LETÍCIA RAFAELA GONÇALVES REZENDE.

ESTELIONATO VIRTUAL: Violação ao Direito de Propriedade.

CURSO DE DIREITO – UniEVANGÉLICA
2023

LETÍCIA RAFAELA GONÇALVES REZENDE.

ESTELIONATO VIRTUAL: Violação ao Direito de Propriedade.

Monografia apresentada ao Núcleo de Trabalho de Conclusão de Curso da Universidade Evangélica de Goiás, como exigência parcial para a obtenção do grau de bacharel em direito, sob a orientação do professor Me. Rivaldo Jesus Rodrigues

CURSO DE DIREITO - UniEVANGÉLICA
ANÁPOLIS – 2023

LETÍCIA RAFAELA GONÇALVES REZENDE.

ESTELIONATO VIRTUAL: Violação ao Direito de Propriedade.

Anápolis, ___ de _____ de 2023.

BANCA EXAMINADORA

_____

_____

AGRADECIMENTOS

A Deus e minha intercessora a Nossa Senhora Aparecida, que permitiram ultrapassar todos os obstáculos encontrados ao longo do curso e da realização deste trabalho. A minha família e ao meu namorado por não me deixarem desistir sempre me incentivando durante a realização deste trabalho. Ao meu orientador, que conduziu o trabalho com paciência e dedicação, sempre disponível a compartilhar todo o seu vasto conhecimento. À instituição de ensino Unievangélica, essencial no meu processo de formação profissional, pela dedicação, e por tudo o que aprendi ao longo dos anos do curso.

RESUMO

O presente trabalho analisa o crime de estelionato praticado na esfera virtual em decorrência do advento da tecnologia. Apresenta os crimes cibernéticos, de maneira principal, o estelionato. O primeiro capítulo apresenta a criação da Lei que alterou o artigo 171 do Código Penal Brasileiro, que trata do estelionato virtual. O segundo capítulo traz um breve histórico do surgimento da Internet, bem como da utilização da Internet pela sociedade, explicando o modo como os infratores utilizam o ambiente virtual para cometer crimes. E por fim, o terceiro capítulo, apresenta um breve comentário sobre os tipos de crimes virtuais e as leis que foram criadas para combatê-los. Bem como, ressalta a necessidade uma definição legal e mais específica para o crime de estelionato virtual, visando a busca da proteção da sociedade contra o prejuízo patrimonial, com uma punição mais eficaz e inibidora da prática deste crime.

Palavras-chave: Estelionato. Internet. Crime Virtual. Tipificação

SUMÁRIO

INTRODUÇÃO

O presente trabalho monográfico analisa o crime de estelionato virtual, aferindo artigos, legislações vigentes e o estudo de grandes doutrinadores com especializações afincas sobre o tema. Atualmente a internet está presente e se faz indispensável no cotidiano de grande parte da população mundial, o que acabou fazendo com que nos tornássemos reféns de máquinas e programas.

A realização desta pesquisa monográfica ocorreu por intermédio do método de compilação, consistindo na aglutinação de diversos pensamentos expostos por doutrinadores acerca do tema abordado e utilização de artigos retirados do meio eletrônico, possibilitando ao leitor uma enorme gama de pensamentos.

Para combater alguns crimes virtuais, entrou em vigor em 2021 a Lei nº 14.155, que incluiu alguns parágrafos no artigo 171 do Código Penal e alterou algumas regras sobre o poder de julgar um crime.

Como parte da discussão do tema, o primeiro capítulo trata dos conceitos que a lei traz e a natureza jurídica do crime de peculato virtual, por fim traz os reais motivos do crescimento desse crime, porém, o crescimento das redes sociais na sociedade atual, bem como sua importância no contexto global.

O segundo capítulo do trabalho trata-se da World Wide Web, também chamada de Internet, surgiu durante a Guerra Fria e, assim como o computador tinha finalidades militares, foi utilizada como uma forma alternativa de comunicação quando os meios convencionais não podiam ser utilizados, neste capítulo foi

abordado o conceito de rede mundial de computadores e as classificações doutrinárias existentes até o momento.

Já no terceiro capítulo tentará traçar algumas considerações sobre o crime de estelionato virtual em si, destacando em particular a ausência de uma norma específica que regule os tipos e as leis pendentes que tratam desta matéria. Para melhor compreensão do estudo que foi realizado, o capítulo será dividido em duas partes, na primeira parte será realizada uma análise geral do crime de peculato virtual no ordenamento jurídico brasileiro. No segundo momento, ele apresentará projetos e leis sobre o assunto.

O interesse por esse assunto surgiu por se tratar de um tema atual e cada vez mais presente no cotidiano da sociedade, considerando que os crimes virtuais são cada vez mais comuns e as pessoas cultivam a sensação de que o ambiente virtual é uma terra sem Leis.

CAPÍTULO I – LEI N° 14.155 DE MAIO DE 2021

Com intuito de combater alguns dos crimes virtuais, entrou em vigor, em 2021, a Lei n°14.155, que incluiu alguns parágrafos no artigo 171 do Código Penal e alterou algumas regras sobre a competência para julgar o delito.

Discorrendo sobre o assunto, o primeiro 1° capítulo trata dos conceitos trazidos pela lei e a natureza jurídica do crime de estelionato virtual, por fim, traz os reais motivos do crescimento deste delito, todavia o crescimento das redes sociais na sociedade atual, bem como a sua importância no contexto mundial.

1.1. Conceito jurídicos

A raiz etimológica da palavra estelionato tem origem a dezenas de séculos atrás, e deriva do vocábulo “estellio”, proveniente do latim, que quer dizer Camaleão, uma espécie de lagarto típico da África, que tem como característica principal a capacidade de alterar sua coloração natural para adaptar-se ao ambiente em que se encontra, visando enganar seus predadores e facilitar a captura se suas presas (NUCCI, 2017)

Comparando-se ao réptil citado anteriormente, o estelionatário possui uma facilidade excepcional em se moldar ao meio social em que habita, que em decorrência de seus disfarces e simulacros, enganar a vítima com seus costumes fraudulentos e age desonestamente todo o tempo, pois assim ele alcança seu objetivo final, que é o de iludir suas vítimas, obtendo a vantagem almejada:

> Pesquisas recentes indicam que por volta de 500 anos antes de cristo, já existiam rumores de que alguns egípcios ludibriavam os ricos e nobres comercializando falsos felinos e outros animais

> embalsamados para serem utilizados nas cerimônias fúnebres, segundo a tradição religiosa daquele povo. Na verdade, as múmias eram fraudulentas, e na maioria das vezes continham em seu interior pequenos pedaços de madeira e outros objetos, que simulavam o peso e o tamanho, e em alguns casos, restos de ossada de outros animais (NUCCI, 2017, p. 125).

No Brasil, o crime de estelionato está descrito no artigo 171 do Decreto-Lei nº 2.484 de 07 de dezembro de 1940 – O Código Penal Brasileiro, abaixo aduzido: Art. 171 - Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento: Pena - reclusão, de um a cinco anos, e multa (BRASIL, 1942)

Quando praticado de maneira ordinária, ou seja, em sua forma típica, o crime de estelionato sintetiza-se essencialmente na possibilidade em que o autor delituoso encontra para obter proveito de modo ilícito, para si, ou para outrem, utilizando-se de meios fraudulentos para tanto. O ordenamento jurídico brasileiro versa que somente a pessoa física pode ser sujeita ativo do crime de estelionato, cometendo-o de forma dolosa, com livre e consciente vontade, embora possa agir de modo diverso para alcançar seus fins (NUCCI, 2017).

Em contrapartida, o sujeito passivo desta modalidade será a vítima que sofreu o prejuízo patrimonial, devendo ser pessoa certa e determinada, embora muitas vezes exista mais de um indivíduo envolvido na relação. O crime de estelionato é delimitado pelo binômio, vantagem ilícita/ prejuízo alheio. A vantagem ilícita é esclarecida por um proveito que não encontra amparo legal no ordenamento jurídico, sendo contrário a ele, não obedecendo ao princípio da legalidade. Se porventura o objeto fosse lícito, o fato poderia ser desclassificado para outra infração penal, como o exercício arbitrário das próprias razões (PRADO, 2002).

Existem inúmeras discursões a respeito da categoria desta vantagem ilícita. A doutrina majoritária, no entanto, posiciona-se no sentido de que a palavra vantagem ilícita abrange toda e qualquer tipo de vantagem, sendo revestida ou não de cunho econômico.

Desta forma, afirma Luiz Regis Prado que:

> Prevalece o entendimento doutrinário de que a referida vantagem não necessita ser econômica, já que o legislador não restringiu o seu alcance como o fez no tipo que define o crime de extorsão, no qual empregou a expressão indevida vantagem econômica. (PRADO,2002, p. 183)

Além da vantagem ilícita obtida pelo agente, a vítima sofre igualmente o prejuízo, que também será de natureza econômica. O prejuízo não se baseia apenas naquilo em que a vítima perdeu, como por exemplo, aquela que entrega determinada quantia ao estelionatário esperando certo tipo de retorno, mas também, naquela que deixou de ganhar o que lhe era devido, quando enganada pelo agente (PRADO, 2002).

O caput do artigo 171 do Código Penal diz que a vantagem ilícita deve ser convertida em acréscimo ao patrimônio do próprio agente ou para terceiro, que neste caso, poderá não saber se aquilo que o delinquente está entregando é ou não produto de crime, afastando sua responsabilidade pelo delito de estelionato, desde que não tenha atuado em concurso de pessoas, antevisto no art. 29 deste mesmo diploma (PRADO, 2002).

A finalidade do legislador originário ao inserir o tipo penal do estelionato dentro do conjunto normativo de leis brasileiro foi a de proteger a inviolabilidade do patrimônio das pessoas que convivem em uma sociedade, bem como a dignidade dos cidadãos de boa conduta, que travam árduas batalhas diárias para conseguir edificar seus bens e não podem ficar à mercê desta espécie de transgressor (PRADO, 2002).

O preceito primário do ilícito penal do estelionato descrito no art. 171 do CPB leciona que ele será cometido mediante a utilização de artifício, ardil, ou qualquer outro meio fraudulento, forma pela qual o agente ilude a vítima, atraindo-a, tecendo uma situação fantasiosa, impossibilitando que o agente passivo tome conhecimento da real situação que está ocorrendo (MIRABETE, 2000).

Segundo o doutrinador Mirabete;

> O artifício existe quando o agente se utiliza de um aparato que modifica, ao menos aparentemente, o aspecto material da coisa, figurando entre esses meios o documento falso ou outra falsificação qualquer, o disfarce, a modificação por aparelhos mecânicos ou elétricos, filmes, efeitos de luz, etc (MIRABETE, 2000)

O emprego de meio ardil é caracterizado pela imaterialidade, astúcia, ou pela simples sutileza de aspecto unicamente intelectual, pois o indivíduo se vale do desfavorecimento da vítima que encontra-se em posição de subordinação perante o estelionatário, e age movida pela emoção, convicção ou ilusão, beneficiando a ação ilícita do criminoso em obter o resultado da subtração do bem patrimonial, sem que ela se dê conta de que está sendo enganada (MIRABETE, 2000).

