CENTRO UNIVERSITÁRIO DO ESTADO DO PARÁ
CURSO DE BACHARELADO EM DIREITO

DIEGO MOREIRA DA SILVA CASTRO
ENZO SERRUYA SAIFE

CRIMES VIRTUAIS: uma análise do delito estelionato virtual

BELÉM
2022

DIEGO MOREIRA DA SILVA CASTRO
ENZO SERRUYA SAIFE

CRIMES VIRTUAIS: uma análise do delito estelionato virtual

Trabalho de Conclusão de Curso apresentado como requisito parcial para obtenção de grau em Bacharel em Direito, pelo Centro Universitário do Estado do Pará.

Orientadora:Prof.ª Me. Luciana Correa Souza Matni

BELÉM
2022

Dados Internacionais de Catalogação na Publicação (CIP)
Biblioteca do CESUPA, Belém – PA

C355c Castro, Diego Moreira da Silva

Crimes virtuais: uma análise do delito estelionato virtual / Diego Moreira da Silva Castro, Enzo Serruya Saife. – Belém, 2022.

24 p.

Trabalho de Conclusão de Curso (Graduação) – Centro Universitário do Estado do Pará, Bacharelado em Direito, Belém, 2022.
Orientadora: Profa. Ma. Luciana Correa Souza Matni

1. Crimes virtuais. 2. Estelionato. I. Saife, Enzo Serruya. II. Matni, Luciana Correa Souza (orient.) III.Título.

CDD 341.5

Regina Coeli Araújo Ribeiro CRB-2/739

DIEGO MOREIRA DA SILVA CASTRO
ENZO SERRUYA SAIFE

CRIMES VIRTUAIS: uma análise do delito estelionato

Trabalho de Conclusão de Curso apresentado como requisito parcial para obtenção de grau em Bacharel em Direito, pelo Centro Universitário do Estado do Pará.

Orientadora:Profª. Me. Luciana Correa Souza Matni

Data de aprovação: _____/_____/_____

Conceito:

Banca Examinadora:

_____
Prof.ª Me. LUCIANA CORREA SOUZA MATINI - Orientadora
Centro Universitário do Estado do Pará (CESUPA)

_____
Nome com titulação
Instituição a que pertence

_____
Nome com titulação
Instituição a que pertence

CRIMES VIRTUAIS: UMA ANÁLISE DO DELITO ESTELIONATO VIRTUAL

VIRTUAL CRIMES: AN ANALYSIS OF THE CRIME VIRTUAL LARCENY

Diego Moreira da Silva Castro[1]
Enzo Serruya Saife[2]
Luciana Correa Souza Matni[3]

RESUMO: O artigo tem como finalidade examinar o aumento dos crimes de estelionato nos meios virtuais e como o direito penal tem sido ausente em acompanhar a modernização deste delito. No âmbito dos aspectos metodológicos, a partir de um levantamento bibliográfico e documental, na primeira seção, analisar-se-á os avanços da tecnologia e conformidade com os riscos penais existentes dentro da internet. Em seguida, passa-se a análise do crime de estelionato propriamente dito e sua aplicação nos meios virtuais, em um primeiro momento, de forma sucinta, a relacionando-o com o saber criminológico crítico, a fim de fornecer substrato teórico para a discussão. Posteriormente, na terceira seção, far-se-á um exame do aumento na utilização dos meios tecnológicos pela sociedade em conjunto com a análise do aumento dos crimes de estelionato virtual, e como o direito penal vem sendo ausente na aplicação de sanções para este delito. Bem como, apontando eventuais falhas e lacunas em sua construção ao longo de sua formulação. Assim, buscar-se-á responder ao seguinte problema de pesquisa: De que modo e quais as dificuldades que o Direito Penal encontra no combate ao crime de estelionato cometido em ambiente virtual?
Palavras-Chave: Direito Penal; Crimes Virtuais; Estelionato.

ABSTRACT: This article aims to examine the increase of larceny crimes through virtual means and how criminal law has been absent in keeping up with the modernization of this offense. In the scope of the methodological aspects, from a bibliographic and documental survey, the first section will analyze the advances in technology and conformity with the existing criminal risks within the internet. Then, the crime of larceny itself and its application through virtual means will be analyzed, in a first moment, briefly, relating it to the critical criminological knowledge, in order to provide a theoretical substrate for the discussion. Subsequently, in the third section, an examination will be made of the increase in the use of technological means by society in conjunction with the analysis of the increase in crimes of virtual larceny, and how criminal law has been absent in the application of sanctions for this offense. As well as, pointing out possible flaws and gaps in its construction along its formulation. Thus, we will try to answer the following research problem: How and what are the difficulties that Criminal Law encounters in combating the crime of larceny committed in the virtual environment?

Keywords: Criminal Law; Virtual Crimes; Fraud.

[1] Graduando em Direito pelo Centro Universitário do Estado do Pará (CESUPA). E-mail: Diego Moreira da Silva Castro

[2] Graduando em Direito pelo Centro Universitário do Estado do Pará (CESUPA). E-mail:enzosaife@live.com

[3] Professora Orientadora. Advogada. Doutoranda em Direito Penal pela Universidade de São Paulo (USP). Mestre em Direito pela Universidade Federal do Pará (UFPA). E-mail: lucianacsouza.adv@gmail.com.

1 INTRODUÇÃO

O presente trabalho tem como objetivo analisar o aumento dos crimes e quais riscos penais que estão presentes na prática do crime de estelionato virtual, bem como, vislumbrar a conceituação do crime de estelionato virtual e quais suas modalidades que são utilizadas pelos criminosos na prática deste delito. Com o intuito de responder o seguinte problema de pesquisa, de que modo e quais as dificuldades que o Direito Penal encontra no combate ao crime de estelionato cometido em ambiente virtual?

O estudo tem seu desenvolvimento por meio do levantamento bibliográfico dos principais penalistas e doutrinadores dos crimes virtuais, sendo estes, Cintra (2009), Teffé (2017), Mirabete (2008), Hungria (1958), Antunes (2020), Greco (2019), Lima (2011), Oliveira (2020), Amoras (2020), Goodman (2015), Rangel (2014), Marra (2019), já a doutrina utilizada de forma essencial para a construção do presente artigo será Bittencourt (2018) e Filho (2018).

A primeira seção tem por finalidade mostrar de forma tanto teórica quanto exemplificativa os riscos existentes no crime de estelionato virtual e, de que maneira tal crime repercute para a vida das vítimas. Dando prioridade no que tange ao risco patrimonial, que poderá ser atingido por meio de sites falsos, e-mails, e outros mecanismos que podem ser utilizados pelos estelionatários para a consumação desse delito, para que desta compreenda-se como este delito está presente no dia a dia da sociedade, e como tal encontra-se vulnerável diante do conhecimento técnico que estes agentes possuem comparado com suas vítimas.

Na segunda seção, examinar-se-á a conceituação do crime de estelionato propriamente dito. Para que assim possa se ter base para uma compreensão mais detalhada do crime de estelionato no ambiente virtual. Adentrando o objeto pretendido no crime, o sujeito ativo e passivo e como ele é tratado pela doutrina penal pátria e pelos dispositivos legais dispostos no Código Penal Brasileiro. Após compreender o crime de estelionato virtual, analisar-se-á como este crime é dividido em suas modalidades e como cada uma é aplicada e consumada pelos criminosos, compreendendo suas peculiaridades e meios que os estelionatários utilizam.

Após a abordagem dos riscos e das modalidades do crime de estelionato virtual, na terceira seção se terá o foco na questão do avanço da tecnologia, e como a tecnologia se demonstra cada vez mais necessária para o dia a dia da sociedade. Em que se disporá sobre como este aumento do número de usuários teve colaboração no aumento do crime de estelionato, através do demonstrativo de dados e estatísticas que apresentam um aumento

significativo do crime de estelionato nos últimos anos, principalmente, após o período pandêmico.

Por fim, tem-se por objetivo demonstrar que apesar de existir dispositivo legal que trate dos crimes virtuais, este dispositivo não se vem mostrando eficaz na contenção da prática do delito de estelionato no ambiente virtual.

