionato, a expressão é de origem grega stelio que denomina uma espécie de lagarto que, como meio de iludir suas presas utiliza-se da estratégia de mudar de cor. A palavra estelionato se encaixa bem com o réptil no que concerne à tipificação do delito que o estelionatário pratica, pois ele usa de artificios e artimanhas para enganar alguém, para iludir. (RIBEIRO, 2019)

Ao crime de estelionato era determinada pena de morte se o prejuízo à vítima fosse acima de vinte mil réis nas Ordenações Filipinas. O nome jurídico “estelionato” foi adotado no ano de 1830 no Código Penal do Império brasileiro. O referido Código prescreveu ao delito de estelionato diversas figuras como, artifício fraudulento por meio do qual se obtem fortuna ou parte dela e quaisquer títulos. A mesma orientação foi seguida pelo Código Penal Republicano de 1890 e tipificou onze figuras que se aliam ao delito de estelionato, das quais se destaca a utilização de artifício com o fim de iludir a vítma e dela extrair proveito ou lucro. (BITTENCOURT, 2012)

O crime de estelionato tem como base a má-fé do sujeito ardil. Este sujeito induz ou mantem a vítima em erro usando qualquer meio fraudulento e, dessa forma, conseguir vantagem patrimonial beneficiando a si próprio ou outra pessoa. (CAMPOS, 2016) O estelionato está tipificado como delito no capítulo V, artigo 171, do Código Penal de 1940 e a pena para quem pratica este delito é a de reclusão de um a cinco anos e multa. Segundo estabelece o artigo 171:

> Art. 171 – Obter para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento:
>
> Pena – reclusão, de um a cinco anos, e multa, de quinhentos mil réis a dez contos de reís. (BRASIL, 1940)

Afirma-se que o crime de estelionato trata-se de crime contra o patrimônio e, portanto, a legislação penal tem como objetivo proteger a inviolabilidade patrimonial que se orienta pela prática de atos que objetivam enganar a vítima e, assim, o agente ser beneficiado. (CUNHA, 2019)

A fraude se constitui como o ponto central do delito de estelionato e, portanto, pode-se identificar os elementos que integram a figura típica, isto é, a conduta do agente cuja direção é a obtenção de vantagem ilícita que prejudica outros; a direção da vantagem é para o autor ou a terceiro; a vítima é colocada ou mantida em erro; o agente usa artifício ou qualquer outro meio ardio ou fraudulente para atingir o objetivo pretendido. (GRECO, 2011)

Não há distinção entre fraude cível e fraude penal, somente depende da existência de uma fraude. Consiste em uma questão de grau e qualidade de prejuízo e que as circunstâncias do caso determinam. Estando presentes os requisitos para consumação do crime de estelionato, deverá haver punição criminal. (GRECO, 2011)

1.2 DISPOSIÇÃO GERAL DOS CRIMES CIBERNÉTICOS

Vale destacar que a Internet passou a ser de grande relevância enquanto ferramenta no mundo globalizado e, essa importância se apresenta pelo fato de que a rede possibilita e favorece o relacionamento entre as pessoas, a transmissão de informações e contribui significativamente com o comércio.

Em “Pássaros voam em bando”, o escritor Percival Henriques enfatiza que a Internet não se restringe mais a somente um projeto acadêmico. No ano de 2015, mais de 3,2 bilhões de pessoas puderam enviar e receber pacotes de bytes, trocar conhecimentos, expressar sentimentos, articular ações, organizar eventos, comprar e vender, pesquisar, mas, também, gritar, vigiar, ser vigiadas, roubar e enganar. (SILVA, 2021)

Entretanto, não são somente benefícios que a Internet traz, pois na mesma medida, ela também traz um número infinito de atos ilícitos que aumentam a cada dia mais e de modo assustador. Assim sendo, na mesma proporção que a Internet tem sido ferramenta de integração mundial, favorecendo os relacionamentos à distância entre as pessoas, ela se constitui como um ambiente fértil para a prática de diversos delitos e crimes. (SANTOS et al., 2017)

A inserção da Internet no mundo fez com que o ser humano perdesse parcialmente sua privacidade, estando submetido a riscos que decorrem da excessiva exposição e acarretando até mesmo danos morais, apesar dos inúmeros benefícios que a rede mundial de computadores inegavelmente trouxe. Dentre os benefícios estão a facilitação de atividades e processos, armazenamento e coordenação de dados, além da integração cibernética. No entanto, a Internet também contribui expressivamente para o aumento de delitos informáticos, servindo de instrumento para prática delituosa. (SPINELLI, 2018)

Entende-se, desse modo, que a pessoa humana teve sua privacidade parcialmente perdida em razão da popularização da Internet, pois por meio dela, é possível verificar que muitos crimes, antes praticados somente no mundo real, passaram a ser praticados usando a rede, dentre eles, está o estelionato virtual.

De acordo com o Grupo de Combate aos Crimes Cibernéticos, da Procuradoria da República no Estado de São Paulo, existem muitas atividades que o ser humano pode realizar utilizando a Internet. Destacam-se o pagamento de contas, conversas em salas de bate-papo, realizar downloads de arquivos, trocar mensagens, comprar e vender produtos, realizar serviços, acessar diversas informações de seu interesse. No entanto, todas as atividades realizadas na rede oferecem riscos para quem a usa, pois muitas outras pessoas mal intencionadas se aproveitam da escala e velocidade com as quais circulam as informações para praticarem delitos e crimes. É preciso, então, muita cautela ao se utilizar a Internet para que não seja vítima de pessoas que utilizam o mundo virtual para praticar crimes que podem prejudicar significativamente a vida da vítima. (OLIVEIRA, 2020)

Grande parte dos crimes praticados na Internet também é praticada no mundo real. Neste caso, a Internet se apresenta apenas como uma facilitadora, especialmente, em virtude do anonimato que a rede proporciona. No que tange ao conceito de crime, efeito e ato, as questões são as mesmas, tanto a aplicação para o Direito Penal ou Direito Penal Digital. No que se refere às inovações jurídicas acerca da esfera digital, as principais mudanças estão nas questões da investigação probatória e da territorialidade, além da necessidade de tipificar as penas para algumas modalidades que merecem um tipo penal próprio em razão de suas peculiaridades. (PINHEIRO, 2013)

O crime digital consiste em um fato típico e antijurídico praticado através da tecnologia da informação ou contra ela. O Direito informático constitui-se como um conjunto de princípios, entendimentos jurídicos e normas advindas da atividade informática. Portanto, o crime informático consiste em ato antijurídico e típico praticado por meio da informática como um todo ou contra um sistema, rede de computadores ou dispositivo informático. Assim sendo, afirma-se que a informática no crime informático ou consiste no bem ofendido ou o meio pelo qual ocorre a ofensa aos bens protegidos pelo Direito Penal. (JESUS, 2016)

No que tange à perspectiva política, social, cultural e econômica, a Internet trouxe diversos pontos positivos para o mundo globalizado. No entanto, muitas mazelas vieram com ela como, a proliferação dos crimes cibernéticos, os quais podem se

destacar as práticas de racismo, pornografia infantil, crimes contra a honra, fraudes em contratos eletrônicos, furtos, dentre outros. (MAUES et al., 2018)

Nos cibercrimes, a conduta pode ser caracterizada como dolosa, isto é, intencional, cujo resultado foi planejado pelo autor da conduta. Pode também ser culposa, ou seja, resultante da imperícia, imprudência ou negligência do autor, é omissiva ou comissiva. A ação pode ter sua prática auxiliada por equipamentos informáticos como computadores, dispositivos correlatos, celulares, tanto na rede mundial de computadores como fora dela. Seu objetivo é ofender direta ou indiretamente a segurança da informática. Desse modo, o alvo não é a Internet, mas sim, o uso de dispositivos de informática. Os cibercrimes podem ser praticados por pessoas físicas, mas, também por pessoas jurídicas e tais condutas devem ser caracterizadas como típica, contravenção penal ou ilícita. (OLIVEIRA, 2020)

Ao contrário do que se pode pensar, a Internet não é um ambiente imune aos rigores da lei, apesar de ser mais difícil a investigação de crimes praticados com o uso da rede. Criminosos e organizações criminosas têm lançado mão dos avanços tecnológicos se aprimorando cada vez mais. Entretanto, a legislação brasileira também tem se adequado no sentido de coibir as práticas de cibercrimes. Sobre o perfil de criminosos e vítimas no ambiente virtual é o que se discute no tópico a seguir.