No que tange o tipo penal referindo-se a qualquer outro meio fraudulento, sabe-se que este meio deve ser idôneo, de maneira a enganar a vítima, que segundo o ilustre professor Mirabete;

> Discute-se, na aferição da idoneidade do meio empregado, se deve ser levada em consideração a prudência ordinária, o discernimento do *homo medius*, ou a pessoa da vítima, concluindo os doutrinadores por esta última hipótese. Embora já se tenha decidido que as manobras fraudulentas devem ser suficientes para embair a média argúcia, a prudência normal, aquele mínimo de sagacidade que a pessoa comum usa em seus negócios, é francamente predominante a jurisprudência de que a idoneidade do meio deve ser pesquisada no caso concreto, inclusive, tendo-se em vista as condições pessoais da vítima (MIRABETE, 2000, p. 53).

1.2. Natureza jurídica

O Código Penal Brasileiro consiste em um compilado de leis penais que foi sistematicamente organizado para auxiliar a aplicação de sanções aos crimes que ocorrem no seio da sociedade. O pilar da produção desse código é o Direito Penal, que surgiu para regular as ações dos indivíduos e preservar a sociedade, buscando livrar o cidadão de crimes e males que coloquem em risco a sua vida e convivência pacífica do coletivo (BRASIL,1940).

Diversos crimes são regulados pelo Código penal, impedindo que direitos em áreas distintas da sociedade sejam prejudicados. Quanto à prática delituosa que permeia a relação consumerista, o legislador material confere tipificação a partir das figuras delituosas definidas como os crimes de estelionato e de fraude (NUCCI, 2017).

Sendo assim, quando se tem a prática de delito na efetivação da relação de consumo, podendo a sua autoria partir de qualquer dos sujeitos, o sistema de justiça confere aplicabilidade da legislação penal a partir dos 02 (dois) tipos penais já estabelecidos (NUCCI, 2017).

No Código Penal Brasileiro, o crime de estelionato está disposto no Artigo n. º 171 da seguinte maneira:

> Art. 171 Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artificio, ardil, ou qualquer outro meio fraudulento:
>
> Pena - reclusão, de 1 (um) a 5 (cinco) anos, e multa. (BRASIL, 1940, p. 56)

Qualquer indivíduo que cometer os atos dispostos no caput do artigo estará cometendo o crime, porém, ainda existem modalidades diferentes do delito que exigem do indivíduo uma característica especial. A vítima desse criminoso será também qualquer pessoa que sofra com o ato, porém, para se caracterizar nas modalidades diferenciadas do crime, deverá a vítima apresentar características especiais. O objeto jurídico que é afetado por esse crime é o patrimônio da vítima, e, o objeto material é a vantagem obtida ou a coisa alheia (NUCCI, 2017).

Segundo Nucci (2017), existem diversas maneiras de se cometer o crime de estelionato, sendo a sua forma genérica a que está disposta no caput do artigo, que é quando o indivíduo obtém determinada vantagem sobre outra pessoa ao induzi-la a erro, ou, fazer que permaneça nele. A vítima deve contribuir com o criminoso, porém sem notar que está colocando a risco o seu patrimônio. O autor do crime pode provocar a situação de engano ou simplesmente fazer que a vítima permaneça em erro, usando de artifícios, meios ardilosos ou qualquer outra forma de fraude.

Como supracitado, existem outras espécies do crime de estelionato, que necessitam de condições especiais do autor e da vítima, entretanto, a pena continua sendo a mesma. As modalidades especiais do crime de estelionato são: Disposição de coisa alheia como própria (§2º I); Alienação de forma fraudulenta de coisa própria (§2º, II); Defraudação de penhor (§2º, III); Fraude na entrega da coisa (§2º, IV); Fraude para o recebimento de indenização ou valor de seguro (§2º, V); Fraude no pagamento por meio de cheques (§2º, VI); Estelionato contra idosos (§2º, VII) (BRASIL, 1940).

O crime de estelionato pode ser classificado em comum, como disposto no caput, ou como próprio e de forma vinculada, levando em consideração o §2º. Se o autor for réu primário, e o prejuízo causado for de pequeno valor, poderá o juiz aplicar a pena seguindo o disposto no art. 155, §2º (BRASIL, 1940).

A pena pode ser aumentada em até 1/3 se o crime for realizado contra alguma entidade de direito público ou instituto de economia popular, de beneficência ou assistência social. Este crime pode ser cometido na forma tentada e o momento em que ele se consuma é quando a vítima perde o seu patrimônio (NUCCI, 2017).

Além do crime de estelionato, outro delito que é cometido com frequência no âmbito virtual é o crime de fraude no comércio, que está expresso no artigo 175 do Código Penal Brasileiro:

> Art. 175 - Enganar, no exercício de atividade comercial, o adquirente ou consumidor:
>
> I - Vendendo, como verdadeira ou perfeita, mercadoria falsificada ou deteriorada
>
> II - Entregando uma mercadoria por outra:
>
> Pena - detenção, de seis meses a dois anos, ou multa. (BRASIL, 1940)

Neste crime, apenas o comerciante pode ser o autor, e ele necessita estar praticando atividade de comércio, e não nos casos que ele estiver praticando atos em negócios entre particulares. A vítima é a pessoa que comprou um pronto com alguma das características contidas no caput do artigo e teve o patrimônio, como bem jurídico violado. O objeto material do crime será a mercadoria falsificada, deteriorada ou substituída (NUCCI, 2017).

Para Nucci (2017), aquele que engana o consumidor durante a atividade comercial, ao vender como sendo verdadeira ou perfeita, uma mercadoria que na verdade é falsificada ou está deteriorada, ou, ainda, que quando faz a substituição de um produto por outro, está cometendo o crime de fraude no comércio.

É possível classificar esse crime como sendo um crime próprio, pois é preciso que o agente causador tenha uma condição especial, no caso, que seja comerciante. Trata-se também de um crime material; de forma livre; comissivo; instantâneo; unissubjetivo e plurissubsistente. A forma tentada deste crime é aceita, e, considera-se o crime consumado no instante que a vítima sofre prejuízo com a negociação (NUCCI, 2017).

Se o agente altera em uma obra que a ele foi encomendada, o peso ou a qualidade do metal, ou, substituir, nas mesmas situações, uma pedra verdadeira por outra que é inferior ou que seja falsa, ou, se vender como verdadeira uma pedra ou

metal falso, passará a ter pena como de reclusão que poderá ser de 1 (um) a até 5 (cinco) anos, além de multa. Porém, se se tratar de um agente réu primário e o objeto do crime for de pequeno valor, permite-se ao juiz a substituição de reclusão por detenção, além de poder diminuir a pena de 1/3 ou 2/3, ou, apenas aplicar uma multa (NUCCI, 2017).

Além do Código Penal, também pode ser encontrado no Código de Defesa do Consumidor uma modalidade do crime de fraude:

> Art. 66 Fazer afirmação falsa ou enganosa, ou omitir informação relevante sobre a natureza, característica, qualidade, quantidade, segurança, desempenho, durabilidade, preço ou garantia de produtos ou serviços:
>
> Pena – Detenção de 3 (três) meses a 1 (um) ano, e multa (BRASIL, 1990).

O fornecedor, que ofereça determinado produto ou serviço com as características contidas no artigo, estará cometendo o crime de fraude em oferta. A vítima desse crime é o consumidor que foi enganado pela oferta fraudada. Aquele que patrocinar a oferta, também responderá pelo crime e incorrerá na mesma pena (ALMEIDA,2013).

Assim, a legislação busca proteger os direitos de livre escolha do consumidor, além de lhe garantir que o mesmo receba sempre a informação adequada sobre o produto que está adquirindo, e completa, que para o autor do crime, a vontade subjetiva presente é a de fazer uma afirmação que seja falsa ou enganosa, e assim, garantir uma venda ou contratação fraudulenta. A modalidade culposa desse crime possui pena diferente, pois esta passa a ser de detenção, e o período nela estipulado é de 1 (um) mês a 6 (seis) meses, além do pagamento de multa. (ALMEIDA, 2009, p. 229),

O crime se consuma quando o fraudador divulga publicamente a oferta falsa, independente de ela ser eficaz ou não. Pode sim ocorrer a forma tentada do crime, mas considera-se de difícil realização (PARODI, 2013).

Conhecido os crimes, torna-se possível analisar a sua ocorrência no comércio virtual. Há ainda o crime denominado Fraude da Loja Falsa, que é uma espécie de fraude, e ocorre com a hospedagem de lojas comerciais falsas em sites da internet, sendo que os responsáveis por gerenciar essa loja são organizações criminosas. Normalmente, a loja recebe uma interface bem desenvolvida que

transmite maior sensação de confiança ao cliente, e passa a ofertar produtos com preços abaixo do valor padrão de mercado. “Muitas vezes, os golpistas simplesmente anunciam uma mercadoria aproveitando dados fictícios ou roubados, empresas laranjas ou fantasmas ou o bom nome de empresas verdadeiras”. (PARODI, 2013, p. 185).

Para atrair vítimas, os criminosos criam perfis falsos e realizam avaliações positivas sobre a loja, o que transmite ainda mais credibilidade sobre a falsa idoneidade da loja. Além de oferecer produtos muitas vezes inexistentes, utilizam também o site para capturar dados das vítimas para efetuar compras ou ter acesso a conta bancária dos mesmos (PARODI, 2013).

Outra modalidade, é a Fraude da página falsa para extrair dados, que consiste em uma reprodução quase idêntica da página de alguma loja bem conhecida pelos consumidores, porém, com diferenças minúsculas e quase imperceptíveis no endereço de acesso a página. Como dito:

> Não são raros os exemplos em leilões virtuais e também a clonagem de páginas de internet banking de entidades bancárias conceituadas brasileiras que, frequentemente, emitem notas públicas, anunciando a referida fraude e é nessas horas que o consumidor precisa ser muito cuidadoso em observar erros de português, endereços e telefones para contato da empresa responsável. (ALMEIDA, 2013, p. 41)

Geralmente, esses endereços falsos são divulgados através de e-mails spam para de inúmeros usuários, que, atraídos pelos preços das falsas promoções do site, iniciam seu cadastro para realizar a compra e são então encaminhados para outra página falsa, que tem apenas a função de coletar dados. Sem perceber, o consumidor acaba informando os seus dados pessoais, como: nome completo, data de nascimento, Cadastro de Pessoa Física (CPF), número e titular do cartão, além do código de segurança que é essencial para realizar compras com o mesmo (ALMEIDA,2013)

Essa técnica recebe o nome de Phishing:

> O phishing pode ocorrer de diversas formas. Algumas são bastante simples, como conversas falsas em mensageiros instantâneos e e-mails que pedem para clicar em links suspeitos. Fora isso, existem páginas inteiras construídas para imitar sites de bancos e outras instituições. (MULLER, 2012, s/p).

Com isso, os criminosos se encontram aptos a realizar compras utilizando os dados do consumidor, que na maioria das vezes descobrem tardiamente que foram enganados por criminosos e seu cartão está cheio de compras que ele não realizou. Outro tipo de página que é muito copiada é a de instituições bancárias, no qual os clientes disponibilizam todos os seus dados, e depois tem as suas contas bancárias invadidas e seu patrimônio violado por criminosos (MULLER, 2012).