Em tal seção abordar-se-á a carência jurídica presente nos processos não só de sanção, como também os de investigação para este delito. Posto isso, o que se vem tratar na última seção será a questão da carência jurídica penal diante da modernidade tecnológica e como esta modernidade também vem modernizando as práticas delituosos nos meios virtuais, de tal modo que gere muita dificuldade para o Estado em acompanhar o avanço na prática deste crime, fazendo-se necessário que o direito acompanhe o avanço da tecnologia para que haja a eficácia na contenção destes novos aparatos tecnológicos que são utilizados pelos criminosos.

2 AS NOVAS TECNOLOGIAS E OS NOVOS RISCOS PENAIS

Iniciando-se a discussão do presente trabalho, é necessário, primordialmente, abordar nessa seção os avanços da modernidade tecnológica, mudanças essas que corroboram com uma nova realidade social, onde é possível vislumbrar-se uma espécie de novo mundo e com ele novas oportunidades, tanto de comunicação, como é o caso das redes sociais, como mercadológica no caso dos shoppings virtuais. Desta maneira, dada a este novo meio ambiente, compôs-se um universo de possibilidade, no entanto, com este, surgem em consonância, riscos penais, os quais deixam suscetíveis os indivíduos da sociedade brasileira, permitindo que novos crimes sejam elaborados.

Os novos riscos surgem da adaptação dos indivíduos aos novos universos virtuais, onde agentes maliciosos utilizam-se desta ferramenta para a elaboração e a aplicação de novos crimes penais em meios virtuais, esta possibilidade demonstra como a comunidade está vulnerável diante dos avanços tecnológicos, bem como a necessidade de adaptação dos códigos legais, de modo que estes consigam evitar ou mesmo barrar ações criminosas.

Atualmente, com o avanço da tecnologia e com surgimento dos meios virtuais, a sociedade vem sendo com o passar do tempo mais dependente da facilidade e praticidade que a tecnologia atribui para seus usuários. Para muitas pessoas, a internet tornou-se um instrumento de extrema utilidade e necessidade para aqueles que a usufruem cotidianamente, tendo em vista

sua utilidade de diversas maneiras, tais como no trabalho, lazer, financeira dentre outros benefícios que esta nova realidade traz para o dia a dia de uma sociedade (CINTRA, 2009).

Apesar de a internet trazer muitos benefícios para seus usuários haverá aqueles que utilizar-se-ão dela de forma ilícita e criminosa para alcançar os seus objetivos, em que quanto mais se tem o avanço da tecnologia, mais aumenta-se os riscos nos meios virtuais e a vulnerabilidade que os seus usuários possuem (BITTENCOURT, 2018).

Inicialmente, para uma melhor compreensão dos riscos existentes na internet, faz-se necessário citar os princípios, garantias e direitos resguardados com o marco civil da internet, os quais serão fundamentais para respaldar os usuários desta nova tecnologia.

O direito respalda-se em três princípios, os quais regem a internet, estes são: a) princípio da neutralidade da rede; b) princípio da privacidade; c) princípio da liberdade de expressão. Para o presente artigo, dois destes princípios são de suma importância para adentrarmos nos riscos que podem ser ocasionados com os crimes virtuais (DE TEFFÉ, 2017).

Deste modo, pode-se observar, que o princípio da neutralidade da rede traz a garantia de que todos tenham acesso à internet e a qualquer tipo de informação contida nela sem qualquer descriminação, não havendo nenhum requisito para diferenciar o acesso de um usuário ao de outro, demandando que a operadora que ofereça o serviço de internet, mantenha de forma imparcial a todos e independentemente do conteúdo. (ABDET, 2015, p.3).

Este princípio corrobora com a democratização do novo espaço virtual, possibilitando que os indivíduos, independente de gênero, raça ou credo, tenham acesso a esta nova plataforma e desta forma possam usufruir de todas as ferramentas e serviços que a internet possa disponibilizar, por isso, ele é um fundamental garantidor de liberdades e direitos aos personagens sociais.

Do mesmo modo, o princípio da privacidade visa proteger todas as informações que são consideradas segredo ou sensíveis para os usuários, logo, serão mantidas em sigilo, para não serem compartilhadas ao público. Só haverá exceção ao princípio com devida autorização judicial, como estabelecido no art. 21 do Código Civil de 2002: “A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma”.

Desta maneira, observando a possibilidade de compartilhamento virtual, e como neste os dados podem ser difundidos mais rapidamente e sem qualquer filtro, tornar-se substancial que certas informações sejam mantidas em sigilo, como é caso de dados particulares e informações pessoais, como extrato bancário, ou mesmo os números de documentos individuais

como a carteira de identidade e o cartão de crédito, por isso, o princípio da privacidade é um dos pilares virtuais, o qual deve ser respeitado.

De igual importância, o princípio da liberdade de expressão está previsto no art. 5°, IV e IX da Constituição Federal de 1988, a carta fundamental que rege a sociedade brasileira, nela é vista a permissão do indivíduo manifestar-se sem medo de ser coagindo, fornecendo sua opinião, ou visão, acerca de determinado assunto. De igual maneira, no universo virtual, este direito fundamental deve ser respeitado, para que os indivíduos possam interagir, sem receios em relação às suas falas. Vale ressaltar ainda, que é necessário compreender os limites, os quais devem permear o direito de expressão, de modo que haja uma justa convivência no meio virtual.

Com base nos princípios apresentados, entende-se que os usuários, dentro deste mundo virtual, devem ter seus direitos básicos protegidos e assegurados, direitos estes como o da garantia de sua saúde mental, de sua honra, de sua dignidade individual, do patrimônio, a não divulgação dos seus dados pessoais, de sua intimidade e da sua liberdade ao uso dos meios virtuais.

Embora, o presente trabalho venha a declinar-se a analisar os riscos citados, o foco será direcionado a violação do direito patrimonial do indivíduo, posto que quando se trata do crime de estelionato virtual, o bem jurídico tutelado será o bem material, por isso, em que pese saber-se que existem outros riscos aos indivíduos, como é o caso da violação da liberdade de expressão, este artigo focar-se-á em estudar o crime patrimonial em forma do estelionato virtual, no intuito de compreender a crescente desta forma de delito e como a falta do Direito Penal Brasileiro em acompanhar o avanço deste em conjunto com o avanço da tecnologia, causa impacto na sociedade.

Com isso posto, ao se aprofundar no crime de estelionato, é possível afirmar que os riscos que envolvem esta modalidade são de cunho patrimonial, isto é, a vítima deste crime está suscetível a ter a integridade de seus bens maculada, ou seja, os agentes criminosos utilizam-se de falsa percepção para subtrair bens dos indivíduos.

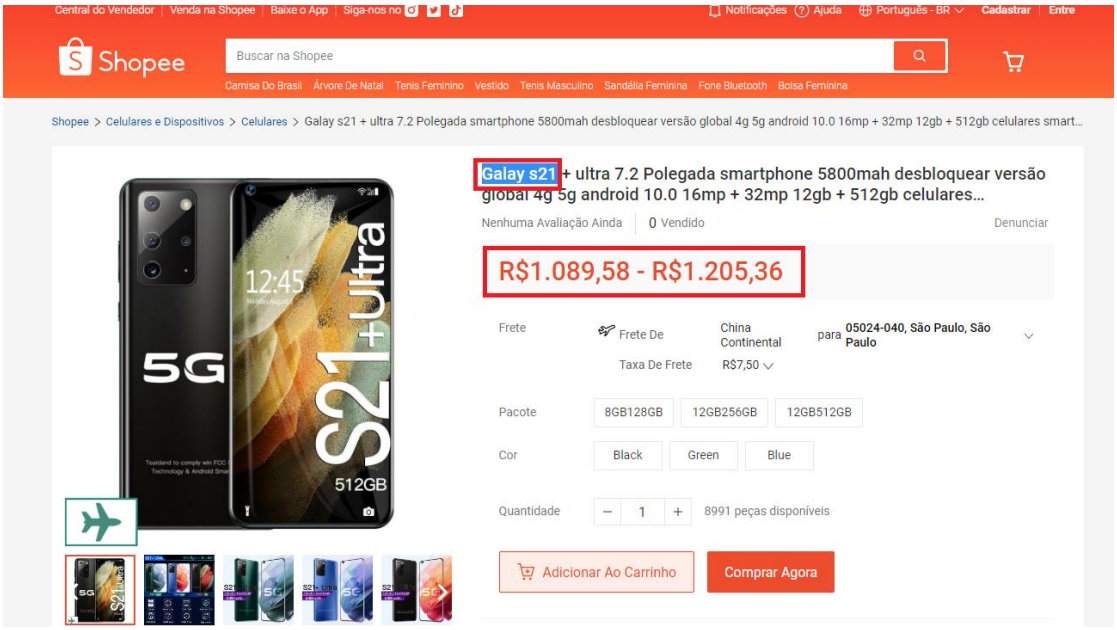
Para entendermos tal risco, deve-se adentrar na concepção das palavras chaves que consubstanciam a prática do estelionato, que por utilizar-se de uma falsa percepção e da boa-fé da vítima cometem o crime, ou seja por meio de mentiras, falsificações e acima de tudo a vulnerabilidade da vítima, aproveitam-se para subtrair seu patrimônio de forma indevida (MIRABETE, 2008).

