CENTRO UNIVERSITÁRIO UNIFACIG

CURSO DE DIREITO

O CRIME DE ESTELIONATO E SUAS IMPLICAÇÕES NA ERA DIGITAL: O CONSTANTE CRESCIMENTO DOS GOLPES CIBERNÉTICOS VIA REDES SOCIAIS

Jainy Breder Pinheiro de Amorim Moreira

Manhuaçu/MG
2023

JAINY BREDER PINHEIRO DE AMORIM MOREIRA

O CRIME DE ESTELIONATO E SUAS IMPLICAÇÕES NA ERA DIGITAL: O CONSTANTE CRESCIMENTO DOS GOLPES CIBERNÉTICOS VIA REDES SOCIAIS

Trabalho de Conclusão de Curso apresentado no Curso Superior de Direito do Centro Universitário UNIFACIG, como requisito parcial à obtenção do título de Bacharel em Direito.

Área de Concentração: Direito Penal.

Orientador: João Pedro Schuab Stangari Silva

Manhuaçu/MG
2023

JAINY BREDER PINHEIRO DE AMORIM MOREIRA

O CRIME DE ESTELIONATO E SUAS IMPLICAÇÕES NA ERA DIGITAL: O CONSTANTE CRESCIMENTO DOS GOLPES CIBERNÉTICOS VIA REDES SOCIAIS

Trabalho de Conclusão de Curso apresentado no Curso Superior de Direito do Centro Universitário UNIFACIG, como requisito parcial à obtenção do título de Bacharel em Direito.

Área de Concentração: Direito Penal.

Orientador: João Pedro Schuab Stangari Silva

Banca Examinadora:

Data da Aprovação: DD/MM/AAAA

Titulação e Nome do Professor – INSTITUIÇÃO (Orientador)

Titulação e Nome do Professor – INSTITUIÇÃO

Titulação e Nome do Professor – INSTITUIÇÃO

RESUMO

Este estudo tem como escopo abordar sobre o aumento do crime de estelionato em sua nova modalidade, praticado em ambiente virtual por criminosos que buscam captar vítimas através das redes sociais. O crime de estelionato virtual vem crescendo aceleradamente, principalmente pela facilidade do agente em abordar os usuários e aplicar o golpe com sucesso de forma tão rápida. Inicialmente, foi mencionado o crime de estelionato puro e simples, sua tipificação e classificação, para uma posterior compreensão do crime de estelionato no ambiente virtual. Em seguida, abordou-se sobre o papel das redes sociais na sociedade no cotidiano das pessoas e as várias novas formas e possibilidades do crime de estelionato. Logo, a proposta do trabalho foi a de trazer pontos essenciais no combate ao aumento do crime de estelionato virtual, abordando a denúncia e a sua importância para a investigação, as delegacias especializadas em crimes cibernéticos, e proposta da educação digital sendo ponto chave o combate à infração penal. O presente trabalho ampara-se na vertente metodológica jurídico-sociológica, e em relação aos seus tipos, utiliza-se o método jurídico dogmático, com uma pesquisa descritiva, de natureza aplicada e abordagem qualitativa. Sendo a pesquisa bibliográfica, utilizando-se do levantamento de referências teóricas já publicadas.

Palavras-Chave: Estelionato. Estelionato Virtual. Redes Sociais. Cibercrimes. Educação Digital.

ABSTRACT

This study aims to address the increase in the crime of embezzlement in its new modality, practiced in a virtual environment by criminals who seek to capture victims through social networks. The crime of virtual embezzlement has been growing rapidly, mainly due to the agent's ease in approaching users and successfully carrying out the scam so quickly. Initially, the pure and simple crime of embezzlement, its typification and classification, was mentioned, for a later understanding of the crime of embezzlement in the virtual environment. Next, the role of social networks in society in people's daily lives and the various new forms and possibilities of the crime of embezzlement were discussed. Therefore, the proposal of the work was to bring essential points in the fight against the increase in the crime of virtual fraud, addressing the complaint and its importance for the investigation, the police stations specializing in cyber crimes, and the proposal for digital education, with the combat being a key point. to the criminal offense. The present work is based on the legal-sociological methodological aspect, and in relation to its types, the dogmatic legal method is used, with descriptive research, of an applied nature and a qualitative approach. Being bibliographical research, using the survey of theoretical references already published.

Keywords: Fraud. Virtual Swindle. Social media. Cybercrimes. Digital Education.

SUMÁRIO

INTRODUÇÃO

O presente estudo tem como objeto o crime de estelionato e suas implicações na era digital, tendo em vista o advento das novas tecnologias digitais e a migração para os meios virtuais dos criminosos com intenção de captar vítimas, tendo como ferramenta as redes sociais. Assim, serão mencionadas as principais propostas para o combate ao crime de estelionato virtual, as leis que tipificam o crime e projetos de lei acerca do tema.

Fabrízio Rosa (2005) disserta que com o avanço crescente da tecnologia, inúmeros criminosos reais passaram a utilizar a internet para cometer crimes virtuais, como o estelionato, a calúnia, o furto, o racismo, sabendo que seria mais difícil a identificação de autoria dos delitos, bem como a reparação do dano.

O autor ressalta que com o avanço da tecnologia, o uso do mundo virtual está se tornando algo recorrente no cotidiano das pessoas, podendo citar alguns exemplos de tarefas realizadas no âmbito virtual diariamente, como por exemplo, as transições bancárias via pix, pesquisas, compra e venda de produtos, dentre outras atividades. A internet se faz presente na vida da população, visto que, o mundo virtual facilita num modo geral o cotidiano. Assim, inúmeros criminosos reais passaram a utilizar a internet para cometer crimes virtuais, como o de estelionato, para captar o maior número de vítimas possíveis com facilidade.

Roque (2007, p.25), diz o crime cibernético é “toda conduta, definida em lei como crime, em que o computador tiver sido utilizado como instrumento de sua perpetração ou consistir em seu objeto material.” Isto posto, o crime de estelionato virtual configura-se crime cibernético, pois tal crime de forma ligeira adaptou-se a nova realidade virtual utilizando-se dos meios eletrônicos para o cometimento de crimes e captações de vítimas.

Já Feitoza (2012), ressalta que a maioria dos indivíduos que praticam delitos de estelionato em ambientes virtuais são pessoas com conhecimentos de informática, sendo que eles estão dispostos a correr riscos, enganar e prejudicar pessoas dentro das redes sociais. A distinção entre o golpe real e o virtual é a estratégia aplicada, considerando que a primeira ocorre em ambiente físico, enquanto a segunda ocorre em ambiente virtual.

Feitoza (2012) considera que o estelionato virtual ainda é algo recente dentro do Estado e dos tribunais brasileiros, todavia, requer total atenção com a

popularização e gradação dessas infrações, que tem alcançado milhares de novos usuários diariamente, aumentando assim, a quantidade de vítimas. Neste contexto, o crime de estelionato digital é um assunto recentemente debatido nos tribunais brasileiros, devido à crescente quantidade de usuários com acesso à internet.

As redes sociais são instrumentos de captação de vítimas, sendo totalmente viável ao crime de estelionato virtual. Os criminosos criam páginas e perfis falsos, oferecem oportunidades surreais e, em muitos casos, enviam mensagens via *WhatsApp*, acabando por enganar as vítimas mais vulneráveis, até mesmo se passando por alguém que a vítima conhece.

Cruz e Rodrigues (2018) trazem a respeito da dificuldade nas investigações quando se trata do mundo virtual, inclusive pela falta de profissionais especializados para agilizar nas investigações. Existem empresas redes sociais como por exemplo, o *WhatsApp*, que também não colaboram com o judiciário, assim, atrasando as investigações e consequentemente colaborando no aumento de crimes virtuais praticados no Brasil, pois, o crescimento dos cibercrimes aumenta principalmente pela limitação da investigação no âmbito virtual.

O Ministério Público, a Polícia e o Poder Judiciário enfrentam várias dificuldades para enquadrar e punir os criminosos que praticam o estelionato virtual. Essas dificuldades tendem a gerar uma sensação de impunidade, levando as pessoas a associarem essa impunidade à falta de leis específicas sobre crimes cibernéticos (CRUZ; RODRIGUES, 2018).

Nesse contexto, Martins (2012) diz a educação digital é essencial para que não continue crescendo o número de vítimas quando se trata dos cibercrimes, deve-se investir na educação no ciberespaço para dotar a sociedade civil de conhecimentos quando estiverem navegando nas redes.

Os criminosos, devido às vulnerabilidades dos usuários de internet, se aproveitam dos usuários sem conhecimentos técnicos dentro das redes sociais para, neste caso, efetuar golpes cibernéticos. Assim, sem o conhecimento necessário para usarem as redes, acabam facilitando para os criminosos aplicarem os golpes. Desta forma, a vulnerabilidade dos usuários é um dos pontos essenciais para que a educação digital seja propagada.