1.3 TIPOS DE CRIMES CIBERNÉTICOS

A priori, entende-se como pertinente abordar de modo suscinto a composição da Internet. A mais conhecida por todas as pessoas é a Surface Web, ou seja, onde as páginas indexadas estão disponibilizadas para os usuários, a internet na superfície. A menos conhecida por todos é a Deep Web, compreendida como a internet profunda, na qual, o conteúdo não está indexado e, portanto, não pode ser encontrado.

A Surface Web é percebida como a internet convencional. Nela, as páginas podem ser encontradas facilmente. Pode-se localizar um servidor de acesso ou uma

máquina a partir de uma Internet Protocol ou IP3. A Deep Web é composta por páginas que não são encontradas na Superface Web. Ela é conhecida como o submundo virtual ou internet secreta e é composta por um conjunto de sites, comunidades e fóruns não identificados precisamente por navegador, tornando, assim, o rastreamento do IP do usuário praticamente impossível. (ANDRADE, 2015).

A Deep Web ou Dark Web é a parte sombria do mundo virtual. Ela armazena conteúdos de forma sigilosa, em geral, conteúdos secretos. É na Deep Web que os crimes materializados na Superface Web são pensados e preparados, pois esta internet possui recursos importantes como o levantamento dos dados das potenciais vítimas. Na Deep Web ou Dark Web podem-se encontrar materiais proibidos e informações e diversos conteúdos ilegais. Ela também favorece a prática de contrabando, comércio ilegal de armas de fogo, invasões de privacidade, falsificações, comércio de loteriais, lavagem de dinheiro, tráfico, terrorismo, tortura real de animais, divulgação e contratação de sexo e pornografia, turismo sexual, contratação de assassinos, crimes contra a liberdade sexual, dentre outros tipos de crimes. Todas as possibilidades de prática criminosa são tratadas atrevés de fóruns ou chats e via sites. (VIGNOLI; MONTEIRO, 2016)

A todo instante, as pessoas podem receber e-mails suspeitos; SMS com informações fake de que a pessoa ganhou alguma promoção da qual ela sequer participou; e-mail solicitando atualização de dados de uma instituição financeira quando a pessoa nem mesmo possui conta nela e, tantos outros tipos de e-mails duvidosos solicitando para clicar em links. Isso é algo que acontece com todo indivíduo que utiliza a Internet por meio de celulares, computadores, notebooks, tablets, etc., que está conectado o tempo todo na rede acessando redes sociais, sites, plataformas e outros. (SILVA, 2021)
Qualquer atividade que tem como ferramenta a rede de computadores ou um computador, se constitui como base de ataque ou meio de crime caracterizado como cibercrime. Essas atividades também são conhecidas como crime digital, crime virtual, crimes eletrônicos ou crime informático. (CASSANTI, 2014)

Os cibercriminosos, sem serem encontrados ou conhecidos, ainda continuam tentando se apropriar de dados pessoas de suas vítimas, roubar e praticar delitos. A

plataforma Consumidor.gov.br apresentou dados que confirmaram o aumento no número de consumidores que tiveram seus dados financeiros ou pessoais consultados, repassados sem autorização, coletados e publicados ilicitamente no ano de 2021. Segundo a plataforma esse número mais que dobrou em relação ao ano de 2020. (SILVA, 2021)

A fraude por meio do envio de e-mail e redes sociais consiste no tipo de golpe mais aplicado com o uso da Internet. Entretanto, ocorrem também o uso indevido de identidade e de informações pessoais, roubo, roubo de informações financeiras às quais terão seus dados vendidos, extorsão, clonagem de cartões, espionagem, invasão de servidores de empresas e órgãos federais, bem como suas autarquias, estelionato, dentre outros. (SILVA, 2021)

De acordo com os dados do DFNDR Lab, que é o laboratório especializado em crimes virtuais, no ano de 2018 ocorreram somente no primeiro trimestre, mais de 56 milhões de tentativas de golpes que usaram links maliciosos. Isso equivale a mais de 26 mil tentativas de fraude por dia e 620 por hora. O phishing que significa ‘pescar’, consiste no golte delituoso mais comum e tem como objetivo roubar dados das vítimas como, identidade, contas bancárias, códigos de segurança e senhas. A tabela abaixo traz uma lista de phishing utilizados para a prática de fraudes.

Tabela 1 – Lista de Phishing Utilizados

PISHING	CARACTERIZAÇÃO
Blind Phishing	É o mais comum de todos. Ele ocorre pelo disparo de e-mails em massa. Neste tipo de phishing, o criminoso conta com a ingenuidade e desconhecimento de suas vítimas desse tipo de crime na Internet. No e-mail consta um link ou anexo tendencioso para que a vítima baixe um vírus em seu dispositivo.
Smishing	É realizado por meio do envio de disparos de SMS para celulares. Em geral, consistem em mensagens com informações de que a vítima possui dívidas ou que tenha ganho em um sorteio inesperado, o que pode fazer com que a vítima tome uma decisão

	imediata e caia no golpe.
Scam	Implicam em tentativas através de arquivos ou links contaminados. Neste caso, os criminosos buscam captar informações acerca das vítimas. O contato ocorre através de telefone, e-mail, pelas redes sociais ou SMS.
Clone Phishing	É responsável pela clonagem de um site original com o intuito de atrair e induzir a vítima a se comportar como se estivesse em um ambiente seguro.
Spear Phishing	Consiste no ataque direcionado para uma pessoa ou grupo específico. Seu objetivo é acessar informações sigilosas de um banco de dados também específico, financeiros ou arquivos confidenciais.
Whalling	Esse Phishing tem como principal alvo, executivos de cargos estratégicos e empresários para obter dados confidenciais.
Vishing	Mecanismo de voz usado para aplicar golpes na Internet. Cria-se uma sensação de urgência por meio de chamada de voz para que, desse modo, a vítima forneça informações e tome medidas rapidamente.
Pharming	Através dele, um site legítimo pode ser manipulado para que os usuários sejam direcionados para outro site podendo instalar softwares maliciosos. É capaz de coletar dados como informações financeiras e senhas bancárias.

Fonte: adaptado de SILVA (2021, p. 8-9)

Até o presente momento, abordou-se o conceito de crimes cibernéticos, apontando diferentes pontos de vista, mas que, todos possuem como ponto em comum, que os crimes praticados utilizando a Internet como ferramenta são os mesmos que os criminosos praticam no mundo real e, embora seja de difícil combate, os crimes virtuais não estão imunes aos rigores da lei.

Diversos são os crimes virtuais, tanto no que tange à honra de uma pessoa como de aspecto financeiro. No entanto, o foco central deste trabalho é o crime de estelionato virtual, tema a ser discutido na próxima seção.

2 O ORDENAMENTO JURÍDICO E O CRIME CIBERNÉTICO

No capítulo anterior ficou evidenciado em que momento o crime de estelionato é consumado, isto é, quando um indivíduo, com o objetivo de obter vantagem ilícita para ele ou para outros, usa como meios a fraude, artifícios ardis para induzir uma vítima ou fazer com que ela se mantenha em um erro gerando-lhe prejuízo.

Outro ponto evidenciado no capítulo anterior é a definição de crime virtual, sobre a qual há unanimidade em apresentar que o crime virtual é aquele praticado no ambiente virtual e utiliza o acesso à rede (Internet) e equipamentos eletrônicos. Portanto, o crime de estelionato virtual consiste no tipo de crime em que uma pessoa usa equipamentos tecnológicos, bem como, o acesso à Internet para pratica-lo em seu próprio benefício, de outras pessoas e causam prejuízo às suas vítimas. No crime de estelionato, o criminoso induz ou mantem a vitima ao erro e, para tal, usa, para obter vantagem ilícita, qualquer meio fraudulento.

