

**FACULDADE EVANGÉLICA DE RUBIATABA
CURSO DE DIREITO
HESROM CÉSAR DE OLIVEIRA**

CYBERCRIMES: DO ESTELIONATO VIRTUAL

**RUBIATABA/GO
2020**

HESROM CÉSAR DE OLIVEIRA

CYBERCRIMES: DO ESTELIONATO VIRTUAL

Monografia apresentada como requisito parcial à conclusão do curso de Direito da Faculdade Evangélica de Rubiataba, sob orientação do professor Lincoln Martins.

**RUBIATABA/GO
2020**

HESROM CÉSAR DE OLIVEIRA

CYBERCRIMES: DO ESTELIONATO VIRTUAL

Monografia apresentada como requisito parcial à conclusão do curso de Direito da Faculdade Evangélica de Rubiataba, sob orientação do professor Lincoln Martins.

MONOGRAFIA APROVADA PELA BANCA EXAMINADORA EM __ / __ / ____

Especialista Lincoln Deivid Martins
Orientador
Professor da Faculdade Evangélica de Rubiataba

Mestre Edilson Rodrigues
Examinador
Professor da Faculdade Evangélica de Rubiataba

Especialista Fernando Hebert Oliveira
Examinador
Professor da Faculdade Evangélica de Rubiataba

AGRADECIMENTOS

Agradeço a Deus pela graça em minha vida, pelo amor supremo que tem comigo, que tem sido meu refúgio em cada detalhe.

Agradeço aos meus pais, que sem medir esforços, tem me dado as condições necessárias de nunca desistir dos meus objetivos.

Agradeço a minha irmã, que mesmo indiretamente, contribuiu na realização deste.

Muito obrigado a minha namorada, que compartilhou comigo esse momento, pelas palavras de incentivo, apoio e ainda mais, pelos momentos de alegria que me proporciona.

Agradeço os meus amigos, que torcem pelo meu sucesso e que me acompanharam nessa trajetória, na qual não é necessário citá-los, pois sabem de quais estou falando.

Sou grato ao meu orientador, pelo suporte e pelas opiniões e disposição na correção do trabalho, e ainda mais por estimular minha capacidade de escrita.

Agradeço a esta Instituição, ao corpo docente por cada conhecimento repassado. Aos representantes das escolas participantes envolvidas, pelo espaço e oportunidade da realização deste trabalho.

Enfim, tenho muito que agradecer a cada um de vocês, que Deus abençoe a todos pela contribuição na minha carreira. Um forte abraço e muito obrigado!

“De certa forma, foi pela mágica que descobri como é bom enganar as pessoas” (Kevin Mitnick)

RESUMO

É certo que os avanços da tecnologia levaram à facilitação de tarefas, bem como a uma maior conexão entre as pessoas, contudo, na mesma velocidade, tem sido palco de pessoas mal-intencionadas que se usam dessas facilidades para em benefício seu ou de outrem, causar dano alheio, o que convencionalmente se ousou chamar de cybercrimes. Na pesquisa em questão se propôs a estudar um crime cibernético em especial, o estelionato virtual. Para abordagem, se definiu como objetivo geral, verificar se a ausência de legislação específica que trate de modo específico do estelionato virtual pode desencadear a falta de aplicação de penalidades aos infratores, e como objetivos específicos: entender o que se trata o crime de estelionato; verificar o que são os cybercrimes e como são tratados pelo ordenamento jurídico brasileiro; e, estudar o crime de estelionato virtual, com considerações acerca dos projetos de lei que visavam tratar sobre o assunto. Para o atingimento dos objetivos o autor se utilizou de doutrinas, artigos, disposições contidas no Código Penal Brasileiro, na Lei nº 12.737, na Constituição Federal e demais documentos normativos pertinentes, jurisprudências do Supremo Tribunal Federal e Superior Tribunal de Justiça, bem como em outras fontes de pesquisa encontradas na internet. Concluída a pesquisa, constatou-se que o crime de estelionato virtual é aquele em que o autor do crime, para obter vantagem ilícita em benefício seu ou de outrem, induz ou mantém a vítima em erro, causando-lhe prejuízo, por meio de artifício, ardio ou outro meio fraudulento. Não há no ordenamento jurídico brasileiro instrumento normativo que trata especificadamente do crime de estelionato virtual, sendo aplicado aos infratores as disposições gerais contidas no art.171, do Código Penal, que por sua vez tipifica o crime de estelionato. Embora existissem três projetos de lei que buscassem tratar sobre o assunto, nenhum prosperou.