A diretriz regulamentada no art. 171, do Código Penal aborda o delito de estelionato, sendo que o mesmo se aplica a modalidade no âmbito virtual. O Código Penal não menciona em seu texto o crime de estelionato virtual, ou seja, a conduta

descrita no art.171, trata-se apenas dos crimes praticados diretamente pelo agente, com a obtenção de benefícios ilícitos em detrimento de terceiros, não importando o meio pelo qual o crime foi efetuado. (FEITOZA, 2012).

O trabalho que se segue tem como problema de pesquisa o estelionato em sua nova modalidade em meio as redes sociais, infração penal que se torna cada dia mais frequente no cotidiano dos usuários das plataformas, intentando responder possíveis formas de combate ao crime, bem como a legislação vigente e os projetos de lei que tratam sobre a matéria.

A pesquisa justifica-se tendo em vista os graves danos causados pelo crime de estelionato virtual à sociedade, sendo que o delito merece atenção especial do legislativo brasileiro. Os projetos em tramitação no Congresso necessitam de atenção para que tenham aprovação dos deputados e dos senadores. Todos os dias, novos usuários tornam-se vítimas desses criminosos, que se aproveitam da falta de fiscalização para enganar as vítimas e fornecer-lhes bens e serviços sem cumprir as obrigações acordadas, causando prejuízos irreparáveis. Dessa forma, o objetivo da pesquisa envolve-se na análise das propostas para combate ao crime.

A pesquisa ampara-se na vertente metodológica jurídico-sociológica, tendo em vista que se embasa na noção de um Direito como ciência social aplicada, que se preocupa com a eficiência, eficácia e efetividade do fenômeno jurídico em um ambiente social mais amplo (GUSTIN; DIAS, 2010). Utilizou-se o método jurídico dogmático, com uma pesquisa descritiva, de natureza aplicada e abordagem qualitativa. A pesquisa que se desenvolve é bibliográfica, utilizando-se do levantamento de referências teóricas já publicadas, com especial ênfase na doutrina sobre a matéria e a análise jurídico dogmática de normas do ordenamento jurídico brasileiro, cuja reflexão discursiva servir-se-á, sobre a base do método hermenêutico doutrinal para a investigação in loco dos conceitos e análise do tema.

O estudo realizado foi dividido em 3 capítulos. No capítulo I foi apresentado o crime de estelionato, sua tipificação e classificação. Traz-se a compreensão o estelionato simples para o entendimento do crime de estelionato em ambiente virtual, que também foi exemplificado dentro deste capítulo. Menciona-se sobre as redes sociais como principais meios de captação de vítimas e o porquê dos criminosos escolherem migrar para o ambiente virtual para procurarem vítimas.

No capítulo II são apresentadas propostas no combate ao crime de estelionato virtual. Perpassa-se a denúncia, a investigação, as Delegacias

Especializadas (Delegacias de Repressão aos Crimes Informáticos). Além disso, é enfatizado sobre a educação digital, tendo como o enfoque principal no combate a este crime.

No capítulo III, são apresentadas as garantias da Legislação Brasileira sobre o crime de estelionato no ordenamento jurídico. Assim como o Direito Penal se aplica e se atualiza para assegurar os direitos das vítimas que sofrem o estelionato virtual, são mencionados os projetos de lei acerca do crime de estelionato em ambiente virtual, e o mais importante, o status de cada um deles.

1. O CRIME DE ESTELIONATO

O crime de estelionato está descrito no artigo 171 do Código Penal, estabelecendo uma pena de reclusão de um a cinco anos e multa para aqueles que obtiverem, para si ou para outros, vantagem ilícita em prejuízo da vítima, a qual é induzida ou mantida em erro por meio de qualquer fraude. Nos termos da classificação doutrinária clássica, o crime de estelionato é considerado um crime comum, sendo doloso e material, determinado pela ação do agente e com consequências definidas. O comportamento do sujeito é engano ou fraude, induzindo a vítima a cometer erros com a intenção de obter benefícios indevidos em detrimento de outrem. Haja vista, os agentes utilizam de diversos meios fraudulentos para cometer o delito (GRECO, 2015).

Importante ressaltar que, via de regra, o estelionato é de natureza material, sendo assim, consuma-se quando o criminoso efetivamente alcança o resultado natural (ou seja, obtém uma vantagem ilegal) e realiza a tentativa. Conforme mencionado anteriormente, o artigo 171 do Código Penal que, prevê formas simples de fraude, seguidas de padrões equivalentes a atos de natureza material, expressas nos incisos I, II, III, IV e VI do §2º, *ipsis litteris*:

> § 2º - Nas mesmas penas incorre quem:
> **Disposição de coisa alheia como própria**
> I - vende, permuta, dá em pagamento, em locação ou em garantia coisa alheia como própria;
> **Alienação ou oneração fraudulenta de coisa própria**
> II - vende, permuta, dá em pagamento ou em garantia coisa própria inalienável, gravada de ônus ou litigiosa, ou imóvel que prometeu vender a terceiro, mediante pagamento em prestações, silenciando sobre qualquer dessas circunstâncias;
> **Defraudação de penhor**
> III - defrauda, mediante alienação não consentida pelo credor ou por outro modo, a garantia pignoratícia, quando tem a posse do objeto empenhado; **Fraude na entrega de coisa**
> IV - defrauda substância, qualidade ou quantidade de coisa que deve entregar a alguém;
> [...]
> **Fraude no pagamento por meio de cheque**
> VI - emite cheque, sem suficiente provisão de fundos em poder do sacado, ou lhe frustra o pagamento. (BRASIL, 1940, online)**.**

O referido tipo penal previsto no artigo 171, caput, do Código Penal destina-se a punir o agente que, por meio de fraude, cause prejuízo a outrem; não

importando a extensão do dano causado, pois até mesmo em situações mais simples, prejudica a confiança recíproca entre as partes, que, no entanto, é tutelada com a especificação do crime.

Andreucci (2014) conceitua o crime de estelionato como ato ilícito de induzir ou sustentar uma pessoa a obter vantagem ilícita para si ou para outrem através do uso de artifícios, subterfúgios ou quaisquer outros meios enganosos. Nesta perspectiva, o agente assegura benefícios ilegais para si ou para terceiros através de qualquer ato que induza a vítima em erro.

De acordo com o autor, o que é importante para o criminoso é que ele obtenha benefícios financeiros da vítima, com intenção maliciosa e que induza a vítima a simplesmente entregar o item ou valor desejado. A vítima que foi completamente manipulada, e o mais importante, enganada, entrega voluntariamente suas coisas, confiante de que o golpista agirá de boa fé e cumprirá sua promessa, com base na confiança e no respeito mútuos. Assim, os bens são entregues pela vítima que acredita na suposta boa índole da pessoa.

Greco (2011) para a consumação do delito não importa se a fraude é civil ou penal, o que importa é que seja uma fraude. Dessa maneira, ocorre apenas uma diferenciação da qualidade e intensidade da fraude, que serão examinados caso a caso. Por meio da análise do caso específico, verificar-se-á como a vítima foi afetada e se realmente foi enganada ou mantida em erro por meio de um ato doloso da pessoa com quem negociou.

O bem jurídico protegido é a inviolabilidade do patrimônio, especialmente em relação a atos praticados por meio de fraudes. Protege-se tanto o interesse social, que está relacionado à confiança mútua entre as partes e que deve prevalecer nas relações patrimoniais individuais ou comerciais, quanto o interesse público representado pela necessidade de reprimir a fraude que cause danos a terceiros. Deve-se ressaltar que é proibido cometer fraudes para obter vantagem ilícita em detrimento de outra pessoa. O estelionatário é considerado criminoso em todas as circunstâncias, mesmo se cometer a fraude em outros contextos que não necessitam de proteção jurídica, pois, sua conduta é ética e juridicamente ilícita (BITENCOURT, 2012).

Para Greco (2020), um dos atos sequenciados é o agente induzir ou manter alguém a erro, significa que a vítima está sendo traída, e não tem ideia do que está acontecendo, pois está sendo iludida. Ele também ressalta que, o estelionato é a

fraude de alienação de bens, dando origem ao binômio “vantagem ilícita de prejuízo alheio”. Mas, para configurar crime não basta ter apenas os elementos acima, deve haver também o último elemento entre eles, ou seja, a conexão causal. Portanto, deve haver uma relação causal ininterrupta entre as duas partes no estelionato.

Andreucci (2014) o indivíduo ativo é aquele que se favorece da vantagem ilícita ou age fraudulosamente, sendo o criminoso. Já o indivíduo passivo é aquele que sofre prejuízo patrimonial em decorrência do ato ilícito, assim como todas as pessoas enganadas devido à fraude praticada pelo autor.

Bitencourt (2012) alerta que é importante ressaltar que crianças e pessoas com condições especiais não podem ser consideradas sujeitos passivos desse crime, pois é necessário que alguém seja induzido ao erro para que a fraude seja consumada. Além disso, é imprescindível que a vítima tenha capacidade de discernimento para poder ser enganada. Como crianças e autistas não possuem essa capacidade, há uma inadequação absoluta do objeto, pois um dos elementos do crime de estelionato é a utilização de meios fraudulentos com o objetivo de iludir ou manter a vítima em erro, sendo que esses indivíduos incapazes não têm a capacidade de compreender e querer, não podendo ser enganados nem ser vítimas desse crime.