2.1 DOS CRIMINOSOS E VÍTIMAS DO ESTELIONATO VIRTUAL

No ambiente virtual, em geral, a prática do crime de estelionato é realizada por indivíduos que possuem notável conhecimento em informática. Estes criminosos podem agir de modos diversos, mas, sua preferência é arriscar-se no mundo dos crimes virtuais, no qual, podem prejudicar e iludir pessoas reais para obterem vantagens ilícitas por meio dessa técnica. O que difere o estelionato real do virtual é o modus operandi utilizado, pois no primeiro caso se pratica tal crime em meio físico e o segundo no ambiente virtual. (FEITOZA, 2012)

O sujeito ativo do estelionato pode ser qualquer pessoa, em razão do fato de que este tipo de crime é muito comum e não exige qualquer tipo de condição especial do agente ou qualidade. O sujeito passivo também será comum, pois qualquer cidadão está propenso a sofrer um desfalque patrimonial através de fraudes empreendidas por um criminoso. Vale destacar que a vítima precisa possuir capacidade de ser iludida, pois, caso contrário, o delito de estelionato não ocorrerá e o agente do estelionato deverá ser julgado por incurso no art. 173 do Código Penal, ou seja, delito de abuso de incapaz. (CUNHA, 2019)

No caso da vítima, ela deverá ser determinada, considerando que, caso venha a ser incerta, fala-se do crime previsto no art. 2º, XI, da Lei 1.521/1951, por exemplo. É importante salientar que os estelionatários são astutos e grandes sedutores, possuem excelente vocabulário e boa aparência, se favorecem de argumentos capazes de convencer pessoas de todas as idades, escolaridade e grupos sociais em geral. Os criminosos não atuam sozinhos e, para que seja configurado como crime de estelionato, a vítima deve entregar espontaneamente a vantagem ao criminoso, pois, do contrário, os crimes seriam outros, como extorsão ou roubo. (HERTES, 2012)

Para a configuração do delito, é totalmente necessária e ativa a participação da vítima. Na maioria dos casos, a participação da vítima é de boa-fé e a pessoa é considerada do bem que foi enganada. Porém, há casos em que, posteriormente à realização das negociações, o resultado concreto ou pretendido por parte da vítima, também pode ser imoral ou ilícito. Nestas situações também se configura o crime de estelionato, pois vale destacar que no direito brasileiro há duas correntes que debatem a temática. (CAPEZ, 2020)

Doutrinadores como Nelson Hungria e Rogério Greco defendem a primeira corrente que entende que quando há o desejo de vantagem ilícita de ambas as partes, se constitui como fraude bilateral e, desse modo, não há crime. A justificativa para esse entendimento é o fato de que seus defensores têm como ponto de partida a ideia de que o resguardo do patrimônio somente pode ocorrer quando ele é usado para fins legítimos. Rogério Sanches Cunha e Bento de Faria são defensores da segunda corrente que também se configura como sendo majoritária na Doutrina. Essa corrente tem o entendimento de que o crime se constitui havendo ou não a boa-fé da vítima, pois a boa-fé não se configura como elemento subjetivo do dolo e do tipo do estelionatário, independe da intenção ou não da vítima e, portanto, não pode ser descartado. (CAPEZ, 2020)

2.2 PROJETOS DE LEI ACERCA DOS CRIMES CIBERNÉTICOS

O estelionato virtual é algo recente no ambiente dos tribunais brasileiros e dentro do próprio Estado, entretanto, carece de especial atenção em virtude da modernização e popularização da Internet que, a cada dia, adquire milhares de usuários novos diariamente. Assim sendo, o estelionato digital é um tipo de crime recente debatido nos tribunais e Estado brasileiros. (FEITOZA, 2012)

Muitas são as dificuldades da Polícia, Poder Judiciário e Ministério Público no sentido de punir os agentes que praticam crimes cibernéticos, o que pode levar para uma sensação de impunidade que, consequentemente, permitem que as pessoas relacionem essa impunidade à inexistência de leis específicas para o trato dos cybercrimes. (CRUZ; RODRIGUES, 2018)

Conforme já dito anteriormente, o crime de estelionato virtual carece maior atenção por parte dos legisladores, especialmente, em razão de este tipo de crime provocar grande impacto na sociedade e, portanto, não se pode mais retardar os projetos em tramitação. É fato concreto que, a cada dia, aumentam os casos de pessoas vítimas e presas fáceis para os criminosos cybernéticos que se aproveitam da inexistência de uma lei regulamentadora. (OLIVEIRA, 2020)

O estelionato virtual se insere em alguns projetos de lei para tipificar as condutas e puni-las. O projeto de lei e seu substitutivo ao PLS/2000, PLC 173/2000 e PLC 89/2003 buscam alterar a lei e abre espaço para a inclusão de um parágrafo segundo ao art. 171 do Código Penal. Este parágrafo define o estelionato virtual e o modo como deveria ser punido e aumenta a pena para este crime. (FEITOZA, 2012)

Considera-se causa para o aumento da pena para quem pratica o crime de estelionato virtual, o uso de meios de tecnologia da informação para essa prática. Destaca-se que este crime consistiu em tema de três projetos de lei com o objetivo de tipificar esta e outras condutas, bem como, puni-las de modo correto. O Projeto de Lei do Senado nº 76/2000, Projeto de Lei do Senado nº 1372000 e Projeto de Lei da Câmara nº 89/2003. Aprovada a redação final do PLC nº 89/2003 foram reatados prejudicados os Projetos de Lei do Senado nº 76 e nº 137, ambos os projetos referentes ao ano 2000 que foram arquivados em setembro de 2008. (OLIVEIRA, 2020)

No que tange ao Projeto de Lei sobrevivente, sua tramitação está encerrada e transformada em norma jurídica com veto parcial em setembro de 2014 e foi encaminhada para a secretaria de arquivo em 18 de setembro de 2014. Verifica-se que, apesar das tentativas de tipificar a conduta de estelionato virtual especificamente, o texto do Código Penal continuou inalterado e, portanto, não houve êxito destas tentativas. (OLIVEIRA, 2020)

No ano de 2020, foi enviado para apreciação do Plenário da Câmara dos Deputados o Projeto de Lei nº 3.376/2020, de autoria dos senhores Sanderso e Major Fabiana. O referido projeto altera o Decreto-Lei nº 2.848 de 7 de dezembro de 1940 no sentido de estabelecer majorante para o crime de estelionato virtual.

> **Art. 1º** Esta Lei altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940, para estabelecer majorante para o crime de estelionato virtual. Art. 2º O art. 171 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940, passa a vigorar acrescido do seguinte parágrafo:
>
> "Art.171…….....
> .
>
> **Estelionato virtual**
> §6º Aplica-se pena em dobro se o crime for cometido mediante a invasão, adulteração ou clonagem de aplicativo de mensagens instantâneas e chamadas de voz para smartphones ou com o emprego da rede de computadores, dispositivo de comunicação ou sistema informatizado." (NR)
> Art. 3º Esta Lei entra em vigor na data de sua publicação. (BRASIL,

A justificativa para a aprovação do Projeto de Lei nº 3.376/2020 é o seu objetivo que consiste no estabelecimento de majorante para o crime de estelionato virtual, em razão do uso cada vez mais diversificado e intenso da Internet que abre portas para a prática de novos tipos de fraudes perpretadas por criminosos golpistas com intuito de obter vantagem ilícita causando prejuízo alheio. Daí a emergência da aprovação do referido projeto.

2.3 NOVOS CRIMES E APLICAÇÃO DA LEGISLAÇÃO AO ESTELIONATO VIRTUAL

O crime de estelionato é tipificado no art. 171 desde a entrada em vigência do Código Penal em 7 de dezembro de 1940. O estelionato era classificado como crime de ação penal pública incondicionada, ou seja, posterior à sua consumação,

dispensava qualquer manifestação da vítima de querer ou não a punição do agente infrator, pois cabia ao Ministério Público o juízo de reprovação após investigações e ingresso da denúncia criminal em desfavor do suposto criminoso. (DINIZ, CARDOSO, PUGLIA, 2022)

A Lei nº 13.964/2019 ou “pacote anticrime” (grifo do autor) trouxe diversas mudanças na legislação processual penal, além de leis extravagantes. O Código Penal teve parte efetuada por mudanças importantes no que tange à ação penal do crime de estelionato. Sua classificaçaõ agora é de crime de ação penal pública que está condicionada à representação da vítima. Isso significa que, mesmo estando ainda a realização das investigações necessárias à cargo da polícia e de o Ministério Público ser ainda o responsável pelo oferecimento da denúncia e condução dos atos prcessuais, a provocação do juízo criminal somente acontecerá caso a vítima demonstre formalmente o desejo de representação contra o autor do crime. Tal mudança implica em consequências jurídicas extremamente relevantes e que deverão ser debatidas em momento oportuno. (DINIZ, CARDOSO, PUGLIA, 2022, p. 10).