A vulnerabilidade da vítima se dá pela falta de conhecimento na utilização dos meios virtuais, em que essa falta de entendimento e percepção do que é verdadeiro e o que não é dentro da internet, a torna um alvo muito fácil para os estelionatários. No crime de estelionato virtual

se tem o dano financeiro quanto aos bens da vítima, em que seus cruciais pontos são a vulnerabilidade técnica dos usuários perante a utilização dos meios de compra e a falsa percepção que é gerada dentro da internet pelos criminosos, colabora para o risco no dano financeiro que a vítima possa vir a sofrer de tal crime. Vale ressaltar que muito desta vulnerabilidade, também é gerada pelo anonimato que é utilizado por estes agentes, que por meio deste anonimato, tem grande vantagem na aplicação do golpe. (HUNGRIA, 1958).

É certo que o crime de estelionato pode ser cometido de variadas formas pela internet, e um exemplo de meio a ser utilizado são os sites de vendas. Existem inúmeros sites de compra e venda, tais como a OLX, Mercado Livre, Aliexpress, Shopee, dentre outros, que apesar de serem sites confiáveis, podem ser utilizados como vitrine para crimes de estelionato, isto se dá, pois são locais virtuais onde os vendedores expõem seus produtos sem uma completa fiscalização, ou seja, há uma certa flexibilidade para a utilização das plataformas. Isto posto, os anúncios de seus vendedores, não fiscalizados podem ser utilizados para a consumação do crime de estelionato, de modo que utilizando da boa reputação do site e a boa-fé da vítima por acreditar que todos os anúncios são confiáveis, são usados com a finalidade ilícita pretendida.

Como é o caso do seguinte anúncio:



Fonte: Shopee, 2022.

Como é possível visualizar neste anúncio, há uma notória tentativa de manipular o interessado com um smartphone de uma marca conhecida e com um valor reduzido, porém, ao analisar profundamente é possível perceber que ao invés da escrita correta “Galaxy” está posto “Galay”, de forma a corromper a percepção do cliente. Este modelo de modificação pode não somente atentar contra os indivíduos desatentos, como contra aqueles que não possuem

conhecimento elevado sobre o produto, fazendo com que estes realizem a compra por pensar que o anúncio se trata de outro aparelho. Este tipo de anúncio, não fiscalizado pelos sites, traz prejuízos aos clientes, que por vezes levam em conta a popularidade da plataforma. De acordo com o levantamento feito pela empresa global de informações e soluções, Transunion, afirmou que comparado ao último semestre de 2021, no segundo semestre deste ano houve um aumento de 20% nas tentativas na de fraudes digitais, sendo suas principais por meio de lojas virtuais (TRANSUNION, 2022).

Um marco temporal que colaborou muito para o aumento desse crime virtual foi a pandemia da COVID-19[4], que devido ao isolamento social decretado pelo governo para diminuir a proliferação do vírus, muitas pessoas foram levadas a aprender a como utilizar a internet para tratar assuntos da sua vida cotidiana, já que não havia como sair de suas casas. Por isso, passou-se a usar da ferramenta digital, como para fazer transferências bancárias, pagar boletos, contas, e até mesmo realizar suas atividades laborais via *Home office* (ANTUNES, 2020)

Esse maior contato da população com os meios virtuais durante a pandemia não apenas trouxe benefícios, como também trouxe problemas para boa parte da sociedade, principalmente para os idosos. Os idosos foram os principais alvos dos estelionatários durante a pandemia, pois por conta da idade e pela dificuldade em que a maioria tem, o manejo e o conhecimento que necessitam para se proteger dentro dos meios virtuais se torna mais difícil para os mesmos. O principal meio para aplicar os golpes contra idosos é a falsificação de boletos que são enviados por e-mail para estas pessoas, que ao verem o boleto creem se tratar de pendências de bancos ou de lojas a qual fazem suas compras. Um levantamento feito pela Federação Brasileira de Bancos revelou que houve um aumento de 60% na tentativa de golpes financeiros contra idosos, isto é um reflexo do quanto a vulnerabilidade nos meios virtuais é de extrema essencialidade para os criminosos que praticam esses crimes, tendo seus alvos com maior vulnerabilidade, mais chance se tem para a consumação do delito. (FEBRABAN, 2020).

Posto isso, com base no avanço tecnológico e na adaptação dos estelionatários na aplicação do crime dentro dos meios virtuais, compreende-se que os princípios constitucionais

[4] A classificação que é atribuída pela OMS (Organização Mundial da Saúde) ao termo pandemia, nada mais é que a situação em que uma grave doença infecciosa tem grande potencial em contaminar simultaneamente pessoas do mundo todo, não estando ligado com a gravidade da doença, mas com sua contaminação em escala geográfica. A pandemia do Covid-19, causada pelo vírus SARS-CoV-2, que teve seu surgimento ao final do ano de 2019 na cidade de Wuhan (China) e teve sua proliferação para os demais cantos do mundo, acarretou mudanças de comportamento em grande parte da população mundial, ocasionando a necessidade de ações para contenção da mobilidade social, como isolamento e quarentena, prejudicando o acesso a bens essenciais como educação, alimentação, medicamentos, transporte, entre outros.

não conseguem dar a devida proteção contra os riscos citados de antemão. Haja vista que com o passar dos anos o número de casos e as maneiras de estelionato vem aumentando e em conjunto a vulnerabilidade de seus usuários aumenta proporcionalmente. Sendo necessário a compreensão de maneira mais aprofundada sobre o crime de Estelionato e como ele se encontra dentro dos meios virtuais.

3 O ESTELIONATO NA ERA DIGITAL

Neste capítulo examinar-se-á o crime de estelionato de modo que se tenha uma melhor compreensão do delito e como ele é visto tanto pela doutrina quanto pela legislação pátria. Primeiramente, é necessário adentrar no crime de estelionato em como se dá seus artifícios e atributos que o conceituam como o crime propriamente dito, para que deste modo se adentre no crime de estelionato virtual cujo qual adequa o crime de estelionato para os meios virtuais.

3.1 O Crime de estelionato

Primeiramente é de suma importância a compreensão do crime de estelionato em si para poder adentrar em sua modalidade virtual. Antes do crime de estelionato estar vigente no Código Penal, o judiciário brasileiro utilizava das ordenações Filipinas, que atribuía o crime de estelionato como uma burla. Foi no ano de 1830, em que foi reconhecido pelo nosso ordenamento como um crime em que se valem de artifícios fraudulentos para obter-se vantagem patrimonial de outrem (BITENCOURT, 2008).

Nos dias de hoje, o Código Penal Brasileiro conceitua o crime de estelionato pelo art. 171 do CP, que por sua vez discorre: "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". Diante do conceito atribuído pelo Código Penal Brasileiro, os conceitos doutrinários no que tange ao crime de estelionato se tornam mais compreensivos.