Palavras-chave: Estelionato. Internet. Vantagem. Virtual.

ABSTRACT

It is true that advances in technology have led to the facilitation of tasks, as well as to a greater connection between people, however, at the same speed, it has been the stage for ill-intentioned people who use these facilities to benefit themselves or others, causing damage from others, what conventionally dared to call cybercrimes. In the research in question, he proposed to study a cyber crime in particular, the virtual fraud. As an approach, it was defined as a general objective, to verify if the absence of specific legislation that deals specifically with the virtual fraud can trigger the lack of application of penalties to offenders, and as specific objectives: to understand what the crime of fraud is; verify what cybercrimes are and how they are treated by the Brazilian legal system; and, studying the crime of virtual fraud, with considerations about the bills that aimed to deal with the subject. To achieve the objectives, the author used doctrines, articles, provisions contained in the Brazilian Penal Code, Law No. 12,737, the Federal Constitution and other pertinent normative documents, jurisprudence of the Supreme Federal Court and Superior Court of Justice, as well as in other research sources found on the internet. Upon completion of the research, it was found that the crime of virtual fraud is one in which the perpetrator of the crime, in order to obtain an illicit advantage for the benefit of himself or others, induces or keeps the victim in error, causing damage, by means of artifice. , ardio or other fraudulent means. There is no normative instrument in the Brazilian legal system that specifically deals with the crime of virtual fraud, with the general provisions contained in Article 171 of the Penal Code being applied to offenders, which in turn typifies the crime of fraud. Although there were three bills that sought to address the issue, none prospered.

Keywords: Embezzlement. Internet. Advantage. Virtual.

LISTA DE QUADROS

QUADRO 1 – PERIGO NA REDE: Páginas na internet denunciadas no Brasil.

QUADRO 2 – Número de atendimentos por tópico da conversa em 2019.

LISTA DE ABREVIATURAS E SIGLAS

| | |
|------|--------------------------|
| Art. | Artigo |
| Cap. | Capítulo |
| Inc. | Inciso |
| N. | Número |
| P. | Página |
| PLC | Projeto de Lei da Câmara |
| PLS | Projeto de Lei do Senado |
| STF | Supremo Tribunal Federal |

LISTA DE SÍMBOLOS

§ - Parágrafo

SUMÁRIO

| | |
|--|----|
| 1. INTRODUÇÃO | 11 |
| 2. DISPOSIÇÕES GERIAIS ACERCA DO CRIME DE ESTELIONATO..... | 13 |
| 3 DOS CYBERCRIMES: UMA OBSERVAÇÃO ACERCA DOS CRIMES COMETIDOS NA INTERNET | 22 |
| 4 DO CRIME DE ESTELIONATO VIRTUAL | 32 |
| 4.1 DO CRIME DE ESTELIONATO VIRTUAL NO ORDENAMENTO JURIDICO BRASILEIRO | 32 |
| 4.2 DOS PROJETOS DE LEI SOBRE O TEMA..... | 40 |
| 5 CONSIDERAÇÕES FINAIS | 42 |

1. INTRODUÇÃO

Os avanços tecnológicos na medida que auxiliam na prática de atividades laborais de modo mais rápido e eficiente pela sociedade moderna, bem como no lazer e entretenimento dos indivíduos, acaba por facilitar a ação de indivíduos mal-intencionados, que procuram obter vantagens ilícitas em prejuízo de outrem por meio de indução ou manutenção deste em erro.

Sabendo disso, a abordagem do tema é importante em razão da prática frequente de estelionato nos meios digitais, e que justamente por isso tem sido um obstáculo para a atuação das autoridades policiais, principalmente no que se refere a identificação do autor do crime, o que leva muitos à sensação de impunidade, fato que amplia o interesse pelos cybercrimes.