A Lei nº 14.155/2021 foi sancionada a partir da necessidade de endurecimento das penas e tornar a lei aplicável em mais casos tipificados. A lei trouxe consigo maior endurecimento das pensas em seus artigos. O art. 154-A dispõe como crime de estelionato virtual invadir dispositivo informático de uso alheio, independente de estar conectado ou não à rede de computadores com a finalidade de obter, adulterar ou destruir informações ou dados sem a expressa autorização ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obtenção de vantagem ilícita. (SILVA, 2021, p. 12)

O § 4º - B estabelece a pena de privação da liberdade de 04 a 08 anos, além de multa, caso o furto mediante fraude for praticado com o uso de dispositivo informático ou eletrônico, conectado ou não à rede de computadores, independente da presença ou não da violação de mecanismo se segurança ou uso de programa malicioso ou outro meio qualquer fraudulento análogo. (SILVA, 2021, p. 12)

O § 4º - C, I, aumenta de 1/3 a 2/3 se o crime for praticado mediante o uso de servidor mantido fora do território nacional; II, aumenta de 1/3 ao dobro se o crime

for pratica contra vulnerável ou idoso. A pena é de reclusão de 1 a 4 anos e multa. O § 2º aumenta a pena de 1/3 a 2/3 se houver prejuízo econômico resultante da invasão e pena de reclusão de 2 a 5 anos e multa. As mudanças tornaram a Lei de violação de dispositivo informático mais duras tanto na definição de crime, fraude eletrônica e estelionato como as suas penalidades. (SILVA, 2021, p. 12)

> **Fraude eletrônica**
>
> § 2º-A. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo. § 2º-B. A pena prevista no § 2º-A deste artigo, considerada a relevância do resultado gravoso, aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional. Estelionato contra idoso ou vulnerável § 4º A pena aumenta-se de 1/3 (um terço) ao dobro, se o crime é cometido contra idoso ou vulnerável, considerada a relevância do resultado gravoso.
>
> **Art. 2º** O art. 70 do Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), passa a vigorar acrescido do seguinte § 4º: § 4º Nos crimes previstos no art. 171 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), quando praticados mediante depósito, mediante emissão de cheques sem suficiente provisão de fundos em poder do sacado ou com o pagamento frustrado ou mediante transferência de valores, a competência será definida pelo local do domicílio da vítima, e, em caso de pluralidade de vítimas, a competência firmar-se-á pela prevenção.” (NR) (SILVA, 2021, p. 12)

Punir com maior rigor os crimes cibernéticos, nos quais, os criminosos usam a Internet para aplicar golpes, extorquir, roubar, se apropriar de informações alheias contra usuários da rede é a proposta de modificação da lei. É de fundamental importância essa alteração, considerando que ocorreu um exorbitante aumento no crescimento das invasões e golpes utilizando a Internet. Portanto, a mudança no ordenamento jurídico é entendida como sendo positiva, em razão do fato da pena de reclusão de 4 a 8 anos e o aumento de 1/3 ao dobro da pena para o crime de estelionato virtual quando praticado contra vulnerável ou idoso. (SILVA, 2021)

No dia 23 de agosto de 2023, a Comissão de Constituição e Justiça (CCJ) aprovou o Projeto de Lei que aumenta a pena para estelionato prevendo novas formas do crime. O Projeto de Lei 2.254/2022 já tinha sido aprovado pela Câmara dos Deçputados e, atualmente, deverá ser analisado pelo Plenário do Senado. O

senador Plínio Valério (PSDB-AM) votou favoravelmente e o referido projeto inclui também no Código Penal variações acerca deste tipo penal, como, por exemplo, o estelionato sentimental crime ocorrido quando a vítima é enganada com promessas afetivas e induzida a entregar bens ao agente criminoso. (AGÊNCIA DO SENADO, 2023)

Como já muito mencionado, o crime de estelionato consiste na conduta típica de induzir a vitima ao erro através de artifícios para alcançar seus objetivos, ou seja, obter vantagem ilícita para si próprio ou para outras pessoas. É entendido como crime patrimonial aquele em que não se utiliza a grave ameaça ou violência, mas, a fraude para obter a vantagem ilícita, principalmente, a financeira. Desse modo, o golpe do amor ou estelionato sentimental se configura quando o estelionato é construído por meio de uma relação afetiva com a vítima com o objetivo de conquistar a confiança e, posteriormente, tirar o proveito financeiro objetivado. (GONÇALVES, 2021)

O estelionato sentimental também é chamado de *scammer* sentimental. *Scammer* consiste em uma palavra de origem inglesa que descreve um conjunto de golpistas virtuais que se inserem em grupos organizados através da Internet e que têm por finalidade extorquir e enganar vítimas que, em geral, são mulheres, principalmente as que possuem carência afetiva abalada, vulneráveis ao convencimento e acalentamento por meio de conversas. (FILHO; KHALIL, 2021)

Primeiramente, o criminoso trabalha a questão emocional identificando o estado frágil da vítima, não se limitando a conversas de cunho pornográfico ou meramente sexual. Desse modo, por meio da confiança estabelecida entre o criminoso, a mulher e até mesmo sua família e amigos, o golpista aplica o golpe financeiro. Assim, pode-se afirmar que o objetivo do golpista é obter por meio do amor da vítima e até mesmo promessa de namoro ou casamento, vantagem financeira ilícita, o que gera prejuízo à vítima, pois as promessas são falsas. O criminosos convence sua vítima a lhe doar presentes, dinheiro e até criptomoedas, principal moeda na Deep Web. (GONÇALVES, 2021)

Outro ponto destacável é a incorrência de delito da mesma gravidade para quem permitir o uso de sua conta bancária para a aplicação de golpes contra outrem. O texto modifica o Código Penal para poder fazer essas alterações. De acordo com o texto, a pena do crime de estelionato e seus novos formatos passa a ser de 2 a 6 anos de privação de liberdade e multa. Até o momento, a pena de reclusão é de 1 a 5 anos e multa. A pena aumenta quando há a utilização das redes sociais, contatos telefônicos e outros meios fraudulentos que sejam semelhantes aos já citados. Desse modo, a pena de reclusão será de 4 a 8 anos acrescida de multa. (AGÊNCIA DO SENADO, 2023)

Os senadores Fabiano Contarato (PT – ES) e Rogério Carvalho (PT – SE) se posicionaram contra a medida argumentando que o aumento da pena conduz a sociedade para a sensação equivocada que os parlamentares estão fazendo alguma coisa de fato concreta acerca do combate aos crimes virtuais. Já para os senadores Eduardo Girão (Novo – CE), Marcos Rogério (PL – RO) e Jorge Seif (PL – SC) pontuam que a ação de infratores deve se dissuadir atravé da rigidez da pena, mas, a mudança precisa ser acompanhada por um sistema apropriado. Argumentam eles que não basta apenas endurecer penalmente que se alcançará a redução da criminalidade, mas sim, a eficiência do sistema de Justiça. Em seu relatório, o senador Plínio retirou do rol de crimes hediondos a inclusão de estelionato contra idosos. (AGÊNCIA DO SENADO, 2023)

Em casos nos quais as vítimas sejam idosas ou vulneráveis, o relator alterou o projeto para que, desse modo, fosse possível aumentar a pena de 1/3 para o dobre como já consta em lei atualmente. Já na proposta da Câmara dos Deputados, tal pena seria triplicada. O relator acatou a emenda de redação que os senadores Contarato e Alessandro Vieira (MDB – SE) no sentido de esclarecer como vulneráveis menores de 14 anos ou deficientes mentais ou acometidos de enfermidade que os incapacitam de discernir o fato ou oferecer resistência a ele. Se o crime for praticado contra entidade beneficiente ou pública, ocorrerá o aumento da pena de 1/3 para até 2/3. Se o prejuízo ocasionado pelo estelionato for entendido como vultoso, existe a possibilidade de aumentar a pena em até a metade. (AGÊNCIA DO SENADO, 2023)

As alterações ocorridas também são entendidas como positivas, pois o que se espera com elas é que o crime de estelionato virtual seja inibido e, desse modo, o uso da Internet seja mais seguro. Compreende-se que isso somente pode acontecer mediante a aplicação de penas mais endurecidas para quem pratica crimes utilizando a rede mundial de computadores.

3 IMPLICAÇÕES JURÍDICAS DO CRIME DE ESTELIONATO VIRTUAL

Nesta seção aborda-se a questão das implicações jurídicas do crime de estelionato virtual. Vale destacar que se considera relevante as alterações pelas quais o crime de estelionato como um todo passou com a Lei nº 14.155/2021, a competência das investigações e julgamento dos casos de estelionato e, por fim, as adequações necessárias para prevenção e combate ao crime virtual no ordenamento jurídico brasileiro.