O crime de estelionato trata-se de um crime patrimonial significativo, em que o estelionato por ser um crime extremamente complexo, pois além de vários componentes os quais devem coexistir em uma sequência causal para que o crime seja consumado, é, ainda, necessário, distinguir o estelionato, delito, de um mero ilícito civil, o que é muitas vezes uma tarefa difícil. Como resultado, há muita controvérsia sobre a interpretação do crime de

estelionato. (FILHO 2018 p.1). A denominação dada ao termo estelionato advém do latim *stellio natus*, que provém da palavra engano (MIRABETE, 2005).

Seguindo o art. 171 do CP, entende-se que o estelionato constitui um tipo penal que exige uma série de elementos conhecidos como cadeia causal, ou seja, uma sequência ordenada de atos cometidos de forma sucessiva: a) fraude; b) erro; c) vantagem indevida; e d) prejuízo alheio. Podemos destacar o seguinte trecho do código "artifício, ardil ou outro meio fraudulento" O primeiro elemento, a fraude, vem descrevendo como "artifício, ardil, ou qualquer outro meio fraudulento". A primeiro ver, a diferença entre artifício e ardil não tem muita relevância, já que ambos são compreendidos pelo sentido mais abrangente de fraude. (FILHO, 2018, p.2)

De qualquer maneira, podemos afirmar que o artifício é a fraude material, na qual há uma alteração exterior da coisa: falsidade, disfarce, uso de aparelhos eletrônicos etc. Ardil já é a astúcia, a malícia, engenhosidade, ou seja, uma fraude puramente intelectual, sem a base material do artifício. (FILHO, 2018, p.2)

O próximo trecho a ser analisado é o "induzindo ou mantendo alguém em erro", o segundo fator constitutivo do estelionato é o erro, no qual "alguém" deve ter sido induzido ou mantido. O erro nada mais é que a falsa percepção da realidade, com o que o enganado não possui a perfeita noção do que está acontecendo. No trecho "vantagem ilícita, em prejuízo alheio" Se no furto uma vítima tem uma coisa subtraída, sem perceber ou sem que possa impedir a subtração. (GRECO, 2019)

Ainda segundo Greco (2019), no estelionato, há uma clara diferença entre o que está acontecendo e o que a vítima supõe que está acontecendo, razão pela qual a vítima realiza o ato de disposição patrimonial, que é o principal fator do crime de estelionato. Deve haver para a consumação do ato ilícito estelionato a soma dos fatores descritos de forma sucessiva já que a mera soma dos fatos não é o suficiente, portanto se faz necessária uma relação de causalidade entre os fatos.

Vislumbrando a os meios utilizados e o objeto pretendido atingir no crime, compreende-se que este delito contém em sua essência fatores que são utilizados e almejados dentro dos meios virtuais por aqueles que os utilizam de forma ilícita, tais como a falsa percepção, o induzimento ao erro, a fraude e por fim o prejuízo alheio, em que como visto de antemão, estes requisitos do crime de estelionato podem ser feitos através de sites, falsos e-mails, o anonimato entre outras inúmeras ferramentas que podem ser utilizadas dentro da internet para a consumação desse delito. Sendo assim, conforme o apresentado pelos conceitos vistos de antemão, ainda que os crimes virtuais se encaixam tanto nos requisitos previsto na legalidade

quanto na doutrina, faz-se necessário ter um olhar especial para o crime de estelionato nos meios virtuais, pois com o avanço da tecnologia o crime de estelionato virtual vem sendo cada vez mais presente dentro da sociedade, sendo necessário compreender as diferenças que o distingue do crime de estelionato propriamente dito para o crime estelionato virtual, que por sua vez será abordado na seção subsequente.

3.2 O crime de estelionato no ambiente virtual

Após o apresentado de antemão sobre o crime de estelionato, a presente seção visa pautar o crime de estelionato cometido nos meios virtuais e como este crime vem se modernizando proporcionalmente com o avanço da tecnologia. Abrangendo também suas modalidades e os meios que se tem a consumação desse delito que se diferenciam do crime de estelionato propriamente dito.

Primeiramente devemos conceituar o que é crime virtual, segundo Rossini (2004), o conceito de delito informático poderia ser descrito como aquela conduta típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, praticada por pessoa física ou jurídica, com o uso da informática, em ambiente de rede ou fora dele, e que ofenda, direta ou indiretamente, a segurança informática, que tem por elementos a integridade, a disponibilidade a confidencialidade.

Outrossim, um ponto importante para a compreensão do crime virtual será identificar o sujeito passivo e o sujeito ativo do crime em questão. Quando se abrange o sujeito Ativo dentro do crime de estelionato no ambiente virtual, cabe tratar de como se configura o indivíduo deste crime. Tendo em vista que o crime de estelionato virtual possui peculiaridades quanto o crime de estelionato em si, uma destas diferenças será quanto às técnicas que o estelionatário virtual possui, o doutrinador Paulo Marco Ferreira Lima atribui as características do sujeito ativo no crime de estelionato com a seguinte conceituação:

> Em princípio, é criminoso de informática alguém que conhece a vulnerabilidade dos sistemas, dos programas de computadores e de tudo que circula em tal ambiente. Deve possuir habilidade de planejar o crime sob esse terreno, percebendo as oportunidades que facilitam sua prática delitiva e seu anonimato após a descoberta de sua conduta. Os indivíduos que cometem os chamados “crimes de computador” possuem certas características peculiares, isto é, os sujeitos ativos têm habilidades para o manejo dos sistemas informáticos e, no mais das vezes, encontram-se em seu ambiente de trabalho em posições estratégicas, que lhes permitem acesso à informação de caráter sensível. Com o tempo se pôde comprovar que os autores dos delitos informáticos são muito diversos e que o que os diferencia entre si é a natureza dos delitos cometidos (LIMA, 2011, p.40)

Já no que tange ao sujeito passivo do crime de estelionato virtual, será aquele que se encontra em situação de vulnerabilidade técnica perante os avanços da tecnologia. Vale lembrar

que esta vulnerabilidade técnica não significa dizer que o indivíduo possui zero conhecimento sobre a utilização dos meios virtuais, mas sim que este possui sua vulnerabilidade com base na sua falta de experiência técnica diante do conhecimento que os estelionatários possuem para a aplicação do ato ilícito dentro da internet, fazendo com que estas vítimas tenham dificuldade em se proteger dos possíveis golpes que podem vir a sofrer. Posto isso, compreende-se que o sujeito passivo deste crime poderá ser qualquer pessoa que utilizando da internet está sem saber correndo o risco de ser vítima da falsa percepção que lhe é auferida (LIMA, 2008).

Após a compreensão de como se classifica os sujeitos ativos e passivos deste crime, fica mais fácil adentrar na questão dos cybers criminosos (criminosos cibernéticos). Estes por sua vez se aproveitaram muito bem do contexto pandêmico para praticar fraudes contra a população que possuem menos informação sobre segurança na internet, elaborando novas estratégias, técnicas e métodos para a realização de crimes. O crescimento do comércio eletrônico, as oportunidades de bons negócios, os descontos avassaladores, são a isca perfeita para a obtenção de vantagens indevidas. (DE OLIVEIRA, 2020)

Apesar do crime de estelionato virtual ter por objeto o patrimônio material da vítima, tal crime pode ser aplicado pelos cybers criminosos de maneiras diferentes, sendo cada uma possuindo peculiaridades que as diferenciam completamente uma da outra. Exemplos de tais modalidades são o golpes do empréstimo fácil, golpes em sites de vendas, Páginas de internet falsas e as pirâmides financeiras, que por sua vez são muito utilizadas para a consumação do delito.

Portanto, diante do crescimento elevado nos últimos anos, mas principalmente durante o contexto pandêmico, se chega à conclusão de que o crime de estelionato virtual vem tendo grande impacto na sociedade e na tecnologia, em que por sua vez por ter inúmeros meios da aplicação do delito, não pode este ser tratado pela legalidade e pelo legislador de forma equivalente ao crime de estelionato propriamente dito. Pois, diante do aumento deste delito nos meios virtuais, é necessário entender como tal crime pode ser aplicado e quais modalidades existentes que são aplicadas pelos criminosos e como estas modalidades apesar de conceituar como crime de estelionato virtual, tais modalidades possuem suas peculiaridades que as diferenciam completamente uma das outras, fazendo-se necessário adentrar-las de forma mais específica em cada uma delas.