Tem-se a Fraude do anúncio falso, relacionado à atividade publicitária enganosa, tendo como definição:

> Conta no sistema de leilão virtual, aberta com dados e documentos falsos, ofertando mercadorias muito atrativas (como tipo e preço), com o único intuito de receber o pagamento adiantado, em uma conta também aberta com documentos falsos, prometendo o envio da mercadoria em seguida e depois sumir. Por demorar um tempo antes que o comprador/vítima se preocupe e denuncie, os golpistas têm uma vantagem e podem aplicar o golpe várias vezes antes de desaparecer. Neste caso normalmente a qualificação do golpista vendedor (ou seja, a nota e o histórico que ele tem), no sistema de leilão virtual, é nula, pois as contas sempre são muito recentes. (PARODI, 2013, p. 184)

O Estelionato na compra online, não está ligado a venda, mas sim a compra de produtos. O delito ocorre da seguinte maneira: a vítima anuncia a venda de algum produto, e logo em seguida é contatado pelo criminoso que diz se interessar em adquirir o objeto, porém diz só pode realizar o pagamento via cartão de crédito, e pergunta se não poderia ser utilizado outra plataforma para que o pagamento seja realizado da maneira desejada (PARODI, 2013).

Sem desconfiar, a vítima concorda e aceita a proposta, e parte para a negociação na plataforma apresentada. O criminoso diz ter realizado o pagamento e logo em seguida a vítima recebe um falso e-mail comprovando o pagamento e solicitando que o produto seja enviado ao endereço do criminoso. Só após perceber que não recebeu dinheiro algum pela venda, constata que enviou ao criminoso o seu produto após ter sido enganado (PARODI, 2013).

1.3. Da aplicação da pena

Para que reste configurado o delito em tela, a lei exige que exista o dolo do agente em praticar a conduta, não sendo admitida a modalidade culposa, estando ele consciente de sua pretensão de iludir a vítima. Da mesma maneira, exige-se também o denominado “elemento subjetivo do injusto” (dolo específico), que nada

mais é do que o *animus* de obter ilícita vantagem patrimonial para si ou para outrem (HUNGRIA, 1980).

A consumação do estelionato se dá no momento da obtenção da vantagem ilícita em prejuízo alheio, na ocasião em que a coisa ou objeto passa da esfera de disponibilidade da vítima para a do transgressor. Por outro lado, a tentativa irá ocorrer, quando, depois de iniciados os atos de execução o agente não consegue obter a vantagem ilícita por circunstâncias alheias a sua vontade, ou na hipótese de o criminoso, embora não tenha conseguido obter a vantagem, pudesse consegui-la, gerando um dano em potencial, também passível de repressão.

Ressalte-se que o estelionato pode ser cometido de maneira comissiva e omissiva, a depender da maneira de proceder do agente delituoso. A conduta típica que tem por finalidade a obtenção de vantagem antijurídica em prejuízo de terceiro é praticada por intervenção da fraude do agente, que induz ou mantém a vítima em erro. Por indução, entende-se o direcionamento do comportamento do autor de forma comissiva para a concretização do ato, isto é, fazendo algo para que a vítima seja induzida a erro (HUNGRIA, 1980).

De outro ângulo, a conduta de manter a vítima em erro poderá ser praticada omissivamente, quando o estelionatário toma conhecimento de que o sujeito passivo encontra-se incorrendo em erro e aproveita-se desta oportunidade para obter o enriquecimento indevido (HUNGRIA, 1980).

Nesse sentido, preleciona Nelson Hungria:

> Há uma analogia substancial entre o induzimento em erro e o doloso silencio em torno do erro preexistente. Praticamente, tanto faz ministrar o veneno como deixar scienter que alguém o ingira por engano (...). A inércia é uma spécies do genus “ação”, é a própria atividade que se refrange sobre si mesma, determinando-se ao non facere. Tanto usa de fraude quem ativamente causa um erro para um fim ilícito, quanto quem passivamente deixa-o persistir e dele se aproveita (HUNGRIA, p. 208-209)

A aplicabilidade penal do estelionato depende diretamente do conteúdo contido no preceito secundário do art. 171 do Código Penal Brasileiro, sem o qual seria impossível impor qualquer tipo de punição aos infratores que sucedem nesta prática. A pena cominada em tal preceito é de um a cinco anos de reclusão, mais o

pagamento de multa, a ser definida pelo magistrado quando do momento da sentença penal condenatória.

Ainda que o crime de estelionato seja uma violação grave ao ordenamento jurídico e ocasione danos muitas vezes irreversíveis, o acusado, desde que não esteja respondendo por outro processo criminal com decisão transitada em julgado, e ainda, não sendo reincidente de crime doloso, preenchendo igualmente as condições satisfatórias no que refere à culpabilidade, os antecedentes, a conduta social e a sua personalidade, bem como os motivos e as circunstâncias, resguardadas pelo artigo 59 do Código Penal, poderão ser beneficiados pela suspensão condicional do processo (SURSIS), prevista no artigo 89, § 1º da Lei 9.099/95, que trata dos juizados especiais criminais, considerando-se que a pena mínima para o estelionato é de um ano, *in verbis:*

> Art. 89. Nos crimes em que a pena mínima cominada for igual ou inferior a um ano, abrangidas ou não por esta Lei, o Ministério Público, ao oferecer a denúncia, poderá propor a suspensão do processo, por dois a quatro anos, desde que o acusado não esteja sendo processado ou não tenha sido condenado por outro crime, presentes os demais requisitos que autorizariam a suspensão condicional da pena.
>
> § 1º Aceita a proposta pelo acusado e seu defensor, na presença do Juiz, este, recebendo a denúncia, poderá suspender o processo, submetendo o acusado a período de prova, sob as seguintes condições:
>
> I - reparação do dano, salvo impossibilidade de fazê-lo;
>
> II - proibição de frequentar determinados lugares;
>
> III - proibição de ausentar-se da comarca onde reside, sem autorização do Juiz;
>
> IV - comparecimento pessoal e obrigatório a juízo, mensalmente, para informar e justificar suas atividades. (BRASIL, 1995)

A suspensão poderá ser proposta por parte do Ministério Público quando do oferecimento da denúncia. Se o acusado aceitar a proposta ofertada pelo Parquet (Ministério Público ou faz referência a um membro do Ministério Público), o juiz irá suspender o processo por um período não inferior a dois anos e não superior a quatro anos, ficando o cumprimento da pena condicionada ao bom comportamento do suspeito, devendo exercê-la com alguma restrição imposta, que pode ser a reparação do possível dano causado, a proibição de frequentar determinados lugares, não se ausentar da comarca em que reside sem autorização da autoridade

competente, comparecer mensalmente em juízo para justificar suas atividades e não ser processado novamente por outro crime, evento que poderá implicar na revogação do benefício.

O sentido real da concessão de suspensão condicional do processo é evitar que o agente entre em contato de perto com o sistema carcerário, alterando seu convívio social e seu ciclo de amizades, haja vista o sistema penitenciário nacional carecer de assistência sob diversos ângulos, afinal, as estatísticas comprovam que na maioria dos estados, mais de 90% dos criminosos que recebem a liberdade, voltam a delinquir.

Portanto, a suspensão de que trata o art. 89 da lei 9.099/95 tem caráter exclusivamente motivador e preventivo, pois oferece ao réu a uma “nova chance” de alterar sua conduta, não voltando a cometer crimes, redimindo-se com a sociedade.

Contudo, se após as investigações for constatado que não há como se aplicar o benefício supracitado, o procedimento irá seguir seu rito normal, onde, ao final, poderá o juiz concluir pela condenação ou absolvição. Em caso de condenação, o réu terá sua pena calculada por intermédio da dosimetria da pena, conforme nos ensina o ilustre docente Jorge Vicente Silva:

> O réu sendo condenado no crime de estelionato terá a fixação da pena aplicada pelo Juiz, por meio da dosimetria da pena, disciplinado no artigo 68 do Código Penal, tratando-se de um sistema trifásico sendo observado primeiramente os critérios do artigo 59 deste dispositivo legal, seguido das considerações quanto às circunstâncias atenuantes e agravantes, e por último as causas de diminuição e de aumento da pena (SILVA, p.55, 2005).

A primeira fase deste sistema de cálculo de pena é a computação da penabase, que deverá ser realizada de acordo com o mínimo e o máximo legal permitido, obedecendo ao inciso II do artigo 59 do código penal, que, no caso do estelionato, a pena mínima será de um ano e a máxima de cinco anos, em conformidade com o artigo 171 deste mesmo diploma legal.

Esta fase inicial do sistema de cálculo é crucial para que se ajuste a pena à conduta individual do acusado, fazendo com que a punição seja equitativa ao ato praticado. É nesta fase que o juiz irá identificar qual o regime inicial de cumprimento

de pena, que no caso do estelionato, é o de reclusão, podendo ser executada no regime fechado, semi-aberto ou aberto (MIRABETE, 2000).

CAPÍTULO II - A REDE MUNDIAL DE COMPUTADORES E OS CRIMES VIRTUAIS

A rede mundial de computadores, também denominada internet foi criada no período da guerra fria, e assim como o computador, possuía fins militares, era utilizada como uma forma de comunicação alternativa, caso não fosse possível utilizar os meios convencionais.

2.1. Conceitos de rede

Criada inicialmente com fins exclusivamente militares, em 1969 foi criada a primeira rede nacional de computadores pelo departamento de defesa dos Estado Unidos da América, a ARPANET (*Advanced Research Projects Administration – Administração de Projetos e Pesquisas Avançados),* com intuito de compartilhar informações, pesquisas e estratégias militares conectando os computadores dos centros de pesquisas, universidades e instituições militares americanas. (ROSA, 2002).

Em 1972 a internet foi apresentada à sociedade pelo governo americano. Com a ideia de implementação da internet nas universidades americanas. E no fim do mesmo ano, Ray Tomlinson desenvolveu o correio eletrônico, hoje popularmente conhecido como e-mail (BARROS, 2013).

Assim, em 1980 se começou a utilizar o protocolo aberto o qual possibilitava uma conexão de sistemas heterogêneos, denominado TCP IP (*Transmission Control Protocol – Internet Protocol*, *em português Protocolo de Controle de Transmissão - Protocolo de Internet*). Este novo protocolo permitiu o acesso de diferentes equipamentos.

O autor Gabriel César Zaccaria de Inellas explica o protocolo utilizado pela rede mundial de computadores: “Protocolo é a designação dada aos formatos de mensagens e suas regras, entre dois computadores, para que possahaver trocade mensagens. Cumpre salientar que o protocolo permite a comunicação entre os dois comunicadores” (2009, p.02).

Contudo, foi em 1983 que surgiu a definição internet. Assim, em 1991 foi lançada a *World Wide Web* (WWW), permitindo a transmissão de imagens, sons e vídeos pela rede, sendo que até então apenas poderiam ser transmitidos textos. A internet se disseminou, e então houve a criação de provedores concedendo o acesso à internet, para que os usuários pudessem dela utilizar (PAESANI, 2013).

Com o passar do tempo, sua estrutura foi sendo ampliada e melhorada, tornando-se mundial, interligando países, e diminuindo as fronteiras geográficas. Nas palavras de Zanellato, “A Internet é um suporte (ou meio) que permite trocar correspondências, arquivos, ideias, comunicar em tempo real, fazer pesquisa documental ou utilizar serviços e comprar produtos” (ZANELLATO, 2002.p.173).