3.1 ALTERAÇÕES SOFRIDAS PELO CRIME DE ESTELIONATO

Uma importante alteração foi sofrida recentemente pelo crime de estelionato. A Lei nº 14.155 de 27 de maio de 2021 alterou e acrescentou alguns parágrafos no art. 171 do Código Penal. Foram incluídos os §§ 2º - A e 2º - B que versam sobre a fraude eletrônica. (SILVA; SANTOS, 2021)

> § 2º-A. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo. § 2º-B. A pena prevista no § 2º-A deste artigo, considerada a relevância do resultado gravoso, aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional (BRASIL, 2021).

No que tange à fraude eletrônica na forma qualificada, o § 2º-A dispõe de uma qualificadora do crime de estelionato quando praticado não presencialmente. Neste

caso, o agente usa informações que constam nas redes sociais, emails, contatos telefônicos à vítima. O texto do dispositivo legal também abre caminhos para a possibilidade da prática do estelionato virtual mediante qualquer outro meio fraudulento análogo. (SILVA; SANTOS, 2021)

Como exemplos de fraude eletrônica na forma qualificada citam-se condutas criminosas utilizando as redes sociais onde o agente simula sorteios através destas redes com o objetivo de obter os dados pessoais das vítimas e, desse modo, envia mensagens por meio do WhatsApp como se fosse um familiar ou amigo da vítima. Dessa maneira, o agente criminoso convence a vítima a efetuar depósitos bancários em contas do mesmo. É muito comum que esses agentes liguem para a vítima com o objetivo de induzi-la ao erro relatando suposto sequestro. (SILVA; SANTOS, 2021)

Outra forma como se apresenta a prática do estelionato virtual é a que usa o envio de e-mails ou outro meio qualquer fraudulento análogo, os criminosos usam emblemas e imagens de instituições financeiras e lojas para obter dados pessoais das vítimas, o que inclui a obtenção de contas bancárias e senhas. (SILVA; SANTOS, 2021)

A Lei n°14.155/2021 incluiu no art. 171 do Código Penal o § 2º-B que trouxe consigo uma causa do aumento da pena de 1/3 para 2/3. A causa consiste em quando o crime é praticado com o uso de servidor estrangeiro e, portanto, a pena deve ser maior. Considera-se a importância do resultado gravoso para, assim, dosar a fração de aumento, considerando que existe grande dificuldade na localização e punição do agente criminoso. Em síntese, a fraude eletrônica na forma majorada consiste no crime praticado com o uso de um equipamento ou servidor cuja localização se encontra fora do território do Brasil. (SILVA; SANTOS, 2021)

Outra recente alteração trazida pela Lei n°14.155/2021foi o §4º do art. 171 do Código Penal. Tal dispositivo traz em seu texto o aumento da pena de 1/3 ao dobro quando o crime de estelionato for cometido contra vulnerável ou idoso. Neste caso, considera-se a importância do resultado gravoso. (BRASIL, 2021).

Houve alteração na fração do aumento da pena quando o estelionato é praticado contra idoso, o que se inclui também o vulnerável. Na redação anterior, o dispositivo legal dispunha a aplicação da pena em dobro quando o crime de estelionato era praticado contra pessoa com idade igual ou acima de 60 anos, considerado idoso. A alteração trazida pela nova lei prevê o aumento da pena de 1/3 ao dobro, abrangendo também o vulnerável e considerando a relevância do resultado gravoso na aplicação da fração do aumento da pena. (SILVA; SANTOS, 2021)

Uma crítica que se faz a essa alteração que a nova norma traz no que diz respeito ao crime cometido contra o idoso é sobre o favorecimento que esta alteração possibilita ao agente criminoso, pois a fração a ser aplicada deverá obedecer ao critério da gravidade do resultado. Já no texto anterior, em qualquer caso, a fração de aumento da pena seria o dobro. A previsão é de que a nova Lei poderá sofrer um retrocesso em benefício do condenado ou acusado.

3.2 DA COMPETÊNCIA DA INVESTIGAÇÃO E JULGAMENTO DO CRIME DE ESTELIONATO

Por não possuir fronteiras, desde o princípio, a Internet foi arquitetada para que, em qualquer parte do planeta, as pessoas pudessem acessa-la, significando a criação de uma realidade virtual isenta de barreiras físicas, isto é, das delimitações territoriais. Neste sentido, ocorreu a multiplicação, por meio desta ferramenta, das relações humanas. Foi criada para não ter fronteiras e ser global, no entanto, esbarra nas diferentes culturas que se refletem nas diferentes legislações, pois um mesmo conteúdo pode ser tratado de modo diverso em países diferentes, pode ser tratado como ilegal ou legal. (DOMINGOS; RÖDER, 2018 apud OLIVEIRA 2020)

O funcionamento correto dessa rede obedece a critérios organizacionais matemáticos, que permitem a fluidez dessa estrutura. Isso significa que as empresas provedoras de internet detêm as informações referentes aos passos que os usuários percorrem na rede: acessos, postagens e comunicações. São essas informações que em geral permitem, de forma precisa, desvendar um crime cibernético ou obter uma prova digital para elucidar um crime real. O que tem

aturdido o mundo jurídico é a obtenção dessas informações, desses dados que consubstanciam a prova digital. (DOMINGOS; RÖDER, 2018 apud OLIVEIRA 2020)

No tocante aos delitos virtuais, investigá-los consiste em uma tarefa muito complexa, tendo em vista que aumenta a dificuldade em precisar a localidade onde estão as provas e, desse modo, coletá-las. Apesar de parecer uma rede etérea, o funcionamento da Internet exige uma infraestrutura bem real, ou seja, para o acesso a uma comunidade virtual, precisa-se de provedores de conexão à rede. Estes provedores fornecem ao usuário um número de IP (Internet Protocol) para que ele possa navegar no ambiente virtual. Depende da estrutura que os provedores de aplicações de Internet disponibilizam, o conteúdo a ser acessado e as plataformas possibilitadoras da produção, por parte do próprio usuário, de conteúdo. (DOMINGOS; RÖDER, 2018 apud OLIVEIRA 2020)

A partir da publicação da Lei nº 14.155/2021, a competência para investigação e julgamento dos crimes de estelionato passou a ser regida pelo local de domicílio da vítima. Anterior à nova norma, a competência era regida pelo local em que o estelionato ou tentado se consumou, isto é, onde o último ato de execução foi praticado consoante o caput do art. 70 do Código de Processo Penal. (GUEIROS; NUNES, 2021)

Anterior à nova lei, havia divergência jurisprudencial nos tribunais. Isso ocorria em virtude do fato de que para a verificação da competência era necessário realizar uma análise da consumação do estelionato. Entretanto, a consumação do delito de estelionato dependerá da maneira como é praticada a infração penal. Com o novo § 4º que foi incluído no art. 70 do CPP, essas divergências caem por terra, mediante a manifestação clara do legislador de que a competência será regida pelo local de domicílio da vítima. (GUEIROS; NUNES, 2021)

É relevante ressaltar que casos nos quais o crime ocorreu antes da publicação da nova lei, mas, o processo penal ainda não tenha se iniciado, a competência ainda permanecerá nos moldes que o STJ fixou.

Leciona o professor Aury Lopes Jr que é no momento da prática do delito que

> nasce a garantia do juiz natural e não quando o processo tem seu início. Não é possível manipular os critérios da competência nem definir, posterior ao fato, qual será o juiz da causa. Isso significa que, mediante as garantias da imparcialidade do julgador e do juiz natural, não há possibilidade de alterar os critérios da competência após o fato, pois pode implicar na pena de se criar tribunais de exceção ou *post factum*. (GUEIROS; NUNES, 2021)

3.3 ADEQUAÇÕES NECESSÁRIAS NO ORDENAMENTO JURÍDICO BRASILEIRO NO QUE TANGE AO CRIME DE ESTELIONATO VIRTUAL

Destaca-se, neste ponto, como o ordenamento jurídico brasileiro trata o crime de estelionato virtual. Para tanto, recorre-se ao texto do art. 171 do Código Penal, já que o mesmo não menciona o uso da Internet e, desse modo, induz muitas pessoas a crerem na impunidade deste crime, pois não há uma previsão normativa para ele. (OLIVEIRA, 2020)