3.2.1 Modalidades de estelionato virtual

Nessa seção analisar-se-á, as modalidades do delito de estelionato no ambiente virtual, no qual o foco será examinar as formas mais frequentes de cometimento do delito dentro do ambiente virtual.

3.2.1.1 O golpe do empréstimo fácil

O golpe do empréstimo fácil envolve o envio de mensagens de texto, e-mails e até ligações telefônicas em que os estelionatários já tem ciência que suas vítimas estão em situação financeira precária, aproveitando-se da oportunidade para oferecer empréstimos com taxas de juros bem abaixo do habitual. Depois que o criminoso consegue atrair a vítima com sua proposta, ele condiciona o empréstimo do valor solicitado pela vítima a um depósito bancário de valor menor como caução. Muitas vezes, a vítima acaba depositando o dinheiro na conta do ladrão, de modo que o dinheiro depositado como caução nunca pode ser recuperado, e obviamente ele nunca recebe o valor do empréstimo.

3.2.1.2 Golpes em sites de vendas

É o caso dos anúncios de venda de itens na internet, como OLX e Mercado Livre. Nesse caso, a vítima é alguém que anuncia seu produto em um determinado site de vendas e obtém rapidamente a resposta de um criminoso que, neste caso, se disfarça de suposto comprador. O criminoso envia várias mensagens manifestando interesse no produto, mas alega que não estava no estado da vítima, solicitando que o produto lhe fosse enviado pelos correios. (AMORAS, 2020)

Uma vez que a vítima negocia o valor com o suposto comprador, o indivíduo normalmente paga o suposto valor na forma de depósito e envia à vítima uma foto do recibo. As vítimas bem-intencionadas acreditam no pagamento e acabam enviando o produto anunciado imediatamente, todavia o valor depositado nunca chega à conta da vítima, pois os criminosos costumam depositar envelopes vazios em caixas eletrônicos ou até mesmo falsificar comprovantes de depósito.

Outra variante desta modalidade acontece quando o agente cria um anúncio de um produto em um site de vendar a um preço abaixo do mercado, e a vítima atraída pelo preço acaba depositando o dinheiro na conta do golpista, que por sua vez ou não enviar o produto ou envia um produto que não condiz com a oferta original e desaparece da rede sem deixar rastros

aparentes, já que na maioria das vezes os criminosos utilizam informações falsas na hora de se registrarem nos sites de vendas.

3.2.1.3 *Phishing* – Páginas de internet falsas

A palavra *phishing* tem origem inglesa e é derivada da palavra *fishing*. Em outras palavras, trata-se de sites criminosos e fraudulentos que visam imitar a aparência de um site legítimo e original com a finalidade de pescar dados. Neste caso, criminosos enviam links de sites para as vítimas, e elas acabam acessando o site acreditando ser o original e informando dados pessoais indevidamente. (AMORAS, 2020)

Dentre as páginas fraudulentas, as principais são as que imitam as páginas de bancos, enviando para as vítimas através de e-mail, SMS ou outros meios, os links destas páginas. Depois que as vítimas acessam as páginas e informam seus dados achando se tratar da página oficial, os agentes salvam as informações sigilosas e as utilizam para praticar atos criminosos com os dados da vítima ou, ainda, subtrair os valores das contas.

3.2.1.4 As Pirâmides Financeiras

A pirâmide financeira[5] é caracterizada pela criação de uma suposta instituição financeira, por um ou mais criminosos, que buscam indivíduos de boa-fé para investir e adentrar a falsa sociedade. Uma pirâmide financeira geralmente busca vítimas para integrar e investir a organização sob a promessa de alta rentabilidade por mês, prometendo, por vezes, que o valor investido seja duplicado ou até triplicado em um curto período. (AMORAS, 2020)

Assim a vítima tentada pelo alto valor lucrativo e a velocidade do retorno prometida pela falsa instituição investe seu dinheiro e ao adentrar e investir seu dinheiro na falsa instituição financeira tem o seu lucro condicionado ao ingresso de outros indivíduos. Desta forma, a vítima somente recebe o suposto lucro investido se convidar duas ou mais pessoas para integrar e investir na instituição.

[5] Apesar de também pretender atingir o patrimônio material de terceiro, o crime contra o Sistema Financeiro Nacional será o crime cometido contra Instituições Financeiras de modo que vise atingir o patrimônio daquela instituição. Contudo, sua peculiaridade tem no eventual dano que possa atingir a higidez e a credibilidade do sistema financeiro nacional. Sendo assim, os crimes cometidos contra o sistema financeiro têm por seu bem jurídico tutelado não somente o patrimônio e a riqueza do investidor, mas sim a ordem jurídica financeira e a segurança econômica (BALTAZAR JR., 2011).

Graças a promessa de alta rentabilidade e o condicionamento de ingresso de outras pessoas como investidores, haverá um crescimento exponencial de indivíduos investindo em uma instituição fraudulenta, logo aumentando a entrada de dinheiro na instituição fazendo com que os golpistas possam adquirir carros e itens de luxo para esbanjar nas redes sociais com o objetivo de atrair mais vítimas para a instituição.

4 O AUMENTO DO CRIME DE ESTELIONATO VIRTUAL NA CONTEMPORANEIDADE E A DIFICULDADE DE APLICAR SANÇÕES AOS ESTELIONATÁRIOS

A presente seção tem por objetivo esclarecer o aumento dos crimes de estelionato virtual vem crescendo de forma significativa nos últimos anos, correlacionando com uma maior presença dos usuários das redes. De modo que possa se compreender como este aumento dos usuários colabora para o aumento deste crime e como o direito penal vem lidando de forma prática com este delito virtual.

Para adentrar no aumento deste delito virtual, cabe ressaltar como a modernização tecnológica vem sendo de extrema necessidade para a vida da população e como esta necessidade vem contribuindo para o aumento dos usuários nos meios virtuais. Como dito nas seções anteriores, vale lembrar que a tecnologia vem adaptando os afazeres do cotidiano da sociedade, solucionando problemas que antes não poderiam ser feitos através da internet. Esta facilidade que a internet trouxe para a população, fez com que o aumento do número de usuários virtuais aumentassem ao passar dos anos, se fazendo muito presente nos anos de 2020. Em março de 2020 (Figura 2) acentuou-se o uso de tecnologias digitais no Brasil, passando de 71% dos domicílios com acesso à internet em 2019 para 83% no ano de 2020, o que equivale a 61,8 milhões de domicílios com algum tipo de conexão à rede.

Tabela 1- Domicílios com acesso à internet no Brasil

Proporção	Ano					
Sim	2015	2016	2017	2018	2019	2020
Total	50,9	53,9	60,8	66,7	71,4	83,2

Fonte: CETIC (2021).