Face o tema proposto, tem-se o seguinte problema de pesquisa: “Sabendo que inexistente legislação específica que trate sobre o estelionato virtual, pode-se afirmar que as normas gerais previstas no art. 171 do Código Penal, são suficientes para reprimir a prática do ato? ”.

Partindo do problema proposto, a pesquisa tem como objetivo geral verificar se a ausência de legislação específica que trate de modo expreso do estelionato virtual pode levar a impunidade dos agentes infratores ou as normas gerais previstas no art. 171 do Código Penal, são suficientes para prevenir a pratica do ato e penalizar os infratores. Os objetivos específicos são: entender o crime de estelionato propriamente dito, por meio da exposição de noções gerais acerca da temática; verificar o que são cybercrimes e como são tratados pelo ordenamento jurídico brasileiro; e por fim, estudar o crime de estelionato virtual propriamente dito, com considerações acerca dos projetos de lei que tratam do assunto.

Como método de pesquisa, elegeu-se o método dedutivo, por meio do qual, a partir de duas premissas que podem ser validas, alcançará a solução para o problema de pesquisa. Ou seja, dentre duas hipóteses, quais sejam, as normas gerais previstas no art. 171, do Código Penal, não são suficientes para combater a prática do crime de estelionato virtual, demandando legislação específica ou as disposições do art. 171, do Código Penal, são plenamente capazes de combater o crime de estelionato virtual, chegará a uma adequada solução do problema.

Para se chegar a solução do tema proposto, o autor, realizou uma pesquisa prioritariamente bibliográfica, utilizando como referencial teórico, as seguintes bases de pesquisa: Ricardo Antônio Andreucci (Manual de Direito Penal); Cezar Roberto Bitencourt (Penal Comentado); Rogério Greco (Código Penal Comentado); Victor Eduardo Rios Gonçalves (Direito Penal Esquematizado); Eliete da Silva Ribeiro (Crime de Estelionato); Felipe Machado Nauata (Crimes virtuais: estelionato); Luís Guilherme de Matos Feitoza (Crimes Cibernéticos: o Estelionato Virtual); Diego Cruz e Juliana Rodrigues (Crimes Cibernéticos e a Falsa Sensação de Impunidade); Riany Alves de Freitas (Estelionato Digital); Pedro Franco de Campos et. al (Direito Penal Aplicado) e Yuri Carneiro Coelho (Curso de Direito Penal Didático).

O interesse pelo tema decorre das notícias frequentes de golpes cometidos na internet, onde o agente ilude a vítima, com o fim de obter vantagem patrimonial ilícita. Justamente por isso, questiona-se se o atual tratamento conferido pelo legislador é suficiente para combater a prática, ainda que por hora, aparente ser demasiadamente frágil, levando a uma certa sensação de impunidade.

O presente trabalho de conclusão de curso será dividido em três partes. Na primeira parte da pesquisa, traçará noções gerais acerca do crime de estelionato, apresentando um breve desenvolvimento histórico, conceituando-o, e apresentando as demais noções introdutórias, tais como, sujeito ativo e passivo, natureza, momento da consumação. Esse estudo auxiliará na compreensão do crime de estelionato, sem o qual não será possível compreender um de seus desdobramentos, que aqui é objeto de pesquisa, o estelionato virtual.

Na segunda etapa da pesquisa, propõe-se a desenvolver um estudo acerca dos cybercrimes, demonstrando principalmente as dificuldades encontradas pelas autoridades policiais em identificar o autor da prática criminosa, que nesse tipo de estelionato, esconde-se atrás de uma tela, muitas vezes, com perfis falsos.

Na parte final da monografia, irá estudar o crime de estelionato virtual de modo específico, apresentando, inclusive, os projetos de lei em tramitação que pretendem combater o crime que a cada dia se torna mais frequente. Nesse momento, avaliará se a legislação penal atual é capaz ou não de combater a prática do crime ou se de fato é necessária a aprovação imediata de algum dos projetos de lei apresentado.

2. DISPOSIÇÕES GERAIS ACERCA DO CRIME DE ESTELIONATO.

Para se chegar a uma solução para o problema de pesquisa, imprescindível tecer algumas considerações introdutórias acerca do crime de estelionato. Sem essa abordagem inicial não é possível compreender suficientemente o que seja o estelionato virtual. Portanto, no presente capítulo, apresentará informações importantes sobre o crime de estelionato na sua forma fundamental, destacando, relato histórico, conceito, sujeitos do crime, natureza e momento da consumação do delito.