Quando infratores criam e-mails, links, dentre outros, falsos, tendo por objetivo o anonimato prometem fazer alguma coisa que sabem que não irão fazer, mas, prometem em troca de alguma vantagem que, na maioria das vezes, é pecuniária, o crime de estelionato virtual acontece. Assim sendo, a consumação do estelionato virtual acontece quando o criminoso induz a vítima, por meio do uso de meios digitais, se aproveitando das brechas que tais meios fornecem para obtenção de vantagens ilícitas. (ATAIDE, 2017)

Atualmente, a Internet possibilita a simplificação de tarefas como, por exemplo, comprar algo. Nos dias de hoje, se pode, em poucos cliques, realizar compras e, inclusive, buscar por produtos com valores menores. No entanto, não há total segurança neste espaço, pois existem pessoas mal-intencionadas esperando a vítima certa para obter vantagem ilícita. (OLIVEIRA, 2020)

Embora, anteriormente, não houvesse uma lei específica para combater e punir crimes cibernéticos, o Judiciário aplicava o Código Penal e o Código Civil com o fim de combater e punir este tipo de crime. Utilizavam-se leis específicas como a Lei 9.296, norma que tipifica o crime nas interceptações de comunicação nos sistema de

informática, telemática e telefonia, bem como, utilizava-se também a Lei 9.609, a qual trata acerca da propriedade intelectual de programas de computadores. (SILVA, 2021)

No ano de 2012, a legislação referente aos crimes cibernéticos evoluiu, a partir do caso da atriz Carolina Dieckman que foi vítima de ataque cibercriminoso, pois um hacker invadiu seu computador e teve acesso a fotos íntimas da atriz. Essas fotos foram divulgadas sem seu consentimento, o que lhe causou prejuízo psicológico em razão das suas imagens terem ganho grande repercussão na mídia. Assim, foi aprovada a Lei 12.737/2012 ou Lei Carolina Dieckman e, desse modo, o crime de invasão de dispositivo ficou tipificado. Foi acrescido no Decreto-Lei 2.848 essa tipificação nos artigos 154-A e 154-B do Código Processual Penal. (SILVA, 2021)

CP - Decreto Lei nº 2.848 de 07 de Dezembro de 1940

Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita: (Redação dada pela Lei nº 14.155, de 2021)
Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa. (Redação dada pela Lei nº 14.155, de 2021)
§ 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput. (Incluído pela Lei nº 12.737, de 2012) Vigência
~~**§ 2º** Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico. (Incluído pela Lei nº 12.737, de 2012) Vigência~~
(Revogado)
§ 2º Aumenta-se a pena de 1/3 (um terço) a 2/3 (dois terços) se da invasão resulta prejuízo econômico. (Redação dada pela Lei nº 14.155, de 2021)
§ 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido: (Incluído pela Lei nº 12.737, de 2012) Vigência Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave. (Incluído pela Lei nº 12.737, de 2012) Vigência Pena – reclusão, de 2 (dois) a 5 (cinco) anos, e multa. (Redação dada pela Lei nº 14.155, de 2021)
§ 4º Na hipótese do § 3o, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidas. (Incluído pela Lei nº 12.737, de 2012) Vigência
§ 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra: (Incluído pela Lei nº 12.737, de 2012) Vigência
I - Presidente da República, governadores e prefeitos; (Incluído pela Lei nº 12.737, de 2012) Vigência
II - Presidente do Supremo Tribunal Federal; (Incluído pela Lei nº 12.737, de 2012) Vigência

> **III** - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou (Incluído pela Lei nº 12.737, de 2012) Vigência
> **IV** - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal. (Incluído pela Lei nº 12.737, de 2012) Vigência Ação penal (Incluído pela Lei nº 12.737, de 2012) Vigência
> **Art. 154**-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime e 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. (Incluído pela Lei nº 12.737, de 2012) Vigência. (BRASIL, 1940)

Uma das maiores empresas de segurança de TI no mundo, a Kaspersky Lab, informou que o número de crimes cibernéticos diminuiu no ano de 2013 após a implementação da Lei 12.737/2012, ou seja, um total de 352.925 incidentes. No entanto, no ano de 2014 os incidentes dispararam com 1.047.031 a mais. A Kaspersky Lab informou também ter registrado o bloqueio de um número maior que 6,2 bilhões de ataques maliciosos em dispositivos móveis e computadores através de seus antivírus, ou seja, um bilhão a mais do que no ano de 2013. Isso demonstra que ainda necessita de aperfeiçoamento a tipificação do crime virtual. (SILVA, 2021)

Pode-se verificar no art. 5º da Constituição Federal, o tratamento das garantias de inviolabilidade da imagem, da honra, da privacidade e da intimidade da pessoa no mundo real. Reconhece-se que a Lei 12.965/2014 que é conhecida como Marco Civil da Internet também assegura essas garantias estabelecendo direitos e deveres, bem como, os princípios norteadores da utilização da Internet no Brasil.

> Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:
> I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;
> II - Proteção da privacidade;
> III - Proteção dos dados pessoais, na forma da lei;
> IV - Preservação e garantia da neutralidade de rede;
> V - Preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas; (BRASIL, 2014)

Desse modo, pode-se verificar que todos os usuários da Internet têm assegurados os princípios que norteiam as relações que acontecem na rede. São estes princípios que buscam garantir que não haja injustiças no contato entre as pessoas na Internet. Tais princípios sustentam a liberdade, o bom funcionamento do

serviço de Internet e a privacidade de seus usuários. (ALVES, 2020 apud GONÇALVES, 2021)

3.4 PREVENÇÃO E COMBATE AO CRIME DE ESTELIONATO VIRTUAL

A Internet oferece grandes facilidades para a prática do bem, no entanto, na mesma proporção, também surgem para a prática do mal. O anonimato que a rede proporciona se apresenta como algo fundamental e esse anonimato é uma dos principais desafios que emergiram em razão da popularização da Internet. É também uma das principais razões que embargam a reação efetiva das autoridades que buscam identificar o criminoso virtual. Esse embargo se apresenta em virtude da inscrição e atuação em provedores digitais usando dados falsos ou de outra pessoa ser algo fácil. (DINIZ, CARDOSO, PUGLIA, 2022)

A Lei nº 14.155/2021 alterou o Código Penal em várias partes como, ampliar o preceito secundário de determinados crimes quando observada a relação da sua prática com o uso ou auxílio específico da Internet e fatores que estão relacionados com as facilidades que a rede proporciona. A nova norma trata questões referentes a crimes de furto, do estelionato e da invasão de dispositivo de informática. As alterações trazidas pela nova lei são consideradas como de grande relevância, em razão do enorme crescimento dos golpes e invasões efetivados pela Internet. (DINIZ, CARDOSO, PUGLIA, 2022)

Apesar dos avanços, ainda há muito o que caminhar no sentido de combater as novas modalidades criminosas, complexas e carregadas de particularidades no seu *modus operandi*. É fundamental que a legislação também evolua constantemente e acompanhada de outros processos, que haja entendimento real do que vem a ser um crime virtual e suas peculiaridades. Essa compreensão e constante busca pela evolução da legislação são cruciais e muito necessárias na guerra contra a criminalidade virtual. (DINIZ, CARDOSO, PUGLIA, 2022)

> Ao se realizar uma análise básica do cenário jurídico criminal brasileiro atual, nota-se que é mais negócio para o criminoso praticar ilícitos por meio da internet (via anonimato) do que ir para as ruas e cometer assaltos. Isto porque, se o objetivo principal de quem comete crimes contra o patrimônio é, na maioria esmagadora das vezes, a vantagem econômica, para o

> criminoso é mais seguro e lucrativo cometer o delito de estelionato do que o de roubo. (DINIZ, CARDOSO, PUGLIA, 2022, p. 15)

Vale destacar que, além das vantagens apresentadas na citação anterior, o estelionato virtual possui pena mais branda, na maioria das vezes, em virtude da dificuldade de se identificar os autores na fase investigatória, que se torna um grande desafio para a solução do fato.