No Brasil, a internet começou a ser implantada de forma lenta e progressiva, houve uma série de ações governamentais para que se desse início ao desenvolvimento das telecomunicações. O setor de telecomunicações era dominado por empresas privadas e seu desempenho era de baixíssima qualidade. Em 1964 foi implantado o Código Brasileiro de Telecomunicações que implantou o Ministério das Comunicações, e mais tarde a Empresa Brasileira de telecomunicações (EMBRATEL) criada para implantar a rede nacional. (DIAS, 2004).

No ano de 1994 a Internet se tornou comercial no país e, no ano seguinte, o Ministério de Ciência e Tecnologia e o Ministério das Comunicações, criou o *Comitê Gestor da Internet* (CGI), formado por representantes da academia, das empresas envolvidas nas conexões, provedores e usuários, com o fim de regulamentar o uso da rede e fomentar o desenvolvimento dos serviços ligados à Internet (OLIVEIRA, 2011).

Houve uma série de outros fatos que influenciaram diretamente a implantação do sistema de internet do Brasil. Contudo, foi apenas em 1996 que a Internet comercial chegou ao Brasil, ainda com uma infraestrutura insuficiente para

atender às demandas de seus provedores e usuários. Houve um crescimento no número de usuários, mas também em transações por meio do comércio eletrônico. E assim, gradativamente houve a implantação de novas tecnologias até os dias atuais. Surgiram ainda, as tecnologias de banda larga, sendo que atualmente existe uma gama de opções de conexão, seja ela via satélite, telefonia celular ou via rádio.

Atualmente, segundo o IBGE (*Instituto Brasileiro de Geografia e Estatística*), mais de 63% dos domicílios brasileiros possuem acesso á internet em casa, o grande aumento deve-se ao acesso em outros dispositivos além do computador, como os smartphones, já que segundo dados 94,8% utilizam o celular para se conectar à rede (IBGE, 2015).

Dessa forma, o avanço tecnológico, e a implantação da internet possibilitou a comunicação direta entre pessoas de qualquer parte do planeta, encurtando fronteiras, sendo considerada como o principal meio de transmissão de informação.

Não existe um consenso entre a doutrina quanto à denominação dos crimes praticados relacionados com o ambiente virtual, assim recebem as mais diferentes nomenclaturas. O crime corresponde de certa forma a todas as condutas tipificadas cometidas com o uso de tecnologia. Contudo, as acepções são amplas e variam de acordo com o ponto de vista de cada um.

Segundo Paulo Quintiliano, observou a diferença entre crimes de informática e crimes cibernéticos:

> Crimes de informática são todas as ações típicas, antijurídicas e culpáveis praticados com a utilização de computadores e/ou de outros recursos da informática. Por sua vez, crimes cibernéticos são aqueles cometidos utilizando a Internet, ou seja**,** o crime cibernético é espécie do crime de informática, uma vez que se utiliza de computadores para acessar a Internet (PECK, 2002).

Já para o autor Sérgio Marcos Roque 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” (2007, p. 25).

Para o doutrinador Augusto Rossini, o delito de informática pode ser defino da seguinte forma:

> [...] “delito informático” poderia ser talhado como aquela conduta típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, praticada por pessoa física ou

> jurídica, com o uso da informática, em ambiente de rede ou fora dele, e que ofenda, direta ou indiretamente, a segurança informática, que tem por elementos a integridade, a disponibilidade a confidencialidade. (2004, p. 110).

Segundo Carla Rodrigues Castro, “a maioria dos crimes é praticado por meio da internet, e o meio mais utilizado é o computador. Dessa forma, são considerados crimes de informática aqueles consumados e realizados através utilização de computadores” (2003, p.09).

Partindo de outro viés, a *Convenção sobre o Cibercrime de Budapeste*, realizada no ano de 2001, definiu os crimes de informática são aqueles perpetrados por meio dos computadores, contra eles ou através deles, de modo que a maioria dos crimes é praticada por meio do sistema de internet (SCHMIDT, 2014).

Assim, pode se dizer que os crimes cibernéticos são todas as condutas típicas, antijurídicas e culpáveis praticadas com a utilização do sistema de informática, classificadas doutrinariamente em crimes puros, mistos e comuns, e, crimes próprios e impróprios (CASTRO, 2003).

Os crimes cibernéticos puros levam em consideração toda e qualquer conduta ilícita que utilize de forma exclusiva o sistema de computador, englobando o atentado físico ou técnico deste, inclusive dados e sistemas. Já os crimes mistos são aqueles o uso da internet ou do sistema é condição primordial para a efetivação da conduta. Por fim, os crimes cibernéticos comuns são aqueles em que a internet é utilizada para como meio para a realização de um crime já tipificado em lei (PINHEIRO, 2002).

Por sua vez, os crimes próprios são considerados aqueles em que o bem jurídico protegido pela norma penal é a inviolabilidade das informações automatizadas. Já os crimes impróprios seriam aqueles que atingem um bem jurídico comum, como por exemplo, o patrimônio do individuo através de um sistema informático (VIANNA; MACHADO, 2013).

Nas palavras de Damásio Evangelista de Jesus (pg.56):

> Crimes eletrônicos puros ou próprios são aqueles que sejam praticados por computador e se realizem ou se consumem também em meio eletrônico. Neles, a informática (segurança dos sistemas, titularidade das informações e integridade dos dados, da máquina e periféricos) é o objeto jurídico tutelado.

> Crimes eletrônicos impuros ou impróprios são aqueles em que o agente se vale do computador como meio para produzir resultado naturalístico, que ofenda o mundo físico ou o espaço “real”, ameaçando ou lesando outros bens, não computacionais ou diversos da informática. (CARNEIRO, 2002).

Portanto, os crimes virtuais próprios são aqueles em que o computador, como sistema tecnológico é usado como objeto e meio para execução do crime, já os crimes virtuais denominados impróprios são aqueles realizados com a utilização do computador, onde este é utilizado como instrumento para realização de condutas ilícitas.

2.2 Classificações doutrinárias

A classificação de crimes virtuais é uma área em constante evolução devido à rápida expansão da tecnologia e do uso da internet em todo o mundo. Segundo Sibal; Bhatia, "a internet é uma ferramenta de comunicação poderosa que tem impulsionado a economia global, permitindo que as empresas expandam seus negócios e aumentem seus lucros". Deste modo, o avanço tecnológico colocou a internet como ferramenta indispensável no dia a dia, consequentemente aumentou a ocorrência de crimes no mundo digital (2015, pg.83).

Para classificar os crimes virtuais, os pesquisadores geralmente se baseiam em categorias estabelecidas pelo governo ou pela polícia, como o FBI nos Estados Unidos. O FBI, por exemplo, classifica os crimes virtuais em três categorias principais: "crimes contra computadores", "crimes contra pessoas" e "crimes contra propriedade". Essas categorias incluem subcategorias, como hacking, phishing, fraudes online, crimes sexuais online, roubam de identidade e muito mais (FBI, 2019).

Alguns doutrinadores propõem classificações mais detalhadas e específicas para crimes virtuais. Por exemplo, uma classificação de sete categorias, incluindo crimes financeiros, crimes contra a privacidade, crimes de propriedade intelectual, crimes de violência, crimes de ódio, crimes de tráfico de drogas e crimes cibernéticos de guerra (KSHETRI, 2018).

Da mesma forma foi proposto uma classificação de seis categorias, incluindo crimes financeiros, crimes sexuais, crimes de vigilância, crimes de hacking, crimes de spam e crimes de assédio (HOLT, 2013).

Assim, a classificação de crimes virtuais é uma área complexa e em constante evolução. As categorias e subcategorias podem variar de acordo com a perspectiva e as necessidades dos pesquisadores e das autoridades governamentais. É importante continuar a desenvolver e aprimorar a classificação de crimes virtuais para garantir que as leis e as políticas estejam atualizadas e possam prevenir e punir adequadamente esses tipos de crimes (ARAS, 2018).

Os Crimes Virtuais, também conhecidos como crimes cibernéticos, podem ser classificados em três categorias principais:

> - Crime informático: envolve o acesso não autorizado a um sistema informático, roubo ou dano de informações, falsificação ou destruição de dados, ou a disseminação de vírus ou malware;
> - Crime financeiro: inclui fraudes bancárias, roubo de identidade, phishing (roubo de informações pessoais por meio de e-mails ou sites falsos), e outras atividades fraudulentas realizadas com o objetivo de obter ganhos financeiros ilícitos;
> - Crime contra a privacidade: consiste em violações de privacidade, incluindo o monitoramento não autorizado de comunicações privadas, a divulgação não autorizada de informações pessoais e o uso indevido de informações pessoais para fins maliciosos.

Essas são apenas algumas das categorias de crimes virtuais, e a lista pode ser muito mais extensa, pois os criminosos estão sempre inventando novas formas de explorar vulnerabilidades e cometer delitos online.

As redes sociais são ambientes onde internautas compartilham fotos, vídeos, textos e diversos outros conteúdos, os quais ficam acessíveis a uma grande quantidade de pessoas. Assim, passou a servir como refugio para a prática de atos criminosos, tendo em vista a forma do anonimato disfarçado. Assim, tem se tornado cada vez mais frequentes demandas judiciais que envolvam crimes praticados em redes sociais, em especial, no *facebook*, *instagram*, e aplicativos de troca de mensagens, como o *Whatssap* (ARAS, 2018).

Atualmente, as redes sociais é o meio de comunicação mais utilizado entre os indivíduos. Dentre alguns dos crimes mais praticados podemos destacar os crimes contra a imagem, honra e intimidade, ou seja, os crimes de calúnia,

difamação, injúria e racismo. E tendo em vista, a velocidade de transmissão de informações e gama de sujeitos que terão acesso ao conteúdo ofensivo, os crimes têm seus efeitos potencializados (ARAS, 2018)

A Constituição Federal de 1988 trata a honra como direito fundamental:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: [...] X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação; (BRASIL, 1988).

Assim, além da natureza jurídica de direito fundamental, a honra também constitui um dos direitos da personalidade, isto é, “aqueles que têm por objeto os atributos físicos, psíquicos e morais da pessoa em si e em suas projeções sociais” (GAGLIANO; PAMPLONA FILHO, 2012).

Os crimes de calúnia, difamação e injúria, estão previstos respectivamente nos artigos 138, 139 e 140 do Código Penal Brasileiro.

> Art. 138 - Caluniar alguém, imputando-lhe falsamente fato definido como crime: Pena - detenção, de seis meses a dois anos, e multa.
>
> Art. 139 - Difamar alguém, imputando-lhe fato ofensivo à sua reputação: Pena - detenção, de três meses a um ano, e multa.
>
> Art. 140 - Injuriar alguém, atendendo-lhe a dignidade ou decoro: Pena - detenção, de um a seis meses, ou multa (BRASIL, 1940).

Contudo, para que haja configuração do crime contra a honra por meio das redes sociais, é preciso que estejam presentes todas elementares do tipo penal, bem como o elemento subjetivo do delito. No caso da calúnia, é necessária a imputação da prática de determinado fato, e que este seja qualificado como crime, sendo consumada quando a referida atribuição se torna conhecida por terceiro (BITENCOURT, 2011).