Para se atingir o objetivo do presente capítulo buscou-se utilizar de pesquisa bibliográfica, legal e jurisprudencial, por meio informações contidas e extraídas de doutrinas, leis, especialmente o Código Penal e jurisprudências, estas últimas, substanciadas em pronunciamentos do Supremo Tribunal Federal.

O termo estelionato provem da expressão grega *stelio* que dá nome a uma espécie de lagarto que muda de cor para iludir suas presas. A origem da palavra atenta para a tipificação do delito cometido pelo estelionatário, que no caso, se usa de artifícios para enganar alguém (RIBEIRO, 2019).

De acordo com a concepção histórica apresentada pelo autor, a palavra estelionato decorre de uma palavra grega que identifica um lagarto que engana as presas por meio da ilusão, assim, o estelionatário, seria aquele que se utiliza de artifícios fraudulentos para iludir as vítimas.

Como introduz Bitencourt (2012) nas Ordenações Filipinas, ao crime de estelionato era cominada a pena de morte quando o prejuízo à vítima ultrapassasse a vinte milréis. O Código Penal do Império de 1830 adotando o nome jurídico “estelionato” prescreveu-lhe várias figuras, indicando, entre elas, todo e qualquer artifício fraudulento em que se obtenha fortuna, parte dela ou quaisquer títulos. O Código Penal Republicano de 1890, por fim, seguindo a mesma orientação, tipificou onze figuras aliadas ao delito de estelionato, dentre elas o ato de utilizar-se de artifício para iludir a vítima, surpreendendo-lhe a boa-fé, com o fim precípua de obter lucro ou proveito.

Consoante o exposto, é possível aferir que ao longo dos anos, tentou-se reprimir cada vez mais a conduta daqueles que procuram mediante prejuízo alheio, obter vantagem ilícita, utilizando-se da boa-fé do primeiro e induzindo-o a erro.

Quanto mais se avançava a sociedade, mais o crime se aperfeiçoava, demandando atualizações legislativas para se evitar a impunidade.

Andreucci (2014) conceitua estelionato como sendo a obtenção de vantagem ilícita, para si ou para outrem, decorrente da indução ou manutenção de alguém em erro, utilizando-se de artifício, ardil ou qualquer outro meio fraudulento. Nessa perspectiva, o estelionatário, garante vantagem ilícita para si ou outra pessoa, mediante quaisquer atos que induzam a vítima a erro.

O crime de estelionato é, segundo se extrai da citação acima um crime que meche com a mente da vítima, que a faz acreditar em situações que se de fato existissem poderiam beneficiá-la. O criminoso engana, ilude, leva a vítima a erro, buscando com isso vantagem ilícita, decorrente de qualquer meio fraudulento.

Para o estelionatário o que importa é a vantagem patrimonial que receberá da vítima, quer para benefício próprio ou alheio, agindo de má-fé para induzir esta a lhe entregar os bens ou valores almejados. A vítima iludida, manipulada, enganada, entrega voluntariamente a coisa, baseada na confiança e respeito mútuos que devem ser sustentados em qualquer negócio jurídico, ela acredita veementemente que o estelionatário agirá de boa-fé.

Em sentido semelhante ensina Campos (2016), ao conceituar estelionato como sendo a obtenção pelo sujeito, de benefício para si ou para outrem, em prejuízo da vítima, a quem induz ou mantém em erro mediante artifício, ardil ou outro meio fraudulento. O crime é embasado, portanto, na má-fé do sujeito ativo, que induz a vítima ou a mantém em erro por qualquer meio fraudulento, com o objetivo de conseguir vantagem patrimonial que beneficiará a si próprio ou outra pessoa.

A partir das considerações dos autores retro transcritos, é possível conceituar estelionato como sendo o ato de induzir ou permitir que se mantenha alguém em erro, por qualquer meio fraudulento, com a finalidade de obter vantagem patrimonial ilícita para si ou para um terceiro.