Com base nas citações pode-se afirmar que, o crime de estelionato somente pode configurar-se de forma dolosa, já que depende da vontade do agente de obter vantagem ilícita utilizando-se de instrumentos fraudulentos para conseguir alcançar o seu objetivo. Observa-se que para iludir alguém o agente pratica atos conscientemente. O crime admite tentativa, mesmo ainda sendo um crime doloso, pois depende da vontade do criminoso de iludir a vítima.

Portanto, não podem ser confundidos os crimes de estelionato e o de furto mediante fraude (previsto no art. 155, §4°, II, do Código Penal), pois existe uma diferença entre eles. No furto mediante fraude, o criminoso subtrai a coisa, e se utiliza de tal coisa, para então iludir a vítima. Enquanto, no estelionato a vítima entrega de forma voluntária o bem, após meios fraudulentos empregados pelo agente.

1.1. ESTELIONATO VIRTUAL

O estelionato virtual é um crime no qual o agente servindo-se de equipamentos tecnológicos e acesso à rede, utiliza os meios fraudulentos para obter uma vantagem ilícita, tendo acesso e utilizando os dados da vítima, fotos, número de telefone, entre outros. Os criminosos mandam mensagens para as pessoas próximas das vítimas e começam a praticar o eventual crime (NASCIMENTO, 2018).

Dessa forma, o crime cibernético tem como conceito o de “toda conduta, definida em lei como crime, em que o computador tiver sido utilizado como instrumento de sua perpetração ou consistir em seu objeto material.” (ROQUE, 2007, p.25). Isto posto, o crime de estelionato virtual configura-se crime cibernético, pois tal crime de forma ligeira adaptou-se a nova realidade virtual utilizando-se dos meios eletrônicos para o cometimento de crimes e captações de vítimas

Não existe uma legislação especifica sobre o crime de estelionato virtual, haja vista o delito tem previsão legal no rol dos crimes praticados contra o patrimônio, no capítulo VI, que trata do estelionato e outras fraudes. Tal crime é disposto no artigo 171, do Código Penal.

Conforme o artigo 171, os elementos constitutivos do crime de estelionato incluem quatro elementos, incluindo crimes virtuais, a saber: intenção de obter vantagem indevida; causar danos a outrem; o agente usa truques ou artimanhas; o mesmo tem a intenção de enganar ou induzir pessoas ao erro, de modo que a vítima tenha uma percepção equivocada dos fatos. No estelionato virtual os criminosos utilizam os meios digitais, para enganar as vítimas e induzi-las a entregar voluntariamente os bens ou itens, acreditando que o estelionatário está agindo de boa-fé.

Observa-se que o estelionato virtual ou real não admite ser crime culposo, pois o criminoso sempre irá agir com a intenção de induzir, prejudicar e manter a vítima em erro, assim, sendo um crime totalmente doloso. O agente age com *animus livre* e com consciência da prática de conduta inserida na norma penal incriminadora.

São chamados de *crackers*, os usuários com entendimento profissional no campo da informática, mas que utilizam do conhecimento para cometerem crimes e outras ações maldosas no ambiente virtual (ROSA, 2005). Fabrízio Rosa, ainda fala da diferenciação de *Cracker* e *Hacker*.

> Cracker é o mesmo que *hacker*. A diferença entre um e outro está em utilizar o seu conhecimento para o mal. Destruir e roubar são suas palavras de ordem. Assim, o cracker usa os seus conhecimentos para ganhar algo, rouba informações sigilosas para fins próprios e destrói sistemas para exibir (ROSA, 2005, p.61).

Para Feitoza (2012) a maioria dos agentes que cometem crimes de estelionato em ambientes virtuais são pessoas com conhecimentos de informática, sendo que eles estão dispostos a correr riscos, enganar e prejudicar pessoas dentro das redes sociais. A única diferença entre o golpe real e o virtual é o *modus operandi* empregado, considerando que a primeira ocorre em ambiente físico, enquanto a segunda ocorre em ambiente virtual.

Explica o autor que a figura do estelionato virtual ainda é algo recente dentro do estado e dos tribunais brasileiros, porém, merece atenção especial com a popularização e aumento de tais crimes, que tem atingido e adquirido milhares de novos usuários todos os dias, dessa forma aumentando também o número de vítimas. Nessa linha de raciocínio, o crime de estelionato digital é um tema recente discutido no estado e tribunais brasileiros, quando da aplicação da norma, especialmente porque o acesso à internet tem a possibilitado a cada vez mais usuários (FEITOZA, 2012).

Diante todo o exposto, o crime de estelionato virtual constitui uma nova modalidade do estelionato puro e simples, tipificado também no artigo 171 do Código Penal, sendo que os agentes aproveitam do conhecimento tecnológico para enganar e levar pessoas ao erro, praticando o crime de estelionato dentro das plataformas, obtendo êxito com facilidade e sendo mais difícil ser identificado.

1.2. REDES SOCIAIS: PRINCIPAL MEIO DE CAPTAÇÃO DE VÍTIMAS

Marteleto (2001, p.72) aplica o conceito de redes sociais como: “um conjunto de participantes autônomos, unindo ideias e recursos em torno de valores e interesses compartilhados”. Ressaltando ainda que:

> As redes nas ciências sociais designam normalmente – mas não exclusivamente, os movimentos fracamente institucionalizados, reunindo indivíduos e grupos em uma associação, cujos termos variáveis e sujeitos a uma reinterpretação em função dos limites que pesam sobre suas ações (MARTELETO, 2001, p.72).

Conforme Corrêa (2000), as Redes Sociais são plataformas digitais, onde as pessoas criam uma identidade virtual, com a finalidade de interagir com os demais

de forma facilitada. O processo de criação do perfil virtual é rápido e prático, e possibilita que o usuário insira informações a seu respeito, que poderão ser compartilhadas com outros usuários.

A internet passou a facilitar o cotidiano das pessoas, conectando vários meios tecnológicos, e fazendo com o que a sociedade consiga interagir em tempo real.

> A presença cada vez mais forte dos computadores em nossas vidas, a capacidade de coletar e analisar dados pelas empresas e pelo Estado, e de disseminá-los através das rápidas vias das telecomunicações, nos têm proporcionado benefícios, mas, na mesma proporção, também malefícios (CORRÊA, 2000, p.2).

Rosa (2005) disserta que, com avanço crescente da tecnologia, inúmeros criminosos reais passaram a utilizar a internet para cometer crimes virtuais, como o estelionato, a calúnia, o furto, o racismo, entre outros crimes, sabendo que seria mais difícil a identificação de autoria dos delitos, bem como a reparação do dano.

> [...] O problema da internet passou a ser identificado quando a tecnologia incrementou e complicou relações sociais consideradas, até então, pacíficas e controladas, possibilitando algumas experiências socialmente desagradáveis e indesejadas, como sua utilização para a prática de crimes, e a criação de novos contatos que colocam em risco bens que ainda não tiveram sua relevância reconhecida pelo Direito (BRITO, 2013, p.9).

A internet interliga as pessoas através das redes sociais, diminuindo as distâncias e facilitando as relações entre povos e culturas no cotidiano. Porém, tudo tem os prós e contras, e não seria diferente dentro das plataformas digitais. Ocorre que tem sido também muito comum a utilização das ferramentas como instrumentos de crimes, quando indivíduos mal-intencionados criam perfis que não condizem com a verdadeira identidade da pessoa usuária, utilizando informações que dizem respeito à outra pessoal real ou até fictício (ROSA, 2005).

Diante do exposto, é possível afirmar que as redes sociais são instrumentos de captação de vítimas, sendo totalmente viável ao crime de estelionato virtual. Os criminosos criam páginas e perfis falsos, oferecem oportunidades surreais e, em muitos casos, enviam mensagens via *WhatsApp,* acabando por enganar as vítimas mais vulneráveis, até mesmo se passando por alguém que a vítima conhece. Os fatos constituem as características do crime de estelionato virtual. Alguns exemplos muito comuns são: empréstimos com juros baixos ou sem nenhuma taxa; empregos

oferecidos na Internet que pagam bem, mas que exigem uma certa quantia de recursos para serem registrados, sites de venda de produtos que nunca são entregues, mensagens em grupo via WhatsApp, comumente conhecidas como “correntes”, todas estas condutam que visam alguma forma buscar uma vantagem ilegal e enganar terceiros.

O *WhatsApp* segue sendo uma das principais redes sociais utilizadas para o cometimento do crime, pois é onde se concentra a maior parte dos brasileiros como meio de comunicação facilitada. Além do erro humano e a falta de se preocupar em quebrar vulnerabilidades de sistema, a prática de *phishing* é relativamente simples e barata. Basta cadastrar um domínio, seja gratuito ou com preço acessível, depois adquirir um certificado digital para o site ser considerado confiável e disparar e-mails em massa a espera de alguma vítima (KAPERSKY, 2018).