Na difamação, é preciso imputação de um fato determinado, fato este ofensivo à reputação da vítima, podendo ser verdadeiro ou não, com a comunicação do fato a terceiros. Já a injúria, requer uma afirmativa que atribua uma

característica depreciativa à vítima, contudo, não é necessário que a ofensa seja proferida de maneira pública, bastando apenas que chegue ao conhecimento da vítima para a sua consumação (BITENCOURT, 2011).

Tais práticas delituosas podem ser perpetradas por meio de *direct message* (DM) no *Twitter* e *Instagram* ou pelo *inbox* do *Facebook*, pois são recursos que permitem o envio mensagens privadas à pessoa visada, ou ainda realizadas em publicações em modo público.

Assim no âmbito das redes sociais, os referidos crimes podem ser cometidos por meio de publicações na própria linha do tempo do usuário ou de terceiros, tweets, comentários nas postagens de outrem e quaisquer meios em que a ofensa seja repassada a terceiros, já que é imprescindível que alguém além da vítima dela tome conhecimento.

Apenas a título de conhecimento, o *Facebook*, dispõe de uma ferramenta onde é possível que usuário possa denunciar uma publicação, foto ou comentário, solicitando a remoção de conteúdo ou da conta que viole os Padrões da Comunidade, sendo assim consideradas as publicações contendo nudez, discurso de ódio, violência e conteúdo gráfico, que veiculem ameaças diretas, *bullying* ou assédio, que ameacem ou promovam exploração ou violência sexual, entre outros. (SOUZA, 2014).

Tais crimes são compatíveis com o meio digital e podem ser facilmente praticados por meio da Internet, já que se trata de crimes de forma livre, que podem ser praticados por qualquer modo, sejam por meio do correio eletrônico, aplicativos de mensagens instantâneas, blogs e redes sociais a fim de disseminar a ofensa. Cabendo ao legislador criar normas a fim de proteger os usuários de ataques a sua honra, intimidade e vida privada (BITENCOURT, 2011).

2.3 Crimes virtuais e crimes praticados em ambientes não virtuais

Os crimes virtuais, também conhecidos como crimes cibernéticos ou crimes eletrônicos, são aqueles que são cometidos por meio de dispositivos eletrônicos, como computadores, smartphones e tablets, ou pela internet. Já os crimes praticados em ambientes não virtuais são aqueles que ocorrem em espaços físicos, como ruas, casas, lojas, etc (PINHEIRO, 2013).

Existem várias diferenças entre os crimes virtuais e os crimes praticados em ambientes não virtuais, dentre elas: Velocidade e alcance: Os crimes virtuais podem ser cometidos em questão de segundos e ter um alcance global, enquanto os crimes em ambientes não virtuais geralmente levam mais tempo para serem cometidos e têm um alcance mais limitado.

> - Anonimato: Os criminosos virtuais muitas vezes conseguem se esconder por trás de identidades falsas ou anonimato na internet, o que torna mais difícil identificá-los e responsabilizá-los pelos seus atos. Já nos crimes em ambientes não virtuais, é mais fácil identificar o criminoso pela descrição física ou por meio de testemunhas.
> - Tipo de crime: Os crimes virtuais tendem a envolver fraude, invasão de privacidade, roubo de identidade, assédio virtual, pornografia infantil, entre outros. Já os crimes em ambientes não virtuais podem envolver roubo, agressão física, assassinato, tráfico de drogas, entre outros.
>
> - Prevenção: A prevenção dos crimes virtuais muitas vezes envolve a adoção de medidas de segurança online, como o uso de senhas fortes, a instalação de programas antivírus e a desconfiança de mensagens suspeitas. Já a prevenção dos crimes em ambientes não virtuais muitas vezes envolve a presença policial, iluminação adequada e outras medidas de segurança física.
>
> - Investigação: A investigação dos crimes virtuais pode ser mais complexa do que a investigação dos crimes em ambientes não virtuais, já que muitas vezes envolve tecnologias sofisticadas e conhecimentos específicos. Além disso, pode haver desafios legais em relação à jurisdição e à obtenção de provas (PINHEIRO, 2013).

Exemplos incluem roubo de informações confidenciais, disseminação de vírus e malware, phishing, fraude online, difamação nas redes sociais, entre outros. Por outro lado, os crimes praticados pelos ambientes não virtuais são aqueles que são cometidos sem a utilização da tecnologia da informação e comunicação. Esses crimes podem incluir, por exemplo, homicídio, roubo, furto, agressão física, sequestro, entre outros (SOUZA, 2014).

Embora haja diferenças óbvias entre esses dois tipo de crimes é importante notar que muitos cibercrimes também podem ser enquadrados em categorias de crimes "tradicionais". Por exemplo, o roubo de informações confidenciais pode ser equiparado ao roubo de propriedade física, como dinheiro ou bens pessoais. Da mesma forma, a difamação online pode ser equiparada à difamação "tradicional" por meio de boatos ou cartazes (PINHEIRO, 2013).

Além disso, os crimes virtuais apresentam desafios únicos em termos de investigação e punição. Muitas vezes, é difícil rastrear os responsáveis por cibercrimes, uma vez que eles podem operar anonimamente ou usar técnicas de ocultação de identidade (PINHEIRO, 2013).

Além disso, as leis e regulamentos relacionados à cibercrimes podem variar significativamente entre diferentes países e jurisdições, o que pode tornar a cooperação internacional e a extradição mais complicadas (PINHEIRO, 2013).

CAPÍTULO III – O CRIME DE ESTELIONATO PRATICADO NA INTERNET

No decorrer do presente trabalho restou demonstrado que o crime de estelionato se consuma quando alguém com o intuito de obter vantagem ilícita para si ou para outrem se utilizada de artificio, ardil ou qualquer outro meio fraudulento, para induzir a vítima ou mantê-la em erro, causando-lhe prejuízo. Os crimes virtuais, por seu turno, são aqueles praticados em ambiente virtual, com a utilização de equipamentos eletrônicos e acesso à rede.

De posse dessas informações, pode se entender preliminarmente que o estelionato virtual é aquele em que o indivíduo servindo-se de equipamentos tecnológicos e acesso à rede, pratica em benefício próprio ou de outrem e em prejuízo alheio, o ato de induzir ou manter a vítima em erro, utilizando-se quaisquer meios fraudulentos e almejando vantagem ilícita.

Dessa maneira o presente capitulo procurara traçar algumas considerações acerca do crime de estelionato virtual, propriamente dito, destacando especialmente a ausência de norma especifica que regulamente a espécie e os projetos de lei em tramitação que cuidam da matéria. Para a melhor compreensão do estudo que aqui se realizará, o capitulo será dividido em duas partes, na primeira parte realizará uma análise geral no crime de estelionato virtual no ordenamento jurídico brasileiro. No segundo momento apresentará os projetos de lei acerca da matéria.

A pesquisa aqui realizada será de suma importância para a solução do problema de pesquisa, vez que alicerçada nos estudos realizados nos capítulos anteriores, demonstrará ao longo do texto, se a norma prevista no art. 171, do Código Penal é suficiente para reprimir a prática de estelionato virtual.

3.1. O estelionato virtual

Diante das considerações preliminares, irá nessa primeira parte do capítulo, destacar como o crime de estelionato virtual tem sido tratado no ordenamento jurídico brasileiro, pois como analisado no capitulo inicial o texto do art. 171, do Código Penal não faz qualquer menção à utilização da internet, o que leva muitas pessoas a acreditarem em uma cera impunidade do crime, em razão da ausência de previsão normativa.

Nesse ponto da pesquisa, irá em verdade concluir o raciocínio iniciado nos capítulos anteriores, e a partir daqui, será possível construir uma resposta ao problema de pesquisa apresentado, daí sua importância para a solução deste. Aqui se apresentará informações suficientes para se dizer se a norma regulamentada no art. 171, do Código Penal, é ou não suficiente para reprimir a prática do estelionato virtual. A pesquisa será sustentada em referenciais bibliográficos e legais.

Nas palavras de Ataide (2017) ocorre crime de estelionato virtual quando os infratores criam links, e-mails, etc., falsos, com o objetivo de não ser identificado e consequentemente prometem fazer algo que sabem não ser possível fazer, mas fazem a promessa em troca de alguma vantagem que em grande parte das vezes é pecuniária. Em síntese, o estelionato virtual se consuma com o induzimento da vítima, utilizando-se de meios digitais, aproveitando-se das brechas que esses lhe permitem para conseguir obter vantagens.

Como recorda Freitas (2009) o mundo virtual oferece inúmeras vantagens aos usuários no momento de realizar uma compra. É possível comprar os mais diversos produtos, sem sair de cada, apenas com poucos cliques e a preços mais baixos. Em razão disso comprar pela internet se torna bem conveniente para o comprador, contudo nem sempre isso ocorre.

Nos dias atuais a internet tem proporcionado a simplificação de tarefas, o ato de comprar algo, por exemplo, hoje pode ser executado em poucos cliques e com valores menores, como assevera a autora, contudo a mesma alerta que o espaço não é tão segura como se espera, pois, pessoas mal-intencionadas podem se valer dessas facilidades para causar dano ao próximo.

Uma das formas mais frequentes de estelionato virtual é a invasão do correio eletrônico da vítima, especialmente aquelas que tem o costume de consultar saldos e extratos bancários pelo computador. Nesse caso em especifico, o estelionatário encontra uma maneira de clonar a página da internet banking e fazer com que a vítima tente fazer o acesso a conta, sem saber que os danos inseridos na dita página serão interceptados por um terceiro de má-fé. Outro tipo bem comum é praticado por pessoas de menor saber informático, os quais se utilizam de crenças populares ou correntes de sorte, para que ao final a vítima deposite determinada importância em dinheiro para que obtenha aquilo que foi veiculado, sendo garantido a esta que ao adquirir o almejado a importância lhe será devolvida, fato que não ocorre (FEITOZA, 2012).

Forma típica de estelionato no ciberespaço, é portanto, conforme a citação acima, aquela que se dá quando a pessoa invade o correio eletrônico da vítima, em especial aquelas que costumam consultar saldos e extratos bancários pelo computador. No caso em questão o estelionatário se vale de medidas para clonar a página legitima do usuário e fazê-lo acreditar que se encontra no local correto, e acreditando nisso inserir os dados de acesso.

Outra forma bem comum, como salienta o autor é executado por pessoas de menor conhecimento de informática, e que vêm a se utilizar de corrente de sorte e de crenças populares encaminhando diversos e-mails para as pessoas que tem a possibilidade de serem persuadidas por aquilo, neste momento eles contam uma história breve e pedem depósitos prévios em dinheiro, para que algo lhes seja realizado, além de garantir o reembolso do dinheiro acaso o prometido não ocorra.

Corroborando com o salientado pelo autor, pode-se afirmar, que tem sido cada vez mais recorrente, o encaminhamento de mensagens para os telefones particulares, cujo conteúdo apresenta falsos links de acesso, que em verdade objetivam implantar vírus que darão acesso ao conteúdo de contas no aparelho, provocando prejuízo à vítima que erroneamente caiu no golpe dos infratores e em beneficio para estes.