O que se destaca é a boa-fé da vítima que realmente se entrega a manipulação do autor, pois baseia-se na confiança que tem no sujeito, o qual por sua vez, se aproveita dessa circunstancia para atingir o patrimônio do primeiro. Veja, não há subtração do patrimônio, mas entrega voluntária do bem pela vítima que acredita em uma suposta boa índole daquele que a ilude.

O delito de estelionato está tipificado no art. 171, do Código Penal (BRASIL, 1940), punindo com pena de reclusão de um a cinco anos e multa, aquele

que obtém, para si ou para outrem, vantagem ilícita, em prejuízo da vítima, a qual por sua vez, é induzida ou mantida em erro, mediante qualquer meio fraudulento.

Sabendo que a fraude é o ponto central do delito de estelionato, é possível se identificar os seguintes elementos que integram a figura típica: a conduta do agente ser direcionada a obtenção de vantagem ilícita em prejuízo de outrem; a vantagem pode ser dirigida ao autor ou a terceiro; a vítima é mantida ou colocada em erro; o agente se vale de um artifício, ardio ou qualquer outro meio fraudulento para atingir o fim pretendido (GRECO, 2011).

Nos termos da citação acima emerge-se que o crime de estelionato, poderá ser identificado mediante a verificação de algumas condutas, quais sejam, condutas do agente com o fim de obter vantagem ilícita, em prejuízo da vítima, a vantagem ser destinada para si ou para outra pessoa, indução da vítima ou manutenção da mesma em erro e ato de valer-se de qualquer meio fraudulento para a obtenção do fim pretendido.

Não há diferenças entre a fraude cível e a fraude penal, depende apenas da existência de uma fraude. Se trata de uma questão de qualidade e grau de prejuízo determinada pelas circunstâncias do caso. Com a análise da dimensão avaliar-se-á se a possível vítima, passou apenas por um mal negócio ou se estão presentes os requisitos para a consumação do crime de estelionato, caso em que deverá ser punido criminalmente (GRECO, 2011).

Destaca o autor, que para a consumação do crime não importa se a fraude é civil ou penal, basta que seja uma fraude, há apenas um dimensionamento da qualidade e grau da fraude, quesitos que serão verificados caso a caso. É por meio, da avaliação do caso concreto que se verificará, se a vítima foi prejudicada pelo fato de ter feito uma má negociação, ou se realmente foi induzida ou mantida em erro, por ato fraudulento daquele com quem negociou.

Ratifica-se, aqui, que o fato de haver perda patrimonial pela vítima decorrente de atos negociais com alguém, por si só não é capaz de consumir o delito de estelionato, é imprescindível a vontade consciente do autor de atingir o patrimônio daquela, o qual beneficiará a si próprio ou a terceiro, e que para atingir seu intento empregue meios fraudulentos para induzir ou manter o prejudicado em erro.

O bem jurídico tutelado é a inviolabilidade do patrimônio, especialmente em relação a atentados praticados mediante fraude. Tutela-se tanto o interesse

social, relacionado a confiança recíproca entre as partes, o qual deve presidir nas relações patrimoniais individuais ou comerciais, quanto o interesse público representado pela necessidade de reprimir a fraude causadora de dano a terceiro. Atente-se para o fato de que é vedado o cometimento de fraude para a obtenção de vantagem ilícita em prejuízo alheio. O estelionatário é tido como criminoso em todos os casos, mesmo que tenha cometido a fraude em relações que por sua própria natureza não precisam de proteção jurídica, porque em todo caso sua conduta é moral e juridicamente ilícita (BITENCOURT, 2012).

O bem jurídico objeto de proteção na criminalização do estelionato, é, nas palavras do autor a inviolabilidade do patrimônio, tutelando-se, tanto o interesse social, pautado na confiança entre as partes, quanto o interesse público consistente na repressão da fraude causadora de prejuízo alheio. Verbera, outrossim, que o estelionatário deve ser visto sempre como um criminoso, mesmo que tenha atuado em situações que dada a sua simplicidade não merecem proteção jurídica, pois sua ação sempre será moral e juridicamente ilícita.

Isto posto, o tipo penal previsto no art. 171, *caput*, do Código Penal, visa repreender o agente que mediante fraude causa prejuízo a outrem, pouco importando a dimensão do prejuízo causado, haja vista, que até em casos mais simples, afeta a confiança recíproca entre as partes, que por sua vez é tutelada com a tipificação do delito.