O ambiente virtual possibilita que os criminosos tenham alcance simultaneamente, a diversas vítimas e, desse modo, se constitui como o ambiente perfeito para se cometer crimes, especialmente, o estelionato virtual. Relevante se faz informar que as características da Internet permitem o desenvolvimento da comunicação e também para o crescimento de crimes de informática que são ancorados pela sensação de anonimato e impunidade. Isso porque no Brasil, no que tange à legislação acerca de crimes virtuais era norteada pela Lei nº 9.983/2000 que acrescentou poucos artigos ao Código Penal. (DAMÁSIO DE JESUS, 2016)

A Confederação Nacional de Dirigentes Logistas realizou uma pesquisa em junho do ano de 2021 e a referida pesquisa demonstrou um aumento potencial do quantitativo de golpes em compras realizadas no ambiente virtual, ou seja, pela Internet em comparaçao com o ano de 2019. Isso significa que a cada 10 pessoas, seis foram vítimas de algum tipo de fraude financeira por meio da Internet. Esse aumento também foi demonstrado pelo Serviço de Proteção ao Crédito – SPC/2021 que apresentou em seus dados um aumento de 28% nos crimes de estelionato virtual. Dentre os golpes mais comuns está a compra e o não recebimento do produto pago pela vítima. (DINIZ, CARDOSO, PUGLIA, 2022)

No que tange à prevenção e combate ao crime de estelionato virtual, verifica-se que as autoridades estão imbuídas na fiscalização do bom funcionamento da sociedade e também o controle, na medida em que observam a disseminação da criminalidade. É dever das autoridades, da legislação, jurisprudência e doutrina, criar e desenvolver planos estratégicos com o objetivo de minimizar a propagação destes crimes e seus impactos não somente nos indivíduos em particular, como também na sociedade como um todo. (DINIZ, CARDOSO, PUGLIA, 2022)

Pode-se trabalhar sob dois aspectos: o preventivo – o qual tem a capacidade de evitar que aconteça o crime e o repressivo – muito necessário quando a conduta criminosa está consumada. O significado da palavra prevenção consiste no conjunto de medidas necessárias para o enfrentamento de alguma situação no sentido de evitar um mal maior, isto é, são medidas preparatórios. No contexto jurídico, a prevenção pode ser definida como sendo um conjunto de maneiras que vão desde a fixação da competência de determinado órgão julgador até a consagração de um princípio. De qualquer forma, todas as maneiras possuem um mesmo sentido que é o de se antecipar ao futuro pensando e promovendo soluções para evitar desordem posterior. (DINIZ, CARDOSO, PUGLIA, 2022)

A prevenção no que se refere à prática de estelionato virtual se concretiza quando as soluções mais eficazes são encontradas para diminuir a consumação do mesmo. As notórios desafios que as autoridades encontram na investigação deste tipo de crime também consiste na principal arma para evitar que aconteça o crime. (DINIZ, CARDOSO, PUGLIA, 2022)

Em síntese, não basta somente promulgar leis em massa para responder aos acontecimentos externos e preveni-los. No entanto, tais leis são cruciais para a repressão quando já se consumou o crime. Deve-se entender que quando o crime já se consumou, os métodos usados para preveni-lo não foram adequados e suficientes para evitar a perpretação do delito. No entanto, não se pode desconsiderar que a prevenção consiste em uma resposta de toda a sociedade, incluindo o sistema e ógãos públicos pode ser mais eficaz no combate ao estelionato virtual.

CONCLUSÃO

Este estudo teve como principal objetivo investigar as implicações jurídicas do crime de estelionato virtual no Brasil. Pretendeu-se também conceituar crimes cibernéticos, especialmente, o estelionato virtual, bem como apresentar o perfil de criminosos e vítimas; analisar a legislação pertinente aos crimes cibernéticos e sua

aplicação no Brasil e; investigar as medidas de prevenção e punição ao crime de estelionato virtual de acordo com a legislação brasileira.

Trata-se de uma revisão integrativa de bibliografia estruturada em três seções, nas quais, a primeira aborda as definições dos crimes cibernéticos e do estelionato virtual, além de apresentar os tipos de crimes cibernéticos. A segunda seção trata do ordenamento jurídico e o crime cibernético apresentando os perfis de criminosos e vítimas do estelionato virtual, bem como, projetos de leis, novos crimes e a aplicação da legislação em relação ao estelionato virtual. A terceira e última seção demonstrou as implicações jurídicas do crime de estelionato virtual, as alterações no que diz respeito ao crime de estelionato virtual, a competência para investigar e julgar e, por fim, a questão da prevenção e combate ao crime de estelionato virtual.

Por meio deste estudo concluiu-se que a Internet é entendida como sendo um dos maiores avanços que o mundo conheceu, proporcionar diversas facilidades para o mundo globalizado, mas, também é inegável que, na mesma medida em que possui benefícios, ela traz problemas e desafios complexos e difíceis de transpor. Cada vez mais, cresce o número de usuários da rede, assim como, aumenta o número de crimes praticados com o uso de dispositivos de informática. Estes crimes estão ainda mais sofisticados, modernos e carregados de dificuldades no sentido de identificar os criminosos. Todos os dias, centenas de pessoas são vítimas de algum tipo de fraude, golpe, roubo, dentre outros, praticados por estelionatários virtuais.

A princípio o crime de estelionato se define como sendo toda ação praticada tendo por objetivo a obtenção de vantagem patrimonial gerando prejuízo à vítima e os intrumentos utilizados são o artifício ou qualquer outro meio fraudulento que conduza a vítima ao erro ou à mantê-lo. A distinção entre o crime praticado fisicamente e o virtual é o modus operandi, pois o crime virtual, em especial o estelionato virtual que é o foco central deste trabalho, é praticado no ambiente virtual, por meio da Internet e o uso de equipamentos tecnológicos que permitem o acesso à rede. Os criminosos criam perfis falsos, roubam dados da vítima, dados bancários, invadem aparelhos de celular, computadores, tablets, para acessar conteúdos de suas vítimas, dentre tantas outras formas de praticar crimes virtuais.

Vale destacar que nem sempre é considerado crime a criação de um perfil falso nas redes sociais, o que tipifica como crime é o objetivo do agente do delito ser de tirar proveito, principalmente, econômico de outras pessoas. O anonimato é uma importante ferramenta nas mãos do criminoso no ambiente virtual e a Internet favorece esse anonimato tornando a identificação dos agentes criminosos uma tarefa desafiadora.

A legislação brasileira não possuia uma legislação específica para tratar o crime de estelionato virtual, seguia o previsto no artigo 171 do Código Penal brasileiro. Entretanto, com o crescimento significativo do número de vítimas de crimes virtuais, especialmente, o estelionato fez emergir a necessidade da legislação também evoluir e avançar no sentido de prevenir e combater esse tipo de crime. O ponto de partida para essas mudanças e avanços foi a publicação da Lei 12.737/2012 ou Lei Carolina Dieckman que teve seu computador invadido e sua privacidade violada e o caso ganhou grande repercussão na mídia. A Lei 12.965/2014 entendida como Marco Civil da Internet que trouxe em seu texto a garantia dos direitos que já o eram no mundo real.

A Lei 14.155/21 trouxe alterações relevantes com maior endurecimento das penas e tipificando novos crimes como o estelionato contra vulnerável e idoso, o estelionato sentimental, a fraude eletrônica. A nova norma prevê penas mais severas e que podem ser aumentadas de reclusão, além de multa. Apesar dos avanços, o caminho para a prevenção e combate ao crime de estelionato virtual ou qualquer outro tipo de crime que usa os dispositivos de informática para sua consumação ainda é longo. Entretanto, esse caminho está sendo trilhado numa constante evolução da legislação, da doutrina e da jurisprudência no sentido de diminuir o número de casos de crimes virtuais, especialmente, o estelionato virtual no Brasil.

REFERÊNCIAS

ANDRADE, Leonardo. **Cybercrimes na deep web**: as dificuldades de determinação de autoria nos crimes virtuais. 2015. Disponível em: https://jus.com.br/artigos/39754/cybercrimes-na-deep-web-as-dificuldades-juridicas-de-determinacao-de-autoria-nos-crimes-virtuais Acesso em 19 mai 2023.

ANDREUCCI, Ricardo Antonio. **Manual de Direito Penal**. 10 ed. São Paulo: Saraiva, 2014.

ATAÍDE, Amanda Albuquerque de. **Crimes Virtuais**: uma análise da impunidade e dos danos causados às vítimas. Maceió, 2017. Disponível em:< http://www.faaiesa.edu.br/aluno/arquivos/tcc/tcc_amanda_ataide.pdf>. Acesso em: 11 ago. 2023

BITENCOURT, Cezar Roberto. **Penal Comentado**. 7 ed. São Paulo: Saraiva, 2012.

BRASIL. **DECRETO-LEI N° 2.848, DE 7 DE DEZEMBRO DE 1940**: Código Penal. Disponível em:< http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado .htm>. Acesso em 15 mar 2023.

BRASIL, Presidência da República. **Lei 12.965, de 23 de abril de 2014**. Disponível em https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm Acesso em 20 ago 2023.