Não há dúvidas de que possa ocorrer a prática de crime de estelionato em ambiente virtual, através da rede mundial de computadores. Aliás, tem sido bem comum que pessoas sejam vítimas de golpes de estelionatários na internet

(FREITAS, 2009). Percebe-se, pois, que cada vez é mais frequente a prática de estelionato virtual, o que se deve principalmente como já analisado, ao avanço da tecnologia e popularização da internet.

De acordo com Junior (2008) comete crime de estelionato aquele que cria página em ambiente virtual ou faz anúncios em sites, simulando por exemplo, a venda de produtos com o objetivo de induzia a vítima em erro para que essa efetue pagamento antecipado para a compra de produtos, na ilusão de que irá recebe-los posteriormente, quando, em verdade, se trata de um golpe empregado pelo agente para obter vantagem indevida, aproveitando-se da boa-fé de pessoas para enganálas e provocar prejuízo patrimonial a elas.

Nos termos da citação acima, outra hipótese de configuração de crime de estelionato virtual ocorre quando o agente cria páginas na internet ou realiza anúncios em sites diversos, simulando a venda de produtos que de fato não existem, para induzir a vítima a fazer o pagamento antecipado de algo que não chegará a receber, valendo-se da boa-fé dos compradores e acarretando-lhes prejuízo patrimonial.

Na mesma linha lecionam Cruz e Rodrigues (2018) quando falam que o estelionato na internet tem se tornado cada vez mais frequente, um exemplo são os indivíduos que maliciosamente produzem sites de vendas com informações falsas de modo a induzir as vítimas a pagarem por produtos que sequer existem. Como informam os autores tem sido comum, a prática de estelionato no meio digital, e os autores, se utilizam de informações falsas para manipular a vítima e fazê-la acreditar em uma suposta vantagem.

A pratica do crime de estelionato em ambiente virtual é na maioria das vezes praticada por pessoas de notável conhecimento em informática, e que embora possam agir de maneira diversa, preferem se arriscar no mundo dos crimes virtuais, iludindo e prejudicando pessoas reais, de modo a obter alguma vantagem ilícita com essa técnica. A única diferença existente entre o estelionato real e o virtual consiste no modus operandi empregado, tendo em vista que o primeiro se realiza em meio físico e o segundo em ambiente virtual (FEITOZA, 2012).

O estelionato virtual tende a ser praticado por pessoas com mais conhecimentos em informática, como bem ressalta o autor, são pessoas que poderiam utilizar seu conhecimento em outras coisas, mas preferem se arriscar no mundo do crime e prejudicar pessoas normais, com a finalidade de obter algum tipo de vantagem. A única diferença entre o estelionato virtual e o estelionato comum, é o modo pelo qual o agente irá operar, pois o estelionato virtual é realizado em ambiente virtual e o estelionato comum em ambiente físico.

O Código Penal não faz menção ao crime de estelionato virtual em seu texto, a conduta descrita no art. 171 do diploma diz respeito tão somente ao delito praticado diretamente pelo infrator, isto é, obter vantagem ilícita em prejuízo alheio, não importando aqui se isto foi realizado por intermédio do computador ou da internet (FEITOZA, 2012).

Assim como explica o autor, o Estatuto Repressivo, não faz qualquer referência ao crime de estelionato virtual, sendo que a conduta disciplinada pelo art. 171, diz respeito apenas ao estelionato puro e simples, consistente no ato de obter vantagem ilícita, para si ou para outro, em prejuízo alheio, mediante artifício, ardio, ou quaisquer atos fraudulentos, independente da utilização ou não de dispositivos informáticos. Ou seja, em tese os agentes que cometem o crime de estelionato virtual, incidiriam nas penas do art. 171 do Código Penal, já que pouco importam os objetos utilizados para a consecução da vantagem indevida.

O impasse que surge quando da tipificação do crime de estelionato virtual, é a ausência de norma penal especifica. A própria Constituição Federal no art. 5º, inc. XXXIX firma o princípio da legalidade, pelo qual não a crime sem lei anterior que venha para defini-lo, nem pena sem prévia previsão legal. A natureza jurídica desse dispositivo acaba por limitar a pretensão punitiva do estado, por inexistir tipificação expressa para o crime de estelionato virtual, em alguns casos seus adeptos são absolvidos devido a esta brecha deixada pelo Código Penal que datado de 1940 é antiquado para os dias atuais (FEITOZA, 2012).

Como verbera Feitoza (2012) a figura do estelionato virtual ainda é algo recente dentro do estado e dos tribunais brasileiros, contudo, merece atenção especial com a popularização e modernização da internet, que tem atingido e adquirido milhares de novos usuários todos os dias. Nessa perspectiva, 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.

Completam Cruz e Rodrigues (2018) que são muitas as dificuldades do Ministério Público, da Polícia e do Poder Judiciário para punir os agentes que praticam os cybercrimes, estas dificuldades tendem a levar a uma sensação de impunidade, e as pessoas acabam a relacionar essa tal impunidade à inexistência de leis especificas que cuidem dos crimes cibernéticos.

Segundo Feitoza (2012) a ausência de legislação especifica acerca do tema acaba por induzir os criminosos a praticarem a infração, pois confiam na impunidade devido a falta do instrumento normativo especifico. São diversos os problemas que envolvem o estelionato virtual, dentre eles se destacam: a dificuldade na identificação dos autores do fato, a delimitação do local do crime e o juízo competente.

Ratifica o autor que a ausência de legislação especifica para o crime de estelionato virtual, acaba por induzir as pessoas a acreditarem que não haverá punição daqueles que cometerem o fato. Mas a ausência de norma reguladora não é o único problema inerente ao crime de estelionato virtual, há também dificuldades na localização do autor do crime, delimitação do local e competência para julgamento do delito.

Isto posto, por inexistir norma especifica que trate do crime de estelionato virtual, a população tende a ter uma certa sensação de impunidade, no entanto as dificuldades de punir os agentes infratores, vai além da inexistência de normas especificas, mas abrange também, as facilidades proporcionadas pela rede, onde o agente pode com facilidade alterar ou apagar dados, e até mesmo se usar de endereços de e-mail e perfis falsos que podem impedir sua correta identificação, até porque podem agir nos mais variados locais e com os mais variados dispositivos eletrônicos.

Como pronuncia Cruz e Rodrigues (2018) o art. 1º do Código Penal Brasileiro, prescreve que não há crime sem lei anterior que o defina e também não há pena sem previa previsão legal. O supradito dispositivo é bem consistente na

conceituação de crime, que de maneira clara é o ato praticado em desconformidade com as normas estabelecidas em lei, de forma que inexistindo norma que vede a prática do ato.

Ratificando as disposições consolidadas na Constituição Federal de 1988, prescrevem os autores, que o art. 1º do Código Penal, traz que não há crime sem lei anterior que o discipline, assim como não há pena sem prévia previsão legal. Destarte o crime é a violação de uma norma pré-fixada, de forma, que inexistindo a norma, não se pode falar em crimes.

Diferentemente do que muitas pessoas creem os crimes praticados por meio da internet possuem tipificação legal e quando se consegue identificar os autores do delito há a sanção penal. O que faz com que as pessoas acreditem na impunidade do fato é a ausência de previsão legal especifica que contenha no seu texto a palavra “internet”. Muito embora o preambulo 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 e RODRIGUES, 2018).

No entanto, conforme concluem os autores, ao contrário do que muitos acreditam os crimes cometidos com a utilização da internet possuem tipificação e sempre que identificados os sujeitos ativos do crime, eles são submetidos a sanção penal. O que os faz acreditar em impunidade diz respeito a falta expressa da palavra internet, mas independente dos meios utilizados, se o sujeito vier a praticar as atividades características do crime de estelionato, previstas no art. 171, irá incidir nas penas previstas para este.

Verbera Ataide (2017) que mesmo com toda omissão no ordenamento jurídico brasileiro e de todas as precariedades que norteiam o sistema, os crimes virtuais praticados no Brasil, são punidos, pois muito embora, não esteja especificado a utilização de internet para a prática do ato, as condutas base estão previstas no Código Penal, o que vem a facilitar a aplicação da lei. Entretanto, necessário entender que para que se venha a punir adequadamente aqueles que cometem crimes virtuais, é necessária uma adequação da norma existente, preenchendo as lacunas que devem ser preenchidas.

Em suma, o crime de estelionato virtual, não possui legislação especifica que o tutele, e os agentes que praticarem o fato, irão incidir nas penas do art. 171, do Código Penal, que trata do crime de estelionato. Contudo, restou evidenciado que os problemas decorrentes da ausência da norma não dizem respeito a tipificação do delito, mas a problemas com a localização do infrator, local do crime e competência, fatos que tornam a norma vigente, insuficiente quando se trata do crime de estelionato virtual especificadamente e levam a uma sensação de impunidade.

Feitas essas considerações, e sabendo que inexiste até o momento norma que preveja expressamente como crime o estelionato virtual, irá no item a seguir apresentar os projetos de lei em tramitação, que cuidam de forma especifica do delito em questão.

3.2. Legislação sobre o tema

É notório que a evolução da internet é constante e a legislação brasileira deve acompanhar esse ritmo, a fim de regular as garantias e os direitos constitucionais, que acompanham esse avanço tecnológico.

Contudo, mesmo diante das mais diversas e reiteradas formas de praticar o cibercrime, o que se teve inicialmente foi adaptações nos meios digitais, com a criação e uso de senhas e softwares para proteger os usuários de possíveis condutas criminosas no ambiente digital, para só depois se avançar na criação de uma legislação específica.

Assim, como inclusive já destacado, em razão da ausência de uma lei própria para os crimes virtuais, os magistrados, nos casos concretos, se utilizavam do próprio Código Penal para a tipificação, o que dava margem a decisões contraditórias (PAGANOTTI, 2013).

Em decorrência de alguns episódios em meados de 2011, ocorrendo vários ataques na navegação de serviços nos sites do governo brasileiro que ficaram instáveis até saírem do ar, bem como, nos inúmeros outros casos de atos criminosos no âmbito virtual, foi apresentado um novo projeto de lei, em 29 de novembro de 2011 na Câmara dos Deputados.

Esse projeto era de autoria dos Deputados Federais Paulo Teixeira, Luiza Erundina, Manuela D'Ávila, João Arruda, Brizola Neto e Emiliano José, e visava a necessidade de criar uma legislação que regulamentasse de forma mais especifica o uso "criminoso" dos meios cibernéticos, dispondo o seguinte:

> São inegáveis os avanços para a sociedade decorrente do uso da Internet e das novas tecnologias. Estes avanços trazem a necessidade da regulamentação de aspectos relativos à sociedade da informação, com o intuito de assegurar os direitos dos cidadãos e garantir que a utilização destas tecnologias possa ser potencializada em seus efeitos positivos e minimizada em seus impactos negativos. (BRASIL, 2011).

Os autores defendiam que as antigas propostas de criminalização, trazidas por outros projetos, eram muito abertas e desproporcionais, não sendo capazes de aplicar a tipificação criminal de condutas corriqueiras praticadas pelos usuários da internet, bem como, tipificavam matérias como o armazenamento e acesso a registros de conexão, que deveriam estar inseridos em diretrizes mais abrangentes e atentas aos direitos dos cidadãos (BRASIL, 2011).