Tabela 2 - Domicílios com acesso à internet no Brasil por região

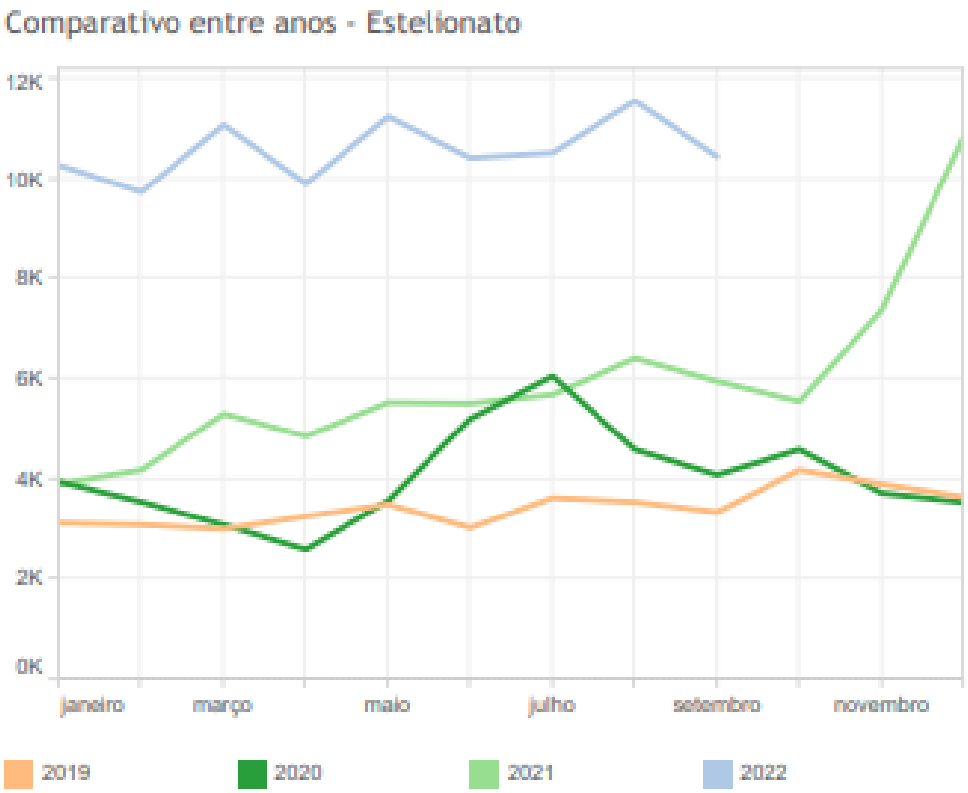
Proporção		Ano						
Sim		2015	2016	2017	2018	2019	2020	2021
REGIÃO	Sudeste	59,6	63,7	69,2	72,8	74,6	85,9	83,8
	Nordeste	39,9	40,3	48,9	56,9	65,3	79,3	77,3
	Sul	52,5	52,1	59,8	69	73,2	83,5	82,7
	Norte	37,6	46,4	48,1	63,2	71,8	81,4	79,4
	Centro-Oeste	48	56,2	67,5	64,1	70,1	81,1	82,7

Fonte: CGI.br/NIC.br

Com base nos dados apresentados de antemão pelos gráficos, a sociedade brasileira vem aumentando consideravelmente o seu contato com a tecnologia e os meios virtuais, tendo um aumento significativo do ano de 2019 para o de 2020, haja vista por conta da pandemia do COVID-19, medidas tomadas pelo governo brasileiro diante da pandemia, fizeram com que a falta de interação social e afazeres do dia a dia que só poderiam ser feitos de forma presencial, tiveram que ser adaptados para os meios virtuais, de modo que colaborou muito para o aumento citado visualizado de antemão.

Contudo, apesar da aproximação da sociedade com a tecnologia ter aderido a muitos benefícios, este maior contato com os meios virtuais trouxe um aumento significativo do crime de estelionato para a sociedade brasileira. Pode-se observar cada vez mais a adaptação das práticas criminosas no meio virtual neste período de pandemia. O isolamento social, de fato, fez acreditar que a residência seria um ambiente seguro, todavia a população está cada vez mais exposta ao mundo virtual e seus riscos.

Gráfico 1 - Casos de Estelionato no Rio de Janeiro



Fonte: ISP, 2022

Seguindo os dados apresentados, entende-se que o aumento de casos do crime de estelionato na internet dá-se pelo aumento desordenado de usuários novos na internet, a crise econômica, o isolamento social, o avanço tecnológico, a pouca informação e o grau de instrução da população no que tange à utilização dos dispositivos que utilizam a internet, tudo isso faz com que haja um forte crescimento de sujeitos passivos nos crimes eletrônicos (GOODMAN, 2015).

Ademais, vale lembrar que dentro dos meios virtuais, estes estelionatários possuem vantagem para a aplicação deste golpe, que é o anonimato que a internet proporciona para estes indivíduos, que por sua vez é uma ferramenta crucial para a aplicação do delito sem que sejam identificados, impulsionando o aumento na prática deste crime através do anonimato. (PINHEIRO, 2010).

Diante desse cenário, com objetivo de diminuir os crimes de estelionato nos meios virtuais, a lei n° 14.155, de 27 de maio de 2021 trouxe uma importante alteração a fim de adequá-lo à nova realidade. Dentre as alterações que foram trazidas pela lei, foram acrescentados os parágrafos 2°-A e 2°-B, que tratam da fraude eletrônica, com a seguinte redação:

> § 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).

Mesmo após a implementação do dispositivo supra-legal citado de antemão, o aumento do crime de estelionato virtual foi considerável no ano de 2022. A empresa Apura Cyber Intelligence S/A fez um relatório sobre o primeiro semestre de 2022 em que constatou-se um aumento de 637% nas fraudes financeiras, comparado ao ano de 2021. (Apura Cyber Intelligence, 2022).

Com isto, conclui-se nesta seção que o avanço da tecnologia foi significativo para a aproximação da sociedade com os novos meios virtuais e as facilidades que atribuem para o seu dia a dia, de modo que também contribuiu para o aumento do crime de estelionato virtual devido à vulnerabilidade técnica das vítimas perante os criminosos e o anonimato que os mesmos possuem para a prática do crime. Diante do avanço da tecnologia e do surgimento de diversas modalidades dos crimes de estelionato virtual, compreende-se que a legalidade que busca repreender este delito não é suficiente. Fazendo com que esta dificuldade na repressão do delito cause este aumento significativo do crime de estelionato nos meios virtuais, sendo necessário compreender o porquê do dispositivo legal está sendo insuficiente e como o Direito Penal pode se adaptar melhor ao surgimento das novas modalidades desse crime e como buscar aplicar as sanções para este crime de forma mais eficiente e específica, objetivando a diminuição na prática deste delito.

5 O DIREITO PENAL DIANTE AS NOVAS MODALIDADES DOS CRIMES VIRTUAIS

Com a criação dos computadores e a propagação da internet, tornaram-se cada vez mais comuns situações em que pessoas tentam prejudicar outras utilizando-se dessas novas ferramentas, vez que elas possibilitaram a criação de um espaço público virtual em que as pessoas têm uma sensação de anonimato e até mesmo impunibilidade. Surgiram então, pessoas especializadas em informática e tecnologia que praticam crimes por todo o mundo. São assim denominados os crimes virtuais ou cibernéticos.

No entanto, ainda não há uma legislação que trate sobre o conceito de crimes cibernéticos, também não há uma classificação, as análises e condenações são feitas a partir do Código Penal Brasileiro. Todavia, alguns autores classificam tais crimes como puros e impuros, sendo os puros as condutas não tipificadas e os impuros os tipos penais já tipificados e que ocorrem no ciberespaço.

A Lei Geral de Proteção de Dados (LGPD), Lei n. 13.709, foi publicada em, de 14 de agosto de 2018 e entrou em vigor na data de 18/09/2020, após dois anos de vacatio legis[6]. A princípio, sua vigência deveria ter acontecido muito antes, em fevereiro de 2020, entretanto, graças aos vários impasses e prorrogações quase ininteligíveis a nova lei só entrou em vigor em setembro de 2020. A falta da LGPD durante esse período gerou um vazio legislativo sobre o tratamento dos dados.

O texto da LGPD permite o compartilhamento de dados pessoais controlados pelos órgãos de segurança pública em casos excepcionais, quando houver interesse público e desde que sejam observadas normas de proteção desses dados previstas no projeto. Do ponto de vista penal, porém, a lei nada designou, pelo contrário. Deliberadamente (artigo 4º LGPD), impediu expressamente o tratamento de dados pessoais nos casos de: segurança pública, defesa nacional, segurança do Estado e/ou atividades de investigação e repressão de infrações penais.