BRASIL. Câmara dos Deputados. **PROJETO DE LEI Nº 3.376, DE 2020**. Disponível em https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1946850#:~:text=Trata%2Dse%20de%20projeto%20de,vantagem%20il%C3%ADcita%20em%20preju%C3%ADzo%20alheio. Acesso em 20 ago 2023.

BRASIL. **Lei nº 14.155, de 27 de maio de 2021**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019- 2022/2021/lei/L14155.htm. Acesso em 15 ago. 2023.

BRASIL. Agência do Senado. **CCJ aprova aumento de pena para estelionato e suas versões virtuais**. 2023. Disponível em https://www12.senado.leg.br/noticias/materias/2023/08/23/ccj-aprova-aumento-de-pena-para-estelionato-e-suas-versoes-virtuais Acesso em 21 ago 2023.

CAMPOS, Pedro Franco de [et al.]. **Direito penal aplicado**: parte geral e parte especial do Código Penal. - 6ª. Ed. – São Paulo: Saraiva, 2016.

CAPEZ, Fernando. **Curso de direito penal**: volume 2: parte especial: arts. 121 a 212. 20. ed. São Paulo: Saraiva Educação, 2020.

CASSANTI, Moisés de Oliveira. **Crimes virtuais, vítimas reais**. 1ª ed. Rio de Janeiro: Brasport, 2014, p.6.

CUNHA, Rogério Sanches. **Manual de direito penal**: parte especial (arts. 121 ao 361). 11. ed. rev., ampl. e atual. Salvador: JusPODIVM, 2019.

CRUZ, Diego; RODRIGUES, Juliana. **Crimes Cibernéticos e a Falsa Sensação de Impunidade**. 2018. Disponível em:< http://faef.revista.inf.br/imagens_arquivos/arquivos_destaque/iegWxiOtVJB1t5C_2019-2-28-16-36-0.pdf>. Acesso em 11 ago. 2023.

DINIZ, Felipe Ferreira; CARDOSO, Jacqueline Ribeiro; PUGLIA, Eduardo Henrique Pompeu. O crime de estelionato e suas implicações na era contemporânea: o constante crescimento dos golpes via Internet. **LIBERTAS DIREITO**, Belo Horizonte, v. 3, n.1, p. 1-34, jan./jul. 2022.

ESTRELA, Kilmara Batista. **Crimes digitais**. 2003. 56f. Trabalho de Conclusão de Curso (Bacharelado em Ciências Jurídicas e Sociais) – Direito, Centro de Ciências Jurídicas e Sociais, Universidade Federal de Campina Grande, Sousa, Paraíba, 2003. Disponível em: http://dspace.sti.ufcg.edu.br:8080/jspui/handle/riufcg/13373. Acesso em: 10 mai 2023.

FEITOZA, luis Guilherme de Matos. **Crimes Cibernéticos**: o Estelionato Virtual. Brasília, 2012. Disponível em:< https://egov.ufsc.br/portal/sites/default/files/crimes_ciberneticos_o_estelionato_virtual.pdf> Acesso em 11 ago. 2023.

FILHO. Edson Benedito Rondon; KHALIL, Karina Pimentel. **Scammers**: Estelionato Sentimental Na Internet. 2021. Disponível em: < file:///D:/Users/DELL/Downloads/397- Texto%20do%20Artigo-1169-1-10-20210524.pdf>. Acesso em 15 ago. 2023.

GONÇALVES, Dayane Maciel. **O canto da sereia** – da captação de vítimas de estelionato virtual por meio das redes sociais. Rubiataba/GO: Faculdade Evangélica de Rubiataba, 2021. Disponível em: http://repositorio.aee.edu.br/bitstream/aee/20162/1/2022%20-%20TCC%20-%20DAYANE%20MACIEL%20GON%C3%87ALVES.pdf Acesso em 15 mar 2023.

GRECO, Rogério. **Código Penal Comentado**. 5 ed. Rio de Janeiro: Impetus, 2011.

GUEIROS, Guilherme; NUNES, Elaine. **Lei dos "crimes cibernéticos" altera competência em caso de estelionato**. 2021. Disponível em https://www.conjur.com.br/2021-jun-04/opiniao-lei-crimes-ciberneticos-altera-competencia-estelionato Acesso em 21 ago 2023.

HERTES, Andrelise. **A (não) configuração do crime de estelionato diante da fraude ou torpeza bilateral**. Jus, 2012. Disponível em: https://jus.com.br/artigos/22442/a-nao-configuracao-do-crime-de-estelionatodiante-da-fraude-ou-torpezabilateral#:~:text=A%20boa%2Df%C3%A9%20da%20v%C3%ADtima,de%20que m%20concebe%20a%20fraude. Acesso em 15 ago. 2023.

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

MAUES, Gustavo Brandão Koury et. al. **Crimes Virtuais**: uma análise sobre a adequação da legislação penal brasileira. 2018. Disponível em:<

https://www.unirios.edu.br/revistarios/media/revistas/2018/18/crimes_virtuais.pdf>. Acesso em: 18 abr 2023.

OLIVEIRA, Hesrom César de. Cybercrimes: Do Estelionato Virtual. **TCC Direito**. Rubiataba/GO: Faculdade Evangélica de Rubiataba, 2020. Disponível em http://repositorio.aee.edu.br/bitstream/aee/17815/1/2020%20-TCC%20-HESROM %20C%C3%89SAR%20DE%20OLIVEIRA.pdf Acesso em 20 mar 2023.

PINHEIRO, Patrícia Peck. **Direito digital**. 5. ed. São Paulo: Saraiva, 2013.

RIBEIRO, Eliete da Silva. **Crime de estelionato**: uma análise da evolução sob a égide da impunidade na cidade de Manaus. 2019. Disponível em: https://semanaacademica.org.br/system/files/artigos/crime_de_estelionato_- _uma_ analise_da_evolucao_sob_a_egide_da_impunidade_na_cidade_de_manaus_eliete_ da_silva_ribeiro_0.pdf. Acesso em 15 mar 2023.

ROCHA, A. A. **Cibercriminalidade**: os crimes cibernéticos e os limites da liberdade de expressão na internet. Faculdade de Ensino Superior e Formação Integral, Curso de Direito, São Paulo, 2017 [Internet]. Disponível em: https://www.faef.br/userfiles/files/23%20%20CIBERCRIMINALIDADE%20E%20OS %20LIMITES%20DA%20LIBERDADE%20DE%20EXPRESSAO%20N %20INTERNET.pdf. Acesso em 15 marc 2023.

ROSA, Fabrízio. **Crimes de Informática**. Campinas: Bookseller, 2002, p. 53-54.

SANTOS, Liara Ruff dos et. al. **Os crimes cibernéticos e o direito a segurança jurídica**: uma análise da legislação vigente no cenário brasileiro contemporâneo. Santa Maria, 2017. Disponível em: < http://coral.ufsm.br/congressodireito/anais/2017 /7-7.pdf>. Acesso em 11 mai 2023

SILVA, Gilsimar Pinheiro da. Crimes digitais: evolução dos crimes e a aplicação do Direito. **Dissertação de Mestrado**. 2021. Universidade Potiguar. Disponível em https://repositorio.animaeducacao.com.br/bitstream/ANIMA/22552/1/CRIMES %20DIGITAIS%20EVOLUCAO%20DOS%20CRIMES%20E%20APLICACAO%20DO %20DIREITO.pdf. Acesso em 15 marc 2023.

SILVA, Francielly Juliana; SANTOS, Ramon João Marcos dos. **Estelionato praticado por meio da Internet:** uma visão acerca dos crimes virtuais. 2021. Disponível em https://repositorio.animaeducacao.com.br/bitstream/ANIMA/18080/1/TCC %2001.12.21%20dep%C3%B3sito%20final.pdf Acesso em 20 ago. 2023.

SPINIELI, André Luiz Pereira. **Crimes informáticos**: comentários ao projeto de Lei n° 5.555/2013. Brasilia, 2018. Disponível em:< http://www.mpf.mp.br/atuacaotematica/ccr2/publicacoes/coletaneas-de-artigos/ coletanea_de_artigos_crimes_ ciberneticos>. Acesso em: 18 mai 2023.

VIGNOLI, Richele Grenge; MONTEIRO, Silvana Drumond. A dark web e seu conteúdo informacional. In: **VI SECIN, Seminário em Ciência e Informação**. UEL: Londrina – PR, 3 a 5 de agosto de 2016.