Assim, o Projeto de Lei nº 2.793 de 2011, apresentou algumas diferenças em relação ao Projeto nº 84/99 (Lei Azeredo) já abordado anteriormente, tais como: trata-se apenas de tipificações penais e apresenta um número significativo menor de tipos penais, veja-se:

> [...] não se abordam as questões relativas a guarda e fornecimento de registros, ou demais obrigações imputáveis a provedores de serviços de internet - questões que encontram lugar mais adequado numa regulamentação civil sobre a matéria. (BRASIL, 2011, D).
>
> [...] Norteamo-nos, nesta escolha, pela compreensão de que grande parte das condutas relativas praticadas por meios eletrônicos já se encontra passível de punição pelo ordenamento jurídico pátrio. Ainda, pautamo-nos pela visão de que não é a proliferação de tipos penais que levará à maior repressão de condutas. (BRASIL, 2011).

Desse modo, a PL buscou excluir as condutas que não eram claras e precisas e, visava uma forma de equilibrar as penas de acordo com a gravidade das condutas e ainda estabelecer uma harmonia com as penas já existentes no Código Penal, bem como, pretendia evitar a expansão desnecessária para novas searas penais (BRASIL, 2011).

Portanto, a sua aprovação seria uma forma de preencher as lacunas presentes na legislação brasileira atual sobre a temática, com o intuito de tentar acompanhar a expansão constante da tecnologia e combater as condutas criminosas praticadas no âmbito digital.

Em 07 de novembro de 2012 foi aprovado o Projeto de Lei, nº 2.793 de 2011, que passou a ser conhecida como “Lei Carolina Dieckmann”, a Lei nº 12.737 de 30 de novembro de 2012, entrando em vigor apenas no dia 02 de abril de 2013. A promulgação da Lei 12.737/12 e a sua rápida tramitação se deu por conta de um caso de repercussão nacional, envolvendo a atriz brasileira Carolina Dieckmann.

Os portais de notícias e as redes sociais contribuíram para a ampla disseminação desse caso, alcançando um enorme número de pessoas em todo o país e de forma célere. A atriz teve seu computador invadido por criminosos, os chamados crakers, após receber um e-mail que julgava ser confiável. Assim, os criminosos tiveram acesso a fotos intimas de Carolina, passando a chantageá-la, exigindo R$ 10.000,00 (dez mil reais) para não divulgar as imagens.

A atriz recebeu inúmeras ligações e mensagens, ameaçando-a sobre a divulgação, mas não cederam as chantagens e registrou boletim de ocorrência na delegacia Contudo, a operação montada pela polícia para prender os agentes em flagrante restou frustrada e, segundo o site de notícias do Globo (G1) (http://www.g1.globo.com), “ao todo, 36 imagens intimas da atriz foram pulicadas na web em maio de 2012”.

Diante de toda repercussão do caso, através da mídia e da internet, bem como do medo e insegurança que tal fato gerou aos indivíduos, que se sentiram vulneráveis e suscetíveis a passar pelas mesmas situações, o Congresso Nacional foi pressionado a criar e publicar uma lei específica para os crimes cibernéticos.

Assim, o Congresso, para acalmar o clamor popular da época, no intuito de demonstrar uma rápida resposta para o problema em questão, aprovou o Projeto de Lei 2.793/11, criando a lei 12.737/2012 que passou a ser denominada como Lei Carolina Dieckmann.

A inovação legislativa trazida pela Lei 12.737/2012, introduziu no Código Penal brasileiro o tipo nominado “Invasão de dispositivo informático”, acrescentando

os artigos 154-A, e 154-B, e ainda alterou o texto dos artigos 266 e 298, inserindo os crimes praticados via meios informáticos na legislação penal. Assim o texto legal possui a seguinte redação.

Dessa forma, foi incorporado ao ordenamento jurídico brasileiro, a previsão de crime de invasão de dispositivo alheio, sem motivo ou sem o consentimento do dono, com penalidade de 3 meses a um ano, e com causa de aumento, caso tal invasão causasse prejuízos econômicos à vítima, ou caso se trata-se da administração pública no polo passivo.

O bem jurídico tutelado referia-se à violação da liberdade do usuário do dispositivo informático, através de outro dispositivo informático (NUCCI, 2014). É crime comum, o qual pode ser praticado por qualquer pessoa, não se exigindo uma qualidade ou condição especial do agente para ser sujeito ativo, ou seja, não necessita que o invasor seja um especialista, conhecido como hacker (JUNIOR, 2013, NUCCI, 2014).

Ademais, o sujeito passivo também pode ser qualquer pessoa que seja responsável pelo bem jurídico que foi violado (NUCCI, 2014) seja ele o proprietário ou detentor do bem, como nos casos de equipamentos fornecidos por empresas aos seus funcionários (PRADO, 2013).

Para sua caracterização é fundamental o dolo (não cabendo, portanto, a forma culposa) e o especial fim de agir que é “a obtenção, a adulteração ou a destruição de dados ou informações, também a obtenção de vantagem ilícita” (REIS, 2014). No entanto, no ano de 2021, a Lei sofreu alterações, mais especificamente pela Lei 14.555/2021, a qual será abordada posteriormente no presente trabalho.

3.2.1. Lei geral de proteção de dados

A Lei Geral de Proteção de Dados (Lei n.º 13.709/2018) foi sancionada em 2018 e entrou em vigor apenas no ano de 2020.

Foi inspirada pela GDPR (General Data Protection Regulation) da União Europeia, e tem como objetivo “proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.” (Brasil, 2020, online).

Essa lei pretende estabelecer uma segurança jurídica, através de uma regulamentação e condutas para proteger dados pessoais de todos os indivíduos que estejam em território brasileiro, observando os preceitos existentes internacionais.

Para Somadossi:

> A LGPD cria uma regulamentação para o uso, proteção e transferência de dados pessoais no Brasil, nos âmbitos privado e público, e estabelece de modo claro quem são as figuras envolvidas e quais são suas atribuições, responsabilidades e penalidades no âmbito civil – que podem chegar a multa de 50 milhões de reais por incidente. (SOMADOSSI, Henrique. 2018, online).

A lei, portanto, cria uma regulamentação referente a proteção de dados, definindo o que são os dados pessoais, estabelecendo, ainda, quais são os dados sensíveis e os de maior proteção, sendo estes os relacionados a crianças e adolescentes.

A fiscalização e aplicação de penalidades quanto ao descumprimento da LGPD, é feita pela Autoridade Nacional de Proteção de Dados Pessoais, a ANPD, sendo necessário também agentes de tratamento de dados, os quais tem suas funções estipuladas pela própria Lei de Proteção de Dados (Brasil, 2020, online).

3.2.2. Lei de stalking

No dia 31 de março de 2021 foi sancionada a lei 14.132/21, conhecida como Lei de Stalking, uma importante inovação legislativa que incluiu o artigo 147-A no Código Penal, criminalizando a conduta de perseguição, em inglês stalking. Vejase:

> Art. 147-A. Perseguir alguém, reiteradamente e por qualquer meio, ameaçando-lhe a integridade física ou psicológica, restringindo-lhe a capacidade de locomoção ou, de qualquer forma, invadindo ou perturbando sua esfera de liberdade ou privacidade. Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa.
>
> § 1º A pena é aumentada de metade se o crime é cometido:
>
> I - contra criança, adolescente ou idoso;
>
> II - contra mulher por razões da condição de sexo feminino, nos termos do § 2º-A do art. 121 deste Código;
>
> III - mediante concurso de 2 (duas) ou mais pessoas ou com o emprego de arma.

> § 2º As penas deste artigo são aplicáveis sem prejuízo das correspondentes à violência.
>
> § 3º Somente se procede mediante representação." (BRASIL, 2021).

Conforme prelaciona Castro e Sydrow (2017) “stalking é uma palavra inglesa aplicada a quem importuna de forma insistente e obsessiva uma outra pessoa, ou seja, a atitude de espionar e perseguir um individuo de forma constante é denominada de stalking”.

Nesse sentido, os autores acrescentam: "trata-se de curso de conduta de importunação, caracterizado pela insistência, impertinência e habitualidade, desenvolvido por qualquer meio de contato, vigilância, perseguição ou assédio."

O delito possibilita que a perseguição também ocorra no meio digital, geralmente com o uso das redes sociais, passando a ser denominado como cyberstalking.

Neste sentido, o projeto de Lei que visa a criminalização dessas condutas foi apresentado pela Senadora Leila Barros, em novembro de 2019, sob a narrativa de que:

> O avanço das tecnologias e o uso em massa das redes sociais trouxeram novas formas de crimes, sendo necessário o aperfeiçoamento do Código Penal para dar mais segurança às vítimas de um crime que muitas vezes começa on-line e migra para perseguição física” (BRASIL, 2021).

O projeto então foi sancionado pelo ex-Presidente Jair Bolsonaro em março de 2021, entrando em vigor no dia 1º de abril do mesmo ano.

Antes, essa conduta era enquadrada apenas como contravenção penal (o (Artigo 65 da Lei de Contravenções Penais - Decreto-Lei 3.688, de 1941), a qual foi revogada e previa como perturbação da tranquilidade alheia, punível com prisão de 15 dias a 2 meses e multa.

Ressalta-se que, a perseguição para ser criminalmente relevante, exige reiteração, de modo a consistir, posteriormente em outro delito, tal como constrangimento ilegal ou ameaça, prejudicando a integridade física ou psicológica

da vítima, abalando seu estado emocional e gerando receio ou intranquilidade (BARRETOS, 2021).

Conforme Castro e Sydow (2017) “trata-se, portanto, de um crime habitual, em razão da exigência de atos reiterados para consumação. Assim, uma conduta isolada do agente não é capaz de configurar o crime, razão pela qual, não se admite a tentativa”.

Ademais, pode ser cometido por qualquer pessoa, seja homens ou mulheres, prevendo a legislação aumento de pena em metade, se caso ocorre com o concurso de agentes ou no caso de uso de armas.

Também terá pena aumentada em 50% quando for praticado contra criança, adolescente, idoso ou contra mulher por razões de gênero.

A forma de consumação pode ser vinculada, uma vez que, o próprio tipo penal prevê “ameaçando-lhe a integridade física ou psicológica, restringindo-lhe a capacidade de locomoção ou, de qualquer forma, invadindo ou perturbando sua esfera de liberdade ou privacidade” (BRASIL, 2021).

Destarte, “a perseguição reiterada na internet, ameaçando a integridade física e psicológica de alguém, interferindo na liberdade e na privacidade da vítima, configuram cyberstalking” (BRASIL, 2021).

Salienta-se que, as penas desse crime, não afastam as penas correspondentes à violência, o que gera maior proteção às vítimas e proporciona uma aplicação mais integral da lei penal (BARRETOS, 2021).

3.3. Competência para julgamento

A Lei n°14.155/2021 também alterou o artigo 70 do Código de Processo Penal, tratando da competência para o julgamento de algumas das modalidades do crime de estelionato. O §4° do referido artigo foi incluído com a seguinte redação:

> § 4º Nos crimes previstos no art. 171 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), quando praticados mediante depósito, mediante emissão de cheques sem suficiente provisão de fundos em poder do sacado ou com o pagamento frustrado ou mediante transferência de valores, a competência será definida pelo local do domicílio da vítima, e, em caso de pluralidade de vítimas, a competência firmar-se-á pela prevenção (BRASIL, 2021).