Como forma de captação de vítimas, tem-se a modalidade de criação de perfis falsos. Nesse *modus operandi*, os agentes escolhem imagens de pessoas desconhecidas para atribuí-las ao seu novo perfil, com finalidade de aplicar golpes dentro da plataforma, inclusive existindo sites com a finalidade de ofertar fotos nesse sentido, com indivíduos que disponibilizam o uso de sua imagem para esse fim em troca de dinheiro. Tal prática não configura crime, estando o criador sujeito a infringir apenas alguma regra dos Termos de Serviço da rede social, sendo que, identificado abuso ou uso indevido de imagens ou informações, somente será punido com a exclusão da conta (KAPERSKY, 2018).

Importante destacar que, ainda que o perfil falso criado seja de uma pessoa que não exista, um animal ou um objeto, é possível afirmar que haja responsabilização dos criadores, uma vez que, em alguns casos, a conduta se adequa a outros crimes previstos na legislação penal.

Ludgero (2020) traz o número de perfis falsos para aplicar golpes vem crescendo cada vez mais. O *Instagram*, outra rede social importante, também tem sido uma das ferramentas mais utilizadas pelos agentes. As plataformas facilitam as ações ilegais, por conta da dificuldade de rastrear o criminoso e a falta de educação digital. Os perfis falsos são difíceis de identificar, pois os agentes agem como se fossem reais, como por exemplo: postam fotos, legendas, *stories* e informações como se fossem reais.

Capez (2020, p.75) disserta que quanto ao crime, “exige-se também o chamado elemento subjetivo do tipo, consistente no fim especial de obter vantagem,

em proveito próprio ou alheio, ou de causar dano a outrem". Dessa forma, de acordo com o entendimento, faz-se necessário a comprovação de que há dolo na conduta, com a intenção de obter vantagem ilícita ou causar dano a alguém, quando da criação do perfil falso nas redes sociais.

Nas palavras de Nelson Hungria (1958, p.108), "a vantagem pretendida pelo agente não poderá ter natureza econômica, pois, se assim fosse, tal conduta seria tipificada como estelionato, delito previsto no artigo 171, do Código Penal".

A partir do momento em que o agente cria o perfil falso com a intenção de obter vantagem ilícita patrimonial, irá ser configurado o crime de Estelionato, tipificado no Código Penal, em seu artigo 171. Portanto, a criação de perfil falso em uma rede social não é necessariamente configurada crime, sendo preciso verificar o real caso concreto, avaliando qual intenção de obter algum proveito com essa conduta.

2. PROPOSTAS PARA COLABORAR NO COMBATE AO CRIME DE ESTELIONATO VIRTUAL

O presente capítulo irá traçar sobre os principais pontos estratégicos para ajudar no combate ao crime de estelionato virtual. Assim, importante destacar sobre como funciona a denúncia e investigação, qual melhoria poderia ser implementada na hora da investigação de cada caso concreto.

Ponto essencial no combate ao aumento deste delito, torna-se a propagação da educação digital, tendo em vista os criminosos cibernéticos aplicam golpes abusando da boa-fé e inocência das pessoas. A falta de conhecimento e malícia digital, auxiliam na efetivação de um golpe. A educação digital e o estudo detalhado sobre os perigos enfrentados na internet e como evitá-los, permitem tornar capaz qualquer pessoa a se defender contra-ataques cibernéticos, principalmente o de estelionato.

Para denunciar um crime virtual é necessário identificar quem está sendo vítima; na maioria das vezes estes crimes não são identificados em um primeiro momento, por esse motivo demora ao fazer a denúncia, tornando difícil para a investigação e menos provável à punibilidade do agente. Deve-se guardar todas as informações e coletar todas as evidências possíveis que estejam ao seu dispor, como por exemplo, prints e gravações de telas, entre outros. Assim, servirão de prova na denúncia e ajudará na investigação do crime (CNJ, 2018).

> A ata notarial serve para pré-constituir prova dos fatos. Muitas vezes não temos como provar uma situação potencialmente perigosa ou danosa. O tabelião é, portanto, uma testemunha oficial cujo ato vai desencadear a fé pública e fazer prova plena perante qualquer juiz ou tribunal (CASSANTI, 2014, p.57).

Quando as evidências iniciais forem reunidas, é fundamental que a vítima faça o registro como prova de veracidade dos fatos, indo até ao cartório mais próximo para registrar uma ata notarial dos documentos e fatos digitais. Sendo indispensáveis dentro do processo para que, as evidências pela vítima coletadas, sejam registradas como verdadeiras, e sejam provas numa futura ação judicial (CNJ, 2018).

> Nas verificações (tanto no meio físico, quanto no eletrônico), o tabelião constata os fatos, relatando fielmente tudo aquilo que presenciou. A ata notarial tem força certificante para comprovar a integridade e a veracidade destes documentos, atribuir

> autenticidade, fixar a data, hora e existência de arquivo eletrônico (CASSANTI, 2014, p.57).

Como em qualquer outro crime, nos crimes virtuais, também é preciso realizar o boletim de ocorrência do delito, tendo em vista ser essencial os dados nele coletados, sendo úteis para conduzir as autoridades em relação ao crime. Existem Delegacias de Repressão aos Crimes Informáticos especializadas, contudo, caso não haja uma unidade na cidade da vítima o B.O., pode ser realizado em qualquer unidade da Polícia Civil. Importante destacar que o boletim de ocorrência é parte essencial do processo, pois os dados nele coletados tornam-se extremamente úteis para conduzir as autoridades em relação ao delito (CNJ, 2018).

Cassanti (2014) traz que os crimes mais investigados pelas delegacias especializadas em crimes virtuais são aquelas contra o patrimônio, como o de estelionato. Em seguida, outros crimes bastante comuns no mundo virtual são calúnia, injúria e difamação, os famosos crimes contra a honra.

Sabe-se que, sobre a quantidade de Delegacias de Repressão aos Crimes de Informática (DRCI), o número exato de delegacias especializadas pode variar ao longo do tempo, uma vez que, novas unidades podem ser criadas e outras podem ser desativadas ou fundidas com outras unidades policiais. De acordo com informações disponíveis até o momento, existem pelo menos 27 DRCIs distribuídas em diferentes estados brasileiros. Alguns exemplos de estados que possuem delegacias especializadas em crimes virtuais são: São Paulo, Rio de Janeiro, Minas Gerais, Paraná, Rio Grande do Sul, Bahia, Pernambuco, entre outros (SAFERNET, 2023).

Em um levantamento realizado sobre as Delegacias Especializadas em Crimes Cibernéticos, pode-se notar os seguintes seguimentos separados por estados:

> BAHIA – Grupo Especializado de Repressão aos Crimes por Meio Eletrônico
> ESPÍRITO SANTO – Delegacia de Repressão a Crimes Eletrônicos
> MARANHÃO – Departamento de Combate aos crimes tecnológico
> MATO GROSSO - Delegacia Especializada de Repressão a Crimes Informáticos (DRCI)
> MINAS GERAIS – DEICC – Delegacia Especializada de Investigações de Crimes Cibernéticos
> PARÁ – Divisão de Prevenção e Repressão a Crimes Tecnológicos (DRCT)
> PARANÁ – (NUCIBER) Núcleo de Combate aos Cibercrimes

> PERNAMBUCO – Delegacia de Polícia de Repressão aos Crimes Cibernéticos
> PIAUÍ – Delegacia Especializada de Repressão aos Crimes de Alta Tecnologia (DERCAT)
> RIO GRANDE DO SUL – Delegacia de Repressão aos Crimes Informáticos (DRCI) – Departamento Estadual de Investigações Criminais (DEIC)
> SÃO PAULO – 4 Delegacias de Delitos Cometidos por Meios Eletrônicos (DIG)
> SÃO PAULO – DHPP
> SERGIPE – Delegacia de Repressão a Crimes Cibernéticos (DRCC)
> RIO DE JANEIRO – Delegacia de Repressão aos Crimes de Informática (DRCI)
> TOCANTINS – Divisão de Repressão a Crimes Cibernéticos – DRCC
> DISTRITO FEDERAL – Delegacia Especial de Repressão ao Crime Cibernético – DRCC
> GÓIAS – Delegacia Estadual de Repressão a Crimes Cibernéticos (DERCC) (SAFERNET, 2023, p.01).

Wendt (2013) diz que é notável que existam poucos estados brasileiros onde se encontram delegacias especializadas em crimes virtuais (DRCI), assim, para uma melhor e maior investigação dos crimes cibernéticos, torna-se necessária a ampliação das unidades instaladas em todos os estados brasileiros.

Rodrigues (2018) traz que é notável a dificuldade das investigações quando se trata dos cibercrimes, sendo um dos problemas encontrados o que que só pode ser aplicado a sanção se houver fortes evidências de que o autor cometeu o crime. Se a importância e a autoria não puderem ser comprovadas, o juiz poderá absolver o agente nos termos do artigo 386 do Código de Processo Penal.

> Art. 386. O juiz absolverá o réu, mencionando a causa na parte dispositiva, desde que reconheça: I - Estar provada a inexistência do fato; II - Não haver prova da existência do fato; III - Não constituir o fato infração penal; IV - Estar provado que o réu não concorreu para a infração (...) V - Não existir prova de ter o réu concorrido para a infração penal (BRASIL, 1940, online).