O que se almeja com a tipificação penal da prática é assegurar a segurança jurídica nos negócios celebrados entre as partes, os quais dependem de confiança e respeito mútuos, determinados pela consciência de ambas as partes e na crença de benefício para ambos.

Quanto aos sujeitos do crime, ressalta Andreucci (2014) que, o sujeito passivo é a pessoa que sofreu o prejuízo patrimonial, ao passo, que o sujeito ativo, é aquele que induz ou mantém determinada pessoa em erro, mediante artifício, ardil, ou qualquer meio fraudulento. Então o sujeito ativo será a pessoa que induz ou mantém a vítima em erro, mediante qualquer recurso fraudulento, e o sujeito passivo, será aquele que tem reduzido seu patrimônio, pela ação do sujeito ativo.

Nas palavras de Gonçalves (2018), o sujeito ativo do delito de estelionato é tanto aquele que emprega a fraude, quanto aquele que dolosamente se beneficia por esta, recebendo a vantagem ilícita. Por exemplo: se João e Pedro, em conluio de interesses, colocam o crime em prática e João emprega a fraude e convence a

vítima a entregar o objeto a Pedro, que após recebe-lo desaparece, é certo que Pedro tomou conhecimento da execução do delito e, portanto, é coautor do crime.

O sujeito passivo por sua vez é aquele que sobre o prejuízo patrimonial, que foram enganados por meio da fraude empregada, sendo plenamente possível que o agente engane a vítima, e esta entrega o bem pertencente a terceiro, hipótese em que ambas as pessoas serão vítimas de um único estelionato. Esta situação, e bem comum em lojas ou similares, em que a pessoa iludida é um funcionário, que entrega bem pertencente ao estabelecimento comercial, portando, pessoas jurídicas também podem ser vítimas do fato na condição de prejudicado economicamente pelo golpe (GONÇALVES, 2018).

Na mesma linha defendida pelo doutrinador anterior, completa o autor em epigrafe, que o sujeito ativo é aquele que concorre com a fraude ou se beneficia com a vantagem ilícita. O sujeito passivo, é, por sua vez, aquele que experimenta o prejuízo patrimonial decorrente do ato ilícito e todos aqueles que foram enganados em razão da fraude empregada pelo autor.

Esclarece, também, que é possível que o autor do crime engane uma determinada pessoa, para que esta lhe entregue bem de uma terceira pessoa, momento em que tanto a pessoa enganada, quando a pessoa que sofreu o prejuízo patrimonial será vítima do delito. Ademais, é possível que pessoas jurídicas figurem no polo passivo da demanda, haja vista que muito embora, não possa ser iludida, pode ser prejudicada economicamente pelo golpe.

Bitencourt (2012) alerta que crianças e débeis mentais, não poderão ser sujeitos passivos desse crime, pois é indispensável para a consumação da fraude, que se crie ou mantenha alguém em erro. E para que a vítima possa ser enganada é imprescindível que ela tenha capacidade de discernimento. Crianças e débeis mentais, não possuem essa capacidade, portanto, há impropriedade absoluta do objeto, pois um dos elementos do crime de estelionato é o emprego de meio fraudulento com o fim de iludir ou manter a vítima em erro, e sendo estes incapazes, não possuem capacidade de entender e querer, não podendo ser ludibriados, e tampouco, vítimas do crime.

O estelionato é um crime doloso que se consuma com a efetiva obtenção da vantagem ilícita pelo autor, em prejuízo da vítima. Admite-se a tentativa. Não se confunde com furto mediante fraude, pois nesse caso ocorre a subtração da coisa com o emprego de fraude que desvie a vigilância e atenção da vítima. No

estelionato, por seu turno, ocorre a entrega voluntária da coisa, em decorrência da fraude empregada pelo autor do delito. O estelionato também se difere na apropriação indébita, pois no estelionato o dolo do agente é anterior a posse ou detenção da vantagem ilícita, sendo que se utiliza de fraude para apropriar-se do bem. Na apropriação indébita ocorre o contrário, o agente recebe o bem de boa-fé, e após resolve apropriar-se dela. (ANDREUCCI, 2014).