Dessa forma, o critério para estabelecer a competência passa ser o domicílio da vítima, sendo a competência determinada pela prevenção em caso de pluralidade de vítimas. Entretanto, quando se tratar de estelionato mediante falsificação de cheque, a competência para processamento e julgamento do crime será do juízo do local da obtenção da vantagem ilícita, conforme prevê a sumula 48 do STJ.

CONCLUSÃO

O estelionato é um crime praticado contra o patrimônio de pessoas determinadas, no qual o infrator busca obter para si ou para outrem, vantagem ilícita, induzindo ou mantendo alguém em erro. Sendo reprimido no Brasil por meio do artigo 171 do Decreto-Lei nº 2.484 de 07 de dezembro de 1940, o Código Penal Brasileiro.

Contudo a sociedade está em constante evolução, se fazendo sempre necessário que o Estado esteja acompanhado de forma a garantir que os frutos por ela conquistados sejam protegidos e preservados contra as ações de indivíduos que buscam se beneficiarem ilicitamente destes, através do crime.

E com a criação da Informática e o surgimento da Internet, os crimes se manifestaram, e se propagaram no meio virtual, sendo inevitável à ação do Estado protetor da sociedade, na busca de meios eficazes no combate aos crimes virtuais.

Entre os crimes virtuais, temos o crime de estelionato que também passou a ser praticado na Internet, dificultando às autoridades competentes em proceder nas devidas punições dos infratores virtuais.

As dificuldades, enfrentadas pelas autoridades, se referem à descoberta da autoria, a confirmação da competência estatal punitiva, a existência de provas da ocorrência do crime, a necessidade de perícia criminal especializada para confirmar o crime, e a dificuldade oriunda da manipulação de Protocolo de Internet pelos infratores, que camufla a base operacional do infrator, ou seja, a identificação do computador utilizado pelo estelionatário.

E, nesse sentido que se faz necessário, a atuação do Estado brasileiro, de levar maior seriedade e celeridade às propostas e aprovações de projetos de lei contra o crime de estelionato eletrônico, suprindo esta necessidade de tipificação do crime de estelionato praticado na Internet, visando disciplinar de

maneira mais clara e precisa sua conduta criminosa, bem como trazer meios punitivos mais eficazes no seu combate.

E assim, este trabalho alcança seu objetivo, trazendo um breve estudo que demonstre ser necessária a tipificação do crime de estelionato eletrônico, com inserção de penas mais severas aos infratores.

Objetivando ainda, contribuir com os estudantes e pesquisares de direito para o avanço do conhecimento na área de direito penal no Brasil, especificamente em criminologia eletrônica, servindo de fonte de pesquisa e material incentivador na realização de novas e outras pesquisas a cerca desta instigante matéria, tendo em vista a evolução social e a busca da melhor proteção de seus frutos pelo Estado brasileiro.

E, por limitação de tempo, não adentrou-se na esfera de necessidade de tipificação aos demais crimes eletrônicos, bem como na repercussão em nível de direito internacional. Acreditando que estudiosos e pesquisadores do direito penal, incentivados por este trabalho, possam assim contribuir.

REFERÊNCIAS

ARAS, Vladmir. **Crimes de Informática**: uma nova criminalidade. Revista Eletrônica Jus Navigandi. Publicado em 01 out 2001. Disponível em: Acesso em: 09 mar 2023.

ATAÍDE, Amanda Albuquerque de. **Crimes Virtuais**: uma análise da impunidade e dos danos causados às vítimas. Maceió, 2017. Disponível em: http://www.faaiesa.edu.br/aluno/arquivos/tcc/tcc_amanda_ataide.pdf. Acesso em: 20 abr. 2023.

ALMEIDA, Fernando Pedroso. **Direito penal**: parte geral: **doutrina** e jurisprudência. 5. ed. Leme, SP: JH Mizuno, 2013.

BITENCOURT, Cezar Roberto. **Tratado de direito penal**: parte geral. 20 ed. São Paulo: Saraiva, 2014. v. 1.

BRASIL. **Código Penal Brasileiro.** Organização dos textos, notas remissivas e índices por Juarez de Oliveira. 46. ed. São Paulo: Saraiva, 2022.

BRASIL. **Constituição da República Federativa do Brasil**. Brasília-DF, Congresso Nacional, 1988.

BRASIL. **Crimes cibernéticos / 2ª Câmara de Coordenação e Revisão, Criminal**. – Brasília-DF: MPF, 2018.

BRASIL. **Decreto-lei nº 3.689**, de 3 de outubro de 1941**.**Código de Processo Penal. Rio de Janeiro-RJ, Congresso Nacional, 1941.

BRASIL. **Lei 9.099, de 26 de setembro de 1995**. Dispõe sobre os Juizados Especiais Cíveis e Criminais. Diário Oficial da República Federativa do Brasil. Brasília, DF, 27 set. 1995.

BRASIL. **Lei n. 12.737, de 30 de novembro de 2012**. Brasília-DF, Congresso Nacional, 2012.

BRASIL. **Lei nº 8.069**, **de 13 de julho de 1990.** Estatuto da Criança e do Adolescente. Brasília-DF, Congresso Nacional, 1990.

BRASIL. **Lei nº 8.072, de 25 de julho de 1990**. Lei dos Crimes Hediondos. Brasília-DF, Congresso Nacional, 1990.

BRASIL. **Lei nº 12.965**, **de 23 de abril de 2014**. Brasília-DF, Congresso Nacional, 2014

BRASIL. Ministério Público Federal. Câmara de Coordenação e Revisão, 2. **Crimes cibernéticos** / 2ª Câmara de Coordenação e Revisão, Criminal. – Brasília : MPF, 2018.

BRASIL. **DECRETO-LEI Nº 3.689, DE 3 DE OUTUBRO DE 1941.**Código de Processo Penal, Rio de Janeiro-DF, Congresso Nacional, 1941.

BRASIL. **DECRETO-LEI Nº 2.848, DE 7 DE DEZEMBRO DE 1940.** Código Penal. Rio de Janeiro-DF, Congresso Nacional, 1941.

CABETTE, Eduardo L. S. **O novo crime de Invasão de Dispositivo Informático**. Consultor Jurídico. Artigo publicado em 4 de fev 2013.

CARNEIRO, Adeneele Garcia. **Crimes virtuais: elementos para uma reflexão sobre o problema na tipificação**. Âmbito Jurídico, Rio Grande, XV, n.99, abr. 2012. Disponível em:. Acesso em: 01 mar. 2018.

CASTRO, Ana Lara; SYDOW, Spencer. **Stalking e Cyberstalking**: obsessão, internet, amedrontamento. Belo Horizonte: D' Plácido, 2017.

CASTRO, Carla Rodrigues Araújo de. **Crimes de Informática e seus Aspectos Processuais**. 2. Ed. Rio de Janeiro: Lumen Juris, 2003.

COLARES, Rodrigo Guimarães. **Cybercrimes: os crimes na era da informática**, 2002. In: Jus Navigandi, Teresina, ano 6, n. 59, out. 2002. Disponível em: http://jus2.uol.com.br/doutrina. Acesso em: 06 mar 2023.

COLLI, Maciel. **Cibercrimes: limites e perspectivas à investigação policial de crimes cibernéticos**. Curitiba: Juruá, 2010.

CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. São Paulo: Saraiva, 2011.

CRUZ, Diego; RODRIGUES, Juliana. **Crimes Cibernéticos e a Falsa Sensação de Impunidade.** 2018. Disponível em: http://faef.revista.inf.br/imagens_arquivos/arquivos_destaque/iegWxiOtVJB1t5C_2019-2-28-16-36-0.pdf. Acesso em: 10 mai. 2023.

Disponível em: https://www.conjur.com.br/2013-fev-04/eduardo-cabette-crime-invasao- dispositivo-informatico . Acesso em: 09 mar 2023.

FEITOZA, luis Guilherme de Matos. **Crimes Cibernéticos**: o Estelionato Virtual. Brasília, 2012. Disponível em: https://egov.ufsc.br/portal/sites/default/files/crimes_ciberneticos_o_estelionato_virtual.pdf. Acesso em: 10 mai. 2023.

FERREIRA, Ivete Senise. **A criminalidade informática**. In: LUCCA, Newton.; SIMÃO FILHO, Adalberto (Coord.). Direito e internet. Bauru: Edipro, 2001.

FREITAS, Riany Alves de. **Segurança Estelionato Digital**. 2009. Disponível em: https://aplicacao.mpmg.mp.br/xmlui/bitstream/handle/123456789/502/Estelionato%20digital.pdf?sequence=3. Acesso em: 10 mai. 2023.

HUNGRIA, Nélson. **Comentários ao Código Penal**. 4º ed. v. 7. arts. 155 a 196. Ed. Forense. 1980, p. 208-209.

MARQUES, Samuel. **Estelionato: Prática comum ao longo da história**. Panorama Empresarial. Resende. Setembro de 2009.

MIRABETE, Júlio Fabbrini. **Código penal interpretado**. 4. ed. São Paulo: Atlas, 2003.

MIRABETE, Julio Fabbrini. **Manual de direito penal**. 16 eds. Vol. 1. São Paulo: Atlas, 2000, p. 292- 295.

NUCCI, Guilherme de Souza. **Manual de Direito Penal**. 13. ed. Rio de Janeiro: Forense, 2017. 1254 p.

PARODI, Lorenzo. **Manual das fraudes**. 2.ed. Rio de Janeiro: Brasport: 2008. Disponível em: http://books.google.com.br/books?id=0lGTAkLxt0AC&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false. Acesso em: 30 out. 2022.

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

PRADO, Luiz R. **Curso de Direito Penal brasileiro**: parte especial, 5 ed. São Paulo, Revista dos Tribunais, 2006, p.273.

RAMOS JÚNIOR, Hélio Santiago Ramos. **Estudo sobre a aplicabilidade das leis penais aos crimes informáticos no Brasil**. In: Proceedings of the Third International Confeerence of Forensic Computer Science. Rio de Janeiro: ABEAT, 2008.

REIS, Wanderlei José dos. **Delitos cibernéticos**: implicações da Lei 12.737/12. Revista Jus Navigandi, Teresina, ano 19, n. 4007, 21 jun. 2014. Disponível em: https://jus.com.br/artigos/29647/delitos-ciberneticos-implicacoes-da-lei-12-737-12.

SILVA, Jorge Vicente. **Estelionato e outras fraudes**. Curitiba: Juruá, 1995, p. 55.

SOMADOSSI, Henrique. **O que muda com a Lei Geral de Proteção de Dados (LGPD).** Disponível em: https://www.migalhas.com.br/dePeso/16,MI286235,31047/O+que+muda+com+a+Lei+Geral+de+Protec ao+de+Dados+LGPD.

TEIXEIRA, Tarcisio. **Curso de direito e processo eletrônico**: doutrina, jurisprudência e prática. São Paulo: Saraiva, 2014.

VIANA, Tulio; MACHADO, Felipe. **Crimes informáticos**. Belo Horizonte: Fórum, 2013

WENDT, Emerson.; JORGE, Higor Vinicius Nogueira. **Crimes cibernéticos**: ameaças e procedimentos de investigação. Rio de Janeiro-RJ: Brasport, 2012.