De acordo com esse entendimento sabemos que, ajuntada de provas nos cibercrimes são bastante complexas, pois a vítima não fica “cara a cara” com o criminoso, assim, ele consegue efetuar o crime sem ser claramente identificado, manipulando a vítima ou até mesmo se passando por outra pessoa. Importante mencionar que, mesmo os criminosos roubando os dados de forma anônima, algumas vezes são deixados alguns vestígios, tais eles que colaboram com

investigações. Sendo, a perícia competente e se tornando totalmente necessária nesse período investigativo.

> Sabe-se que a prova pericial tem importância cada vez maior e sua realização deve se adequar a uma série de cuidados, sobretudo no que diz respeito à forma de realização. O exame de corpo de delito, em verdade, é perícia no escopo de se provar a materialidade de um crime. Em crimes informáticos, comumente o corpo de delito é direto, incidindo sobre os vestígios deixados pela infração. Excepcionalmente, pode ser indireto, quando os vestígios desapareceram (JESUS; MILAGRE, 2016, p.193).

Jorge e Wendt (2013) trazem que a coleta das informações dos crimes virtuais em tempo hábil, antes que elas desapareçam, é uma tarefa muito difícil. No entanto, uma vez concluída, o objetivo da investigação é descobrir o IP da máquina e seus logs (ou seja, seus registros de login), que são umas das formas de identificar o culpado. “O log é o equivalente cibernético dos registros mantidos pela companhia telefônica, [...]” (JORGE; WENDT, 2013, p.130).

Para Jorge e Wendt (2013), o sucesso nas investigações, está vinculado a necessária quebra do sigilo telemático, pois o mesmo só se encontra disponível se a polícia realizar a solicitação. Dessa forma, deve-se acionar o servidor, para que ele envie os dados de conexão do IP, data, hora do crime virtual. Logo, é preciso que, o servidor de acesso, forneça detalhadamente o logs (dados físicos do titular da conta de internet que estava conectado no momento que foi acessado) assim, contribuindo para a celeridade da investigação. É através desta correlação envolvendo provedor de serviços e provedor de acesso é possível chegar à autoria de crimes na internet (CASSANTI, 2014, p.80).

Cruz e Rodrigues (2018) trazem que além do longo processo, outro problema também é evidente, que é a recusa das empresas de prestar informação e assistência às autoridades policiais e judiciais. Por exemplo, o *WhatsApp* recusou-se a fornecer as informações dos usuários sob investigação, mesmo sendo autorizado pelo tribunal, assim, como forma de punição, a rede social ficou bloqueada por tempo limitado.

A falta de pessoas especializadas para agilizar nas investigações, redes sociais como o WhatsApp que não colaboram com o judiciário, corroboram para o aumento do número de crimes virtuais praticados no Brasil. Importante frisar que a facilidade de compra de hospedagens de IP localizada fora do País faz com que

estrangeiros praticam tal crime contra pessoas no Brasil, causando um conflito de competência acerca de que órgão deve julgar os crimes cibernéticos, assim, atrasando o processo (CRUZ; RODRIGUES, 2018).

Entretanto, o estado encontra-se absolutamente vulnerável perante os criminosos virtuais, apesar de que se tem percebido que algumas medidas estão sendo adotadas para coibir esta prática. Assim, como mencionado acima, como a criação de delegacias especializadas no assunto, o treinamento e aperfeiçoamento dos policiais e outros profissionais que lidam com esta prática cotidianamente e o entendimento dos juízes no âmbito dos tribunais, visando unificar alguns entendimentos sobre o mesmo tema.

> Como promotor de justiça criminal, sei que infelizmente, os criminosos são mais rápidos que os legisladores. Isso acontece em todo o mundo e o Brasil não é exceção. Ainda mais, em se tratando de internet, que passou a ser largamente utilizada em nosso país a pouco tempo e que possui peculiaridades que outros meios de comunicação não têm. A facilidade que a internet oferece para a prática de crimes, deixou os juristas completamente assarapantados. Não possuímos legislação específica a respeito de crimes virtuais em nosso Código Penal de 1940. Evidentemente, no combate aos crimes virtuais, a justiça utiliza o Código Penal, pois a grande maioria das infrações penais cometidas através da internet, pode ser capitulada nas condutas criminosas previstas no Código Penal. Todavia, o ideal seria a existência de lei especial, onde estivessem capituladas as condutas especificas, isto é, as condutas criminosas, praticadas através da internet (DE INELLAS, 2009, p.100).

A dificuldade em desenvolver uma investigação no cibercrime abre espaço para que novos criminosos migrem para esta modalidade cada vez mais, principalmente os crimes de estelionato virtual com a facilitação das novas modalidades de pagamentos bancários, como por exemplo o PIX. Entretanto, acredita-se que a pretensão punitiva do Estado se encontra deficiente no que tange ao meio cibernético; garantindo aos criminosos na pior das hipóteses, penas absolutamente incompatíveis com a conduta praticada, fazendo com que eles tenham a certeza de que o crime em ambiente virtual realmente é o melhor caminho para atingir suas finalidades, valendo-se da forma branda de punir do estado e na dificuldade de investigação no âmbito virtual.

2.1. NECESSIDADE DE PROPAGAÇÃO DA EDUCAÇÃO DIGITAL

Fabrízio Rosa (2005) disserta que com o avanço da tecnologia e a popularização da internet, o estelionato virtual tem se tornado uma preocupação cada vez maior. Nesse contexto, a educação digital surge como uma ferramenta fundamental de prevenção para evitar cair em golpes e proteger-se contra o estelionato virtual.

Sabe-se que é necessária a propagação da “Segurança Digital” juntamente com a “Educação Digital”, dessa forma, possivelmente, o número de vítimas irão diminuir. A Cartilha de Segurança para Internet apresenta dez precauções que devem ser tomadas pelos usuários quando estiverem navegando na internet (CERT. BR, 2012).

> 1. Ficar em alerta com mensagens com nome de alguma instituição, principalmente se estiver pedindo informações ou instalação de programas; 2. Questionar-se por que a instituição da mensagem está mandando mensagem para você e se realmente possui relação com ela (por exemplo, se um banco que você não possui conta manda recadastrar); 3. Fique atento a mensagens que chamam muito a atenção ou ameace caso não cumpra o que está escrito; 4. Não considere uma mensagem confiante por que conhece o remetente, inúmeros atacantes usam contas invadidas ou manipuladas; 5. Seja cuidadoso ao acessar links, sempre analisando se o endereço está correto mesmo, antes de digitar dados pessoais; 6. Caso não suspeitar do link visualmente, passe o mouse por cima, caso houver técnica de ofuscar, ao posicionar o mouse sobre o link o endereço real da página falsa aparece; 7. Utilize mecanismos de segurança, como antimalware, firewall pessoal e filtros antiphishing; 8. Verifique se a página utiliza conexão segura; 9. Verifique as informações mostradas no certificado; 10. Acesse a página da instituição que supostamente enviou a mensagem e procure por informações (a maioria não adiciona páginas como suporte, sobre, etc.) (CERT. BR, 2012, p.11).

Sabe-se que os criminosos se utilizam de diversas estratégias para captar a atenção das possíveis vítimas, até mesmo roubando contas de outros usuários já existentes nas redes sociais, com o intuito de se passarem por estas pessoas, pois, dessa forma, a garantia de eficácia da armadilha é maior, principalmente se passando por pessoa conhecida da vítima (TELLES; GARCEZ, 2002). Portanto, é relevante a importância da investigação contextual de cada situação e educação digital para que não se torne vítima.

> Como as pessoas avaliam em que contexto se encontram? A quais características do contexto prestam atenção? Um contexto pode ser conceptualizado não simplesmente como decorrência do ambiente físico (cozinha, sala de estar, calçada em frente à farmácia), ou de combinação de pessoas (dois irmãos, marido e mulher, bombeiros). Muito mais que isso, um contexto se constitui pelo que as pessoas

> estão fazendo a cada instante e por onde e quando elas fazem o que fazem (TELLES; GARCEZ, 2002, p.217).

Desta forma, reafirma-se a importância de avaliação contextual além da educação digital e o conhecimento detalhado das redes para não se tornar vítima de tais crimes cibernéticos como o golpe de estelionato através das redes sociais. É de suma importância ao combate ao cibercrime, o investimento na educação no ciberespaço para dotar a sociedade civil de conhecimentos quando estiverem navegando nas redes (MARTINS, 2012).

Branco (2021) enfatiza que, por falta de conhecimento o indivíduo pode se envolver em golpes através de um aceite trivial de e-mail, ocasionando um grande perigo. Já o ingresso ao DNS do equipamento da vítima é um processo laborioso, no qual os golpistas buscam a oportunidade de modificar as configurações do computador do alvo, que só é possível quando ele está infectado. Os golpes vão dos mais simples aos mais complexos, desde o desenvolvimento de páginas falsas até a alteração da configuração do IP da vítima, conduzindo a mesma, ao acesso sites falsos.