Sendo assim, em novembro de 2020, um ano após a criação de uma comissão focada em preencher essa lacuna deixada pela LGPD, apresentou um projeto de lei ao presidente da Câmara dos deputados. O anteprojeto tem doze capítulos e sessenta e oito artigos, que se dividem em oito eixos temáticos: 1. âmbito de aplicação da Lei; 2. condições de aplicação; 3. base principiológica; 4. direitos e obrigações; 5. segurança da informação; 6. tecnologias de monitoramento; 7. transferência internacional de dados; e 8. a autoridade de supervisão. Podemos observar uma grande lacuna legislativa deixada pela LGPD o que gera uma grande insegurança jurídica para a população.

O surgimento do chamado mundo virtual ou ciberespaço, que representa novas concepções de tempo e principalmente de espaço, tornou-se um obstáculo à aplicação do direito penal, pois o conceito clássico de território presente no artigo 5° do código penal adquire uma conotação diferente, um espaço virtual, ou seja, um ambiente global em que os limites territoriais (da vida real) são ultrapassados. Portanto, o ciberespaço não é propriamente um território, mas caracteriza-se por um fluxo constante de informação através de redes de comunicação, pelo qual a localização da informação torna-se relevante porque dá a ideia de um

[6]Prazo definido para a sociedade se adequar à nova legislação.

território do espaço físico, resultando em várias questões que precisam ser tratados pelo direito penal e pelo processo penal estamos, então, diante do debate entre lugar e “não-lugar” (MARCONDES FILHO: 1996: 146-7).

Além disso, deve-se ter em mente que os crimes cometidos em ambiente virtual são de natureza transnacional, pois atingem vários países ao mesmo tempo, o que, aliado ao caráter global do ciberespaço, exige uma nova análise da atuação do direito penal no espaço. É preciso lembrar que, em um mundo cada vez mais globalizado, o direito penal precisa acompanhar os constantes desenvolvimentos tecnológicos para garantir a correta aplicação do direito e, com isso, alcançar o ideal de justiça e a promoção da paz social.

Com isso observa-se os novos desafios enfrentados pelo direito penal na contemporaneidade já que as infrações perpetradas no âmbito informático, de um modo geral, não deixam rastros que, em função das incertezas que a Rede Mundial de Computadores ainda perpetua, muitos casos carecem da identificação do autor do fato.

Um desses desafios é o da responsabilização penal que só pode ser apurada quando há um conjunto de provas fortes que estabeleçam a autoria e conduta ilícita . Para isso, os instrumentos probatórios demonstram os atalhos que os magistrados devem seguir para tomar decisões com base em fatos contestados. Nas palavras de Paulo Rangel, “meios de prova são todos aqueles que o juiz, direta ou indiretamente, utiliza para conhecer a verdade dos fatos, estejam eles previstos em Lei ou não”. (RANGEL, 2014, p. 463)

É mais provável que as provas em ambiente informático desapareçam porque só são preservadas se houver alguma relevância para o fornecedor de acesso ou uma autoridade judicial determinar que é relevante. Nesse contexto, vale destacar que o armazenamento de dados pelos provedores de acesso é fundamental para o enquadramento probatório dos crimes virtuais. As informações armazenadas pelo provedor podem identificar o IP e, assim, a localização do criminoso. Portanto, a evidência física acima mencionada é vista como um grande passo para encontrar o autor do crime informático.

Ademais, existem situações que nossa lei não prevê, como os vírus, como eles apareceram na Internet e ainda não possuem nenhuma lei específica que as prevê como práticas criminosas , portanto, são atípicas. Estas são formas amplamente utilizadas para praticar o "phishing", conforme mencionado anteriormente. Além disso, embora o Código possa tentar antecipar quase todas as situações, a internet é um ambiente muito complexo, logo, de nada adianta ter normas proibitivas se não for possível encontrar os agentes desses crimes.

Por exemplo, dessa dificuldade de encontrar os agentes podemos observar que o processo de investigação de crimes cibernéticos começa com a identificação sobre a origem da

comunicação, também identificando seu Internet Protocol denominado IP. Todos os dispositivos eletrônicos que podem se conectar à Internet têm sua forma de identificação.

Por meio do IP, é possível rastrear o autor do crime até uma localidade, bem como a comprovação da gravidade do crime, já que dele decorre todo o trânsito gerado pelo usuário, seu histórico de navegação. Mas identificar o IP nem sempre é uma tarefa fácil, já que existem várias formas de disfarçar o seu IP e até quem não tem muita experiência sobre internet pode fazer isso através do uso de várias ferramentas, uma delas por exemplo o chamado VPN ou "Virtual Private Network" ou rede virtual privada que permite a duas redes se conectarem de forma segura utilizando um canal público de comunicação, essa tecnologia cria túneis que transmitem os dados criptografados entre as redes, tornando a identificação mais difícil, e quando se trata de criminosos com grande conhecimento, a tarefa é ainda mais difícil.

Nesse sentido, é absolutamente necessário formar profissionais com conhecimento específico deste meio, como muitos criminosos os chamavam os Hackers e Crackers são especialistas neste campo e é preciso dar igual conhecimento para ser verdadeiramente eficaz. Além disso, não só o conhecimento, mas também a tecnologia, como ela está evoluindo a cada dia, ficando mais rápido e complicado , portanto, é preciso investir nessas tecnologias para estar à frente, ou pelo menos no mesmo nível dos cibercriminosos.

CONSIDERAÇÕES FINAIS

O presente artigo teve como objetivo principal analisar o aumento dos crimes e quais riscos penais estão presentes na prática do crime de estelionato virtual, bem como, vislumbrar a conceituação do crime de estelionato virtual e quais suas modalidades que são utilizadas pelos criminosos na prática deste delito. Com o intuito de responder o seguinte problema de pesquisa: De que modo e quais as dificuldades que o Direito Penal encontra no combate ao crime de estelionato cometido em ambiente virtual?

Para alcançar o problema de pesquisa ora proposto, utilizou-se pesquisa bibliográfica elaborada a partir de livros, revistas, dissertações, teses e publicações em periódicos e artigos científicos e documental por meio da utilização de relatórios de pesquisa e documentos oficiais.

Ademais, a fim de alcançar ao objetivo ora proposto, na primeira seção analisou-se as novas tecnologias e os novos riscos penais onde se buscou analisar as novas formas que os criminosos desenvolveram e que novos riscos para população essas novas modalidades trouxeram, onde foi possível identificar que a internet abriu um leque de possibilidades positivas e negativas, criando novas formas de comunicação, novas formas de pagamentos e até

mesmo novas formas de realizar compras. Todavia a internet também ampliou as formas que os criminosos podem tirar proveito das pessoas.

Uma vez entendido os novos e riscos, tecnologias e as novas práticas do crime de estelionato criadas pelo mundo moderno, passou-se ao principal momento do trabalho, onde demonstrou-se o aumento do crime de estelionato virtual, as dificuldades de aplicação das sanções e por último e mais importante, como o direito penal vem enfrentando as novas modalidades dos crimes virtuais.

Discorreu-se de forma mais aprofundada como o direito vem enfrentando estes novos desafios, fazendo seu exame a partir da LGPD e da Lei 14.155/2021, e encerrando com os avanços e desafios enfrentados no combate a essas novas inseguranças geradas pela internet . Bem como, apontando eventuais falhas e lacunas presentes que possam servir de empecilho.

Verificou-se que diante de inúmeras situações que envolvem vários tipos de crimes, a partir da internet que se originou o denominado direito digital, e com isso um novo espaço de evolução na ciência jurídica para o combate desses tipos de crimes, que cada vez mais cresce no Brasil.

Com essa finalidade, que várias medidas no âmbito do direito tiveram que ser tomadas tentando diminuir os números de casos e uma forma de proteção para que a justiça se faça presente dentro do ambiente jurídico, onde todo cidadão tem o direito de proteção jurídica, porém, um dos grandes entraves que acarretam a impunidade, é a dificuldade na identificação dos criminosos e a obtenção de provas. Mesmo assim, se busca cada vez mais criar medidas que possam proteger vítimas desse tipo de crime, como por exemplo as alterações feitas na lei 14.155/2021.

Logo, conclui-se que um novo pensar sobre o Direito Penal é necessário, tendo em vista as enormes transformações trazidas pela globalização e que implicam, também, no incremento da criminalidade de caráter transnacional, especialmente, tendo em vista que a consumação de um crime praticado pela Internet se dá em todos os lugares em que a rede é acessível.