Os governos devem avaliar as atuais políticas e práticas de segurança cibernética à medida que o mundo continua a mudar-se, uma vez que, se a medida de segurança cibernética evoluir, será favorável aos resultados do combate ao crime em ambiente virtual. O Serviço Governamental de Compartilhamento Cibernético (GCI) atualizou questões sobre o papel dos setores de infraestrutura crítica (CIRTs) nos acordos de cooperação na estrutura organizacional e percepção pública. Estas mudanças, porém, tornarão o GCI menos comparável ao longo do tempo, pois a atualização reflete os atuais compromissos dos países mais preciso (ITU, 2020).

A vulnerabilidade dos usuários e de algumas ferramentas é um dos pontos essenciais para que a educação digital seja propagada. A vulnerabilidade de uma plataforma é como se fosse uma fraqueza em um sistema, rede ou aplicativo que pode ser explorada por um invasor para comprometer a confidencialidade, integridade ou disponibilidade do mesmo, como uma falha na configuração de um programa ou uma falha nas medidas de segurança dele. Assim, permitindo o acesso a um determinado sistema, rede ou aplicativo, sem a autorização do usuário, configurando-se em ataque cibernético (CERT.BR, 2012).

Cardozo (2017) disserta que os criminosos, devido às vulnerabilidades, se aproveitam dos usuários sem conhecimentos técnicos dentro das redes sociais para, neste caso, efetuar golpes cibernéticos. Na maioria das vezes usuários se tornam vítimas por falta de privacidade e conhecimento técnico. Portanto, acabam facilitando para os criminosos aplicarem os golpes.

> Ainda têm as fraudes de *phishing*. *Phishing* é um vocábulo que provém do inglês, e quer dizer pescar, usado para definir condutas ilegítimas executadas no ambiente virtual. Assim, esta espécie de golpe faz a utilização da engenharia social para ludibriar a vítima e conseguir informações confidenciais e pessoais (PINHEIRO, 2000).

O *phishing,* dessa forma, acontece quando usuários recebem e-mails falsos para capturar suas informações, ou melhor, dados importantes. Considera-se uma forma de crime cibernético que aproveita da falta de conhecimento do indivíduo na diferenciação de sites reais de falsos (KUMARAGURU et al., 2009).

O ataque de *phishing* pode ocorrer em diversos meios digitais, como: “SMS, comunicadores instantâneos, redes sociais, páginas da web, aplicativos maliciosos, documentos digitais e qualquer outro meio digital que possibilite a execução dessa técnica criminosa” (PINHEIRO, 2020, p.56).

3. DO CRIME DE ESTELIONATO VIRTUAL NO ORDENAMENTO JURIDICO BRASILEIRO

Feitoza (2012) ressalta que o Código Penal não menciona em seu texto o crime de estelionato virtual, ou seja, a conduta descrita no art.171 trata-se apenas dos crimes praticados diretamente pelo agente, com a obtenção de benefícios ilícitos em detrimento de terceiros, não importando se o crime foi efetuado através de computador ou da Internet.

O Código Penal se refere ao estelionato puro e simples, consistente no ato de obter vantagem ilícita, para si ou para outro, em prejuízo alheio, mediante artifício ou quaisquer atos fraudulentos, independente da utilização ou não de dispositivos informáticos. Portanto, os agentes que cometem o crime de estelionato virtual, incidiriam nas penas do art. 171 do Código Penal, já que não mencionam os objetos utilizados para a consecução da vantagem ilícita, assim, englobando o estelionato virtual.

A maioria dos agentes que cometem crimes de estelionato em ambientes virtuais são pessoas com conhecimentos de informática, os mesmos estão dispostos a correr riscos, enganar e prejudicar pessoas dentro das redes sociais. A única diferença entre o golpe real e o virtual é o *modus operandi* empregado, considerando que a primeira ocorre em ambiente físico, enquanto a segunda ocorre em ambiente virtual (FEITOZA, 2012).

A prática de estelionato virtual é algo recente no contexto judicial brasileiro, mas demanda uma atenção especial devido à sua popularização e ao aumento de crimes dessa natureza, que diariamente afetam e acarretam novos usuários, resultando também em um aumento no número de vítimas. Nesse sentido, o delito de estelionato digital é um assunto recentemente discutido nos tribunais e no Estado brasileiro, especialmente quando se trata da aplicação da legislação, uma vez que o acesso à internet tem permitido cada vez mais usuários envolvidos.

O crime de estelionato cresce a cada dia mais, em virtude de os agentes conseguirem escapar com facilidade das punições, pois as redes sociais não dão suporte eficaz para que o agente seja identificado e punido.

Complementam Cruz e Rodrigues (2018) que são muitas as dificuldades do Ministério Público, da Polícia e do Poder Judiciário para configurar a punição aos criminosos que praticam o estelionato virtual, essas dificuldades tendem a gerar

uma sensação de impunidade, levando as pessoas a relacionarem essa sensação à falta de leis específicas que abordem os crimes cibernéticos.

A ausência de legislação específica acerca do tema pode auxiliar os criminosos a praticarem a infração, pois confiam na impunidade, devido a falta do instrumento normativo específico. (FEITOZA, 2012). São diversos os problemas que envolvem o estelionato virtual, dentre eles se destacam: a dificuldade na identificação dos agentes do fato, a delimitação do local do crime, e, o juízo competente.

Haja vista, a ausência de norma reguladora não é o único problema existente ao crime de estelionato virtual, há também dificuldades na localização do autor do crime, delimitação do local e competência para julgamento do delito. Dessa forma, por inexistir norma especifica que trate do crime de estelionato virtual, a população tende a ter uma certa sensação de impunidade, no entanto cresce as dificuldades de punição aos agentes infratores, abrange também as facilidades proporcionadas pelas redes sociais, onde o agente pode com facilidade alterar ou apagar dados, e até mesmo se usar de perfis falsos na maioria das vezes, dificultando ainda mais a sua identificação correta.

Ao contrário do que muitos acreditam, os crimes cometidos através da internet possuem tipificação legal e, quando os autores do delito são identificados, há punição penal. Apesar disso, o preâmbulo do dispositivo legal não faça menção ao termo “internet”, o fato dos sujeitos se utilizarem da rede mundial de computadores para praticar o ilícito, tem-se que a consumação possui tipificação, devendo ser aplicadas as sanções previstas (CRUZ; RODRIGUES, 2018).

A Lei 13.964/2019 (Pacote Anticrime) modificou a natureza da ação penal no crime de estelionato, incluindo o § 5º no artigo 171, com a seguinte redação:

> § 5º Somente se procede mediante representação, salvo se a vítima for: I - a Administração Pública, direta ou indireta; II - criança ou adolescente; III - pessoa com deficiência mental; ou IV - maior de 70 (setenta) anos de idade ou incapaz (BRASIL, 2019, online).

Antes da referida lei, a ação penal em regra seria pública incondicionada, sendo ressalvadas as exceções trazidas no artigo 182 do Código Penal. A partir da alteração, tem-se a representação como condição de procedibilidade para instauração da ação penal, ressalvadas as hipóteses dos incisos I a IV.

Em suma, o crime de estelionato virtual, está tipificado no art. 171, do Código Penal, assim, os agentes que praticarem o fato, irão incidir nas penas deste artigo, abrangendo o crime de estelionato de uma forma geral. Ficou evidenciado que os problemas decorrentes da ausência da norma não dizem respeito a tipificação do delito, mas sim com a localização do infrator, local do crime e competência, fatos que tornam a norma vigente, sendo insuficiente quando se trata do crime de estelionato virtual especificadamente, e assim, levam a uma sensação de impunidade.

Realizadas essas considerações, sabe-se que inexiste até o momento norma que preveja expressamente o crime o estelionato virtual especificadamente, sendo necessário então no item a seguir apresentar os projetos de lei em tramitação, que cuidam de forma específica do crime em questão.

3.1 DOS PROJETOS DE LEI SOBRE O TEMA

O estudo que aqui se pretende, será sustentado principalmente na avaliação ao Projeto de Lei do Senado nº 3.376/20; ao Projeto de Lei do Senado nº 9.441/17 e ao Projeto de Lei da Câmara nº 4.229/15 que, de acordo com a pesquisa realizada, nos sites da Câmara de Deputados e do Senado Federal, são os projetos de lei que estão em tramitação que tratam da matéria.

O Projeto de Lei 3.376/20 foi idealizado em prol do aumento de golpe estelionatário em âmbito virtual. A ementa refere-se em alterar o Decreto-Lei nº 2.848, de 7 de dezembro de 1940, para estabelecer majorante para o crime de estelionato virtual. Pela redação essa modalidade teria pena de reclusão, de 2 a 10 anos e multa, que se confrontada ao estelionato comum, é sancionada com o dobro (AGÊNCIA CÂMARA DE NOTÍCIAS, 2020).

> O estelionato virtual será caracterizado, conforme o texto, se o crime for cometido mediante invasão, adulteração ou clonagem de aplicativo de mensagens instantâneas e de chamadas de voz para telefones celulares ou com o emprego da internet, de dispositivo de comunicação ou de sistema informatizado (AGÊNCIA CÂMARA DE NOTÍCIAS, 2020, p.01).

Importante frisar que, este Projeto de Lei foi apensado na data 04/12/2020 ao Projeto de Lei 9.441/17, uma vez que, os assuntos e propostas são semelhantes.

O Projeto de Lei 9.441/17, tem como proposta alterar o art.171 do Decreto-Lei n. 2.848, de 7 de dezembro de 1940 - Código Penal para estabelecer aumento

de pena a prática do estelionato virtual. Em sua redação, destacam-se sobre o uso da internet pelos agentes, com objetivo de alcançar benefícios ilícitos, sendo que estes deveriam estar sujeitos a penas mais severas quando praticarem tal delito (BRASIL, 2017). O Deputado Moises Rodrigues, anexou ao Projeto de Lei em sua justificação as palavras de Damásio de Jesus e José Antônio Milagre.

> O Brasil passou a tratar e se preocupar com o tema nas últimas duas décadas. Hoje, o país é o quarto do mundo com maior número de ameaças virtuais. Pesquisas sempre revelaram que o Brasil está na rota dos crimes cibernéticos. De acordo com a polícia federal em notícia do ano de 2004, de 10 hackers ativos no mundo 8 vivem no Brasil(...). A web permite que os criminosos tenham acesso a muitas vítimas, logo, estamos a falar da escalabilidade do cibercrime. Além disso, técnicas são utilizadas e crackers recrutados para ocultar atividades de criminosos. As invasões às estruturas críticas dos países crescem a ritmo inimaginável e no Brasil não é diferente (JESUS, 2016. p.26).

Já o Projeto de Lei 4.229/15, tem como ementa aumentar as penas dos agentes que cometem o crime de estelionato, com enfoque em golpes de endividamento das vítimas, vendas de bens, saques de quaisquer tipos de aplicações financeiras, entre outros. A pena prevista é de até sete anos e meio de reclusão, vez que, atualmente a pena atualmente prevista é de 1 a 5 anos de reclusão e multa. O mesmo se encontra em espera para apreciação do Senado Federal (BRASIL, 2015).

O autor da proposta é o deputado Marcelo Belinati (PP-PR), que argumenta que o principal objetivo é desestimular os agentes na aplicação de golpes que impliquem em endividamento das vítimas, ou que as façam perder os bens. Ele ainda argumenta sobre a importância de proteger os idosos e vulneráveis quando se trata do crime de estelionato, assim, mencionou na nova ementa do Projeto de Lei que é necessário incluir no rol de crimes hediondos o crime de estelionato que for contra idoso e vulnerável (AGÊNCIA CÂMARA DE NOTÍCIAS, 2015).

> São bastante conhecidas histórias de idosos que passaram a arcar com descontos em seu benefício do INSS para o pagamento de empréstimos consignados que nunca contraíram. Também não faltam casos de servidores públicos que, um belo dia, descobriram débito semelhante em seu contracheque sem jamais terem visto a cor do dinheiro fruto do empréstimo (AGÊNCIA CÂMARA DE NOTÍCIAS, 2021, p.01).

Feitoza (2012), tendo em vista os graves danos causados pelo crime de estelionato virtual à sociedade, ressalta que o delito merece atenção especial do legislativo brasileiro. Os projetos em tramitação no Congresso necessitam de atenção para que tenham aprovação dos deputados e dos senadores. Todos os dias, novos usuários tornam-se vítimas desses criminosos, que se aproveitam da falta de fiscalização para enganar as vítimas e fornecer-lhes bens e serviços sem cumprir as obrigações acordadas, causando prejuízos irreparáveis.

O crime de estelionato virtual deve ser objeto de atenção pelos legisladores, pois tem provocado grande impacto na sociedade, assim, não se pode mais retardar os projetos em tramitação. A cada dia aumentam os casos de pessoas que se tornam vítimas de tal crime, pois os criminosos aproveitam da facilidade virtual para aplicar o golpe, principalmente através das redes sociais com intenção de obter vantagem ilícita (JESUS, 2016).

De acordo com o disposto estima-se que, embora tenha havido Projetos de Lei para aumento de pena na conduta de estelionato virtual, não se obteve êxito, até então, permanecendo inalterado o texto do Código Penal, e sem qualquer norma especifica que trate do assunto.

CONSIDERAÇÕES FINAIS

No presente trabalho, apresentou-se uma abordagem sobre o crime de estelionato e suas implicações na era digital, seu constante crescimento dentro das redes sociais atualmente. As plataformas têm sido ferramenta dos criminosos para captação de vítimas e aplicações dos golpes. Foram apresentadas propostas do combate ao crime de estelionato virtual, e exposto como o ordenamento jurídico se aplica e se atualiza sobre este crime, inclusive foi mencionando projetos de lei acerca do tema.

No capítulo I, observou-se a tipificação e classificação do crime de estelionato, que está previsto no artigo 171 do Código Penal. Configura-se crime de estelionato quando o agente obtém, para si ou para outrem, vantagem ilícita, em prejuízo da vítima, a qual por sua vez, é induzida ou mantida em erro, mediante qualquer meio fraudulento, punindo com pena de reclusão de um a cinco anos e multa. Também foi exemplificado o crime de estelionato virtual, visto que, é um crime no qual o agente servindo-se de equipamentos tecnológicos e acesso à rede, utiliza-se dos meios fraudulentos para obter uma vantagem ilícita, tendo acesso e utilizando os dados da vítima, fotos, número de telefone, entre outros. Nota-se que, não existe uma legislação específica sobre o crime de estelionato virtual, haja vista o delito tem previsão legal no rol dos crimes praticados contra o patrimônio, no capítulo VI, que trata do estelionato e outras fraudes, disposto no artigo 171, do Código Penal.

Dessa forma, destacou-se que para a consumação do crime não importa se a fraude é civil ou penal, basta que seja uma fraude. Há apenas um dimensionamento da qualidade e grau da fraude, que serão verificados caso a caso. Através da avaliação do caso concreto que se verificará, como a vítima foi prejudicada, e se realmente foi induzida ou mantida em erro, por ato fraudulento daquele com quem negociou.

Mostra-se ainda no capítulo I, que as redes sociais vem sendo um dos principais meios de captação de vítimas para os criminosos, que aproveitam da facilidade do mundo virtual, e, por ser onde concentra-se o maior número de pessoas nos dias atuais, utilizando-as principalmente como meio de comunicação. Assim, os agentes enganam as vítimas mais vulneráveis, e até mesmo se passam por alguém que a vítima conhece para que obtenham sucesso rápido no delito.

No capítulo II, dissertou-se a respeito das propostas para o combate ao crime de estelionato virtual. Sobre os principais pontos estratégicos para colaborar neste combate, destaca-se em como denunciar um crime cibernético, seja em Delegacia Especializada ou Comum. Abordou-se o registro das evidências em cartório como Ata Registral, que se torna de suma importância como prova de veracidade dos fatos.

Porém, um ponto controverso trazido pelo capítulo, foi o que para a obtenção do sucesso nas investigações, mesmo que as vítimas colaborem com as provas documentais, as redes sociais também devem fornecer informações no decorrer da investigação. Foi exposto que, além do longo processo, o problema da recusa das empresas de informação em prestar assistência às autoridades policiais e judiciais é evidente. A juntada de provas nos cibercrimes se torna bastante complexa, pois a vítima não fica “cara a cara” com o criminoso, assim, o mesmo consegue efetuar o crime sem ser claramente identificado, manipulando a vítima ou até mesmo se passando por outra pessoa. Sendo de suma importância, a coleta das informações dos crimes virtuais em tempo hábil, antes que elas desapareçam, é uma tarefa muito difícil. No entanto, viu-se que, uma vez concluída, o objetivo da investigação é descobrir o IP da máquina e seus logs (ou seja, seus registros de login), que são umas das formas de identificar o culpado.

Indo além, a pesquisa demonstrou que existem poucas unidades de delegacias especializadas em crimes virtuais nos estados brasileiros. Com um número reduzido de locais especializados, e com profissionais ainda insipientes na temática, torna-se difícil a investigação, devido a grande quantidade de casos existentes e poucos profissionais para lidar com a temática.

Outro ponto essencial no combate ao aumento deste delito, que a pesquisa demonstrou, consiste na propagação da educação digital. Os criminosos cibernéticos aplicam golpes abusando da boa-fé e inocência das pessoas, e a falta de conhecimento ajuda na efetivação de um golpe malicioso. Dessa forma, com a educação digital propagada, torna-se mais efetiva a defesa e prevenção de qualquer contra ataques cibernéticos, principalmente o de estelionato.

Vale ressaltar que, crianças e pessoas com condições especiais, não poderão ser sujeitos passivos desse crime, pois é indispensável para a consumação da fraude, que se crie ou mantenha alguém em erro. E para que a vítima possa ser enganada é imprescindível que ela tenha capacidade de discernimento.

Mostra-se que, os governos devem avaliar as atuais políticas e práticas de segurança cibernética à medida que o mundo continua a mudar, uma vez que, se a medida de segurança cibernética evoluir, será favorável aos resultados do combate ao crime em ambiente virtual.