Portanto, ao final do artigo, foi possível responder ao problema de pesquisa ora proposto após verificar de que modo o Direito Penal combate o estelionato virtual e suas principais dificuldades nesse combate no ambiente virtual.

REFERÊNCIAS

ACADEMIA BRASILEIRA DE DIREITO DO ESTADO – ABDET. **Comentários ao Marco Civil da Internet.** Disponível em: <https://www.conjur.com.br/2019-mar-14/veja-stjjulgado-crimes-sexuais-internet. Acesso at: 7 Mai 2021>.
Acesso em: 5 de out. de 2021.

AMORAS, E. A. P. **AS FORMAS DE FRAUDES ECONÔMICAS NA ERA DIGITAL**. In: Caderno de pós-graduação em direito: crimes digitais. [s.l.] UniCEUB; ICPD, 2020. p. 88-94.

ANTUNES, Ricardo. **Coronavírus: o trabalho sob fogo cruzado**. São Paulo: Boitempo, 2020.

APURA CYBER INTELLIGENCE S/A. **Relatório de cibersegurança 1º semestre de 2022,** Disponível em:<https://conteudo.apura.com.br/relatorio-primeiro-semestre-2022>
Acesso em: 24 de out. 2022

ALMEIDA, Thábata Clezar de. **O estelionato digital no e-commerce: a fraude da loja virtual fantasma**. Orientador: Prof. Esp. Diego Archer de Haro. 2013. 119 f. Trabalho de Conclusão de Curso (Curso de Graduação em Direito) - Universidade do Sul de Santa Catarina, Araranguá, 13/05/2013. Disponível em:
<https://repositorio.animaeducacao.com.br/handle/ANIMA/7644>
Acesso em: 15 mar. 2022.

BALTAZAR JR., José Paulo. **Crimes federais**. Porto Alegre: Livraria do Advogado Editora, 2011.

BITTENCOURT, Rodolfo Pacheco Paula. **O anonimato, a liberdade, a publicidade e o direito eletrônico**. 2016, Disponível em:
<https://rodolfoppb.jusbrasil.com.br/artigos/371604693/o-anonimato-a-liberdade-a-publicidade-e-o-direito-eletronico>
Acesso em: 20 de Maio 2017.

BITENCOURT, Cezar Roberto. **Tratado de direito penal**. 3 ed. São Paulo, 2008.

BITENCOURT, Cezar Roberto. **Tratado de direito penal**. São Paulo: Saraiva, 2018. Volume II.

BORGES, F. ALVES FAGUNDES, B.; NUNES DA CUNHA, G. **VPN: Protocolos e Segurança**. [s.l: s.n.]. Disponível em:
<https://www.lncc.br/~borges/doc/VPN%20Protocolos%20e%20Seguranca.pdf.>

BRASIL. **Código penal e Constituição Federal (1988)**. 45. ed. São Paulo: Saraiva, 2007.

CETIC.BR. **TIC Domicílios**. Disponível em: <http://data.cetic.br/cetic/explore?Id>
Pesquisa=TIC_DOM . Acesso em: 18 mar. 2022.

CINTRA, ERICKSON BRENER DE CARVALHO. **A Informatização do Processo Judicial e seus Reflexos no Poder Judiciário, no Superior Tribunal de Justiça e na Sociedade Brasileira**.Monografia de conclusão de especialização em Gestão Judiciária. 138 f. Universidade de Brasília- UNB, Brasília, 2009.

DE OLIVEIRA, H. C. **CYBERCRIMES: DO ESTELIONATO VIRTUAL**. Monografia Apresentada Como Requisito Parcial À Conclusão Do Curso De Direito—Faculdade Evangélica de Rubiataba: [s.n.].

DE TEFFÉ, C. S.; DE MORAES, M. C. B. **Redes Sociais virtuais: Privacidade E Responsabilidade civil. Análise a Partir Do Marco Civil Da Internet**. Pensar - Revista De Ciências Jurídicas, v. 22, n. 01, p. 108–146, 2017.

FEBRABAN. **Golpes financeiros contra idosos cresceu em 60% desde o início da pandemia.** Disponível em: <https://portal.febraban.org.br/noticia/3522/pt-br/ https://www.gov.br/casacivil/pt-br/assuntos/noticias/2022/setembro/violencia-patrimonial-e-financeira-pessoas-idosas-sao-as-maiores-vitimas-no-brasil#:~:text=A%20Federa> Acesso em: 08 de set. 2022

HUNGRIA, Nélson; FRAGOSO, Heleno. **Comentários ao Código Penal**. 5 ed. Rio de Janeiro: Forense, 1982. v. 6.

LIMA, Paulo Marco Ferreira. **Crimes de Computador e Segurança Computacional.** 2. ed. São Paulo: Atlas, 2011.

GOODMAN, MARC. **Future Crimes: tudo está conectado, todos somos vulneráveis e o que podemos fazer sobre isso**; tradução de Gerson Yamagami-São Paulo: HSM editora, 2015.

FILHO TOURINHO, Fernando da Costa. **Manual de Processo Penal**. São Paulo: Saraiva, 2009, p.522.

GRECO, Rogério. **Curso de Direito Penal: Parte Especial. 16**. ed. Niterói, RJ: Impetus, p. v. 2. 2019.

LEMOS, Ronaldo. **O marco civil como símbolo do desejo por inovação no Brasil**. In:LEITE G. S. ; LEMOS, R. (Coord). Marco Civil da Internet. São Paulo: Atlas, 2014. p. 3-11.

MARCONDES FILHO, Ciro (coord) (1996): **Pensar – pulsar: Cultura Comunicacional, tecnologias e velocidade**. São Paulo: Edições NTC.

MARCONI, M. A.; LAKATOS, E. M. **Fundamentos de metodologia científica**. 8. ed. São Paulo: Atlas, 2017.

MARRA, F. B. **Desafios Do Direito Na Era Da Internet: Uma Breve Análise Sobre Os Crimes Cibernéticos**. campo jurídico, v. 7, n. 2, p. 145–167, 12 dez. 2019.

MIRABETE, Julio Fabbrini. **Manual de direito penal**. 23. ed. São Paulo: Atlas, 2005. p. 303.

NUNES, Mário Vinicius de Azevedo; MADRID, Fernanda de Matos Lima. **CRIMES VIRTUAIS: O DESAFIO DO CÓDIGO PENAL NA ATUALIDADE E A IMPUNIDADE DOS AGENTES. ETIC - ENCONTRO DE INICIAÇÃO CIENTÍFICA** - ISSN 21-76- 21 8498, [S. l.], ano 2019, p. 1-15, 19 mar. 2019. Disponível em: <http://intertemas.toledoprudente.edu.br/index.php/ETIC/article/view/7895> Acesso em: 15 mar. 2022.

PINHEIRO, Patrícia Peck. Direito digital. 4ª ed. São Paulo: Saraiva, 2010.

RANGEL, PAULO. **Direito Processual Penal**. São Paulo, Atlas, 2014, Ed. 22ª, p. 463.

Série Histórica - ISP Visualização. Disponível em: <http://www.ispvisualizacao.rj.gov.br/>. Acesso em: 28 nov. 2022.

SHOPEE. **Galay s21 + ultra 7.2 Polegada smartphone 5800mah desbloquear versão global 4g 5g android 10.0 16mp + 32mp 12gb + 512gb celulares**.Disponível em: https://shopee.com.br/Galay-s21-ultra-7.2-Polegada-smartphone-5800mah-desbloquear-vers%C3%A3o-global-4g-5g-android-10.0-16mp-32mp-12gb-512gb-celulares-smartphone-i.423156927.9644288668. Acesso em: 18 nov.2022.

TRANSUNION. **Tentativas de fraude digital no Brasil aumentam 20% no segundo trimestre de 2022,** Disponível em: <https://newsroom.transunion.com.br/tentativas-de-fraude-digital-no-brasil-aumentam-20-no-segundo-trimestre-de-2022/> Acesso em: 14 de set. 2022.