No capítulo III, é dado espaço sobre a contextualização do ordenamento jurídico brasileiro, visto que, o artigo 171 do Código Penal aborda sobre o crime de estelionato, não importando por qual meio foi efetuado o crime, sendo assim, o praticado em ambiente virtual, também está tipificado neste artigo. Mostra-se que são muitas as dificuldades do Ministério Público, da Polícia e do Poder Judiciário para configurar a punição aos criminosos que praticam o estelionato virtual, estas dificuldades tendem a levar a uma sensação de impunidade. Assim, a ausência de norma reguladora não é o único problema existente ao crime de estelionato virtual, há também dificuldades na localização do autor do crime, delimitação do local e competência para julgamento do delito.

Mostra-se ainda no capítulo III os projetos de lei sobre o tema. O crime de estelionato virtual deve ser objeto de atenção pelos legisladores, pois tem provocado grande impacto na sociedade, assim, não podendo retardar os projetos em tramitação acerca do tema, sendo a majoração das penais uma possível solução e proposta para combate ao crime de estelionato virtual.

Ante ao exposto, pode-se observar que, o Estado se encontra parcialmente vulnerável perante os criminosos virtuais, apesar de que se tem percebido que algumas medidas estão sendo adotadas para coibir esta prática, como por exemplo, a criação de delegacias especializadas, o treinamento e aperfeiçoamento dos policiais e outros profissionais que lidam com esta prática cotidianamente, além do entendimento dos juízes no âmbito dos tribunais, visando unificar alguns entendimentos sobre o mesmo tema.

REFERÊNCIAS

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

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

BRANCO, D. C. **Golpes virtuais**: veja como funcionam as duas principais abordagens dos criminosos. 2021.

BRASIL. Câmara dos Deputados. **Projeto de Lei n° 4229, de 22 de dezembro de 2015.** Altera o Código Penal para aumentar a pena prevista para o crime de estelionato quando levar a endividamento, venda de bens ou saque de qualquer tipo de aplicação financeira da vítima. Brasília: Câmara dos Deputados, 2015. Disponível em: https://www.camara.leg.br/propostas-legislativas/2076094. Acesso em: 20 de set. 2023.

_____. Câmara dos Deputados. **Projeto de Lei n° 9441 de 20 de dezembro de 2017.** Altera o art.171 do Decreto-Lei n. 2.848, de 7 de dezembro de 1940 - Código Penal para estabelecer como causa especial de aumento de pena a prática do estelionato pelo meio eletrônico. Disponível em: https://www.camara.leg.br/propostas-legislativas/2167149. Acesso em: 20 de set. 2023.

_____. Câmara dos Deputados. **Projeto de Lei n° 3316 de 17 de junho de 2020.** Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940, para estabelecer majorante para o crime de estelionato virtual. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2255409. Acesso em: 22 de set. 2023.

_____. **Decreto-lei nº 2.848, de 07 de dezembro de 1940**. Código Penal. Disponível em: https://www.planalto.gov.br/ccivil_03/DecretoLei/Del2848compilado.htm. Acesso em: 06 de nov. 2023.

_____. **Lei n° 13.964, de 24 de dezembro de 2019.** Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13964.htm> Acesso em: 22 de nov. 2023.

BRITO, Auriney. **Direito penal informático**. São Paulo: Saraiva, 2013. 189 p.

CAPEZ, Fernando. **Curso de Direito Penal.** Parte Geral**.** Vol. 1, 18ª ed. São Paulo: Saraiva, 2014.

_____. **Parte especial arts.121 a 212**. **Coleção Curso de direito penal.** Vol. 2, 20. ed. São Paulo: Saraiva Educação, 2020.

_____. **Parte especial arts. 213 a 359**. Coleção Curso de direito penal. Vol. 3, 18**.** ed. São Paulo: Saraiva Educação, 2020.

CARDOSO, L. de H. M.; FRACASSO, C. R.; MARIN, M. M. A. **O direito na era digital:** o Cibercrime no Ordenamento Jurídico Brasileiro. 2018. Disponível em: <https://cepein.femanet.com.br/BDigital/arqPics/1611400792P734.pdf> Acesso em: 20 set. 2023.

CASSANTI, Moisés de Oliveira. **Crimes virtuais, vítimas reais**. Rio de Janeiro: Brasport, 2014.

CERT. BR. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança No Brasil. Cartilha de Segurança para Internet: **Ransomware.** Disponível em: <http://cartilha.cert.br/ransomware/> Acesso em: 20 set. 2023.

CONSELHO NACIONAL DE JUSTIÇA – CNJ. **Ações de Direito do Consumidor**. 2018. Disponível em: https://www.cnj.jus.br/sgt/consulta_publica_assuntos.php. Acesso em: 15 de set. 2023.

CORRÊA, Gustavo Testa. **Aspectos Jurídicos da Internet**. São Paulo: Saraiva, 2000. p. 170.

CRUZ, Diego; RODRIGUES, Juliana. Crimes Cibernéticos e a Falsa Sensação de Impunidade. **Revista Científica Eletrônica do Curso de Direito**, v. 13, jan. 2018. Disponível em: <http://faef.revista.inf.br/imagens_arquivos/arquivos_destaque/iegWxiOtVJB1t5C_2019-2-28-16-36-0.pdf> Acesso em: 19 ago. 2023.

DE INELLAS, Gabriel Cesar Z. **Crimes na internet.** 2. ed. São Paulo: Juarez de Oliveira, 2009.

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: 19 ago. 2023..

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

_____. **Curso de direito penal:** parte especial, volume 3. 12. ed. Niterói: Impetus, 2015. 769 p.

_____. **Curso de Direito Penal**. 20. Ed. Rio de Janeiro: Impetus, 2018.

GUSTIN, Miracy Barbosa de Souza; DIAS, Maria Tereza Fonseca. **(Re)pensando a pesquisa jurídica:** teoria e prática. 3 ed. Belo Horizonte: Del Rey, 2010.

HUNGRIA, Nelson. **Comentários ao Código Penal.** Vol. IX. Rio de Janeiro: Forense, 1958.

JESUS, Damásio E. de. **Direito penal.** Vol. 3: parte especial. 32. ed. São Paulo: Saraiva, 2012.

_____. **Direito penal**. Vol.2. 33 ed. São Paulo: Saraiva, 2013.

_____. **Manual de crimes informáticos**. São Paulo: Saraiva, 2016.

JESUS, Damásio E. de; MILAGRE, José Antonio**. Marco Civil da Internet:** Comentário à Lei 12.965/14. 1. ed. São Paulo: Saraiva, 2014.

KASPERSKY. **Brasileiros são maiores vítimas de golpes phishing no mundo**. 2018. [Internet]. Disponível em: https://www.kaspersky.com.br/blog/phishing-klsec-brasil-assolini/10642/ Acesso em: 10 set. 2023.

LUDGERO, Paulo Ricardo. **O que são *Scammers*?** Entenda a fraude. Disponível em: <https://ludgeroadvocacia.jusbrasil.com.br/artigos/883306590/o-que-sao-scammers-entenda-a-fraude> Acesso em: 12 de set. 2023.

MARTELETO, Regina Maria. Análise de redes sociais: aplicação nos estudos de transferência da informação. **Ciência da Informação**. Brasília, v.30, n.1, p. 71-81, Instituto Brasileiro de Informação em Ciência e Tecnologia, 2001.

MARTINS, Patrícia Vieira. **Crimes Cibernéticos e a Correlação Ao Crime Contra Honra**. 2012. Disponível em:http://revistas.unifenas.br/index.php/BIC/article/download/192/146. Acesso em: 17 de nov. 2023.

NASCIMENTO, Anderson. **O** que é backbone? **CanalTech**. 2018. Disponível em: https://canaltech.com.br/telecom/o-que-e-backbone/. Acesso em: 19 out. 2023.

PINHEIRO, Patrícia Peck. **Proteção de dados pessoais**: Comentários à Lei 13.709/2018 - LGPD**.** São Paulo: Saraiva, 2020.

PINHEIRO, Reginaldo César. Os cibercrimes na esfera jurídica brasileira. 2000. **Revista Eletrônica Jus Navigandi**. Disponível em: <http://jus.com.br/revista/texto/1830/os-cybercrimes-na-esfera-juridica-brasileira>. Acesso em: 15 de set. 2023.

ROSA, Fabrízio. **Crimes de informática**. Campinas: Bookseller, 2005, 2ª Edição.

ROSSINI, Augusto Eduardo de Souza. **Informática, Telemática e direito penal**. São Paulo: Memória jurídica, 2004.

WENDT, Emerson; JORGE, Higor Vinicius Nogueira. **Crimes Cibernéticos**: Ameaças e Procedimentos de Investigação. 2. ed. Rio de Janeiro: Brasport, 2013. Disponível em: <https://pt.scribd.com/read/436286113/Crimes-ciberneticos-ameacase-procedimentos-de-investigacao-2%C2%AA-Edicao. Acesso em: 02 de nov. 2023.