Extraí-se da citação retro que o crime de estelionato é doloso, o que é plenamente previsível já que depende da vontade do agente de obter vantagem ilícita se utilizado de meios fraudulentos para a consecução do objetivo. Observe que para iludir alguém o autor do fato pratica atos conscientemente. Mesmo sendo um crime doloso, pois depende da vontade do agente de iludir a vítima, o crime admite tentativa.

Há também de se entender que estelionato e o crime de furto mediante fraude previsto no art. 155, §4º, II, do Código Penal, não são expressões sinônimas. No furto mediante fraude, o autor do fato subtrai a coisa, e se utiliza de tal coisa, para iludir a vítima. No estelionato, por sua vez, a vítima entrega de forma voluntária a coisa, após meios fraudulentos empregados pelo criminoso.

Também não identificam o mesmo fato, o estelionato e a apropriação indébita, haja vista que enquanto no estelionato, o dolo do agente é prévio a posse da coisa, na apropriação indébita o dolo é posterior a posse, pois o autor recebe o bem de boa-fé, sem más intenções, e após entende por bem se apropriar deste.

No crime de estelionato o ressarcimento do prejuízo antes de oferecida a denúncia não é caso de exclusão do crime, mas apenas de diminuição, nos termos do art. 16 do Código Penal. Se o ressarcimento ocorrer após o recebimento da denúncia, haverá circunstância atenuante genérica, consoante o disposto no art. 65, III, b, do Código Penal (ANDREUCCI, 2014).

Concluindo a análise do disposto pelo autor, tem-se que o ressarcimento do dano à vítima até o recebimento da denúncia, enseja a diminuição da pena a ser aplicada ao sujeito ativo e sendo o ressarcimento posterior ao recebimento da denúncia, ter-se-á circunstância atenuante genérica.

Quanto ao dolo no crime de estelionato, ressalta Campos (2016) que quando o dolo no crime de estelionato se trata de fraude em contrato, a indução ou manutenção da vítima em erro, deve ser inicial, ou seja, o ato lesivo deve coexistir no início da execução contratual, não se caracterizando o crime de estelionato a

intensão lesiva nascida a posteriori, na busca de proveito indevido, não visado anteriormente, situação em que se caracteriza mero inadimplemento contratual. Da mesma maneira, só haverá crime de estelionato acaso o dolo esteja presente no momento na formação do contrato, porque a fraude contratual só ofende a esfera civil, passando longe da orbita penal. Em verdade a fraude penal tem por objeto o lucro ilícito e não o objeto contratual.

Tal como ratifica o autor, o crime de estelionato, exige dolo prévio a prática do ato, pois depende da vontade consciente do autor de obter vantagem indevida para si ou para outrem. Então o intento de lesar a vítima por meio da indução ou sua manutenção em erro é previa.

Quanto ao momento da consumação do crime de estelionato, o Supremo Tribunal Federal (BRASIL, 2014), firmou entendimento por meio da Ação Cível Originária 2.361, com relatoria do Ministro Luiz Fux, que o delito em epígrafe se consuma com a obtenção da vantagem ilícita. *In casu*, pronunciou-se o Supremo em um Conflito Negativo de Atribuições, suscitado pelo Ministério Público de Minas Gerais em face do Ministério Público de São Paulo, para atuação em inquérito policial em andamento em São Paulo, o qual se destinava a investigar a suposta prática de estelionato.

O inquérito policial foi instaurado após o investigado ter vendido ingressos e hospedagem para o carnaval que ocorreria na cidade de Muzambinho, Minas Gerais, com o intuito de obter vantagem ilícita, já que sabia que não iria cumprir o acordo, ou seja, não iria entregar os ingressos nem prestar os serviços de hospedagem. A vantagem indevida, foi obtida após depósito de quantia pela vítima, em conta corrente de titularidade do autor do crime, cuja agência situava-se na cidade de Guaranésia, Minas Gerais (FUX, 2014).

Não contente com o primeiro golpe, o investigado, para eximir-se da obrigação de entregar os ingressos e prestar o serviço de hospedagem emitiu cheques para compensar os prejuízos da vítima, que por sua vez não foram compensados por ausência de fundos. Dada a multiplicidade de atos, questionou-se o local onde deveria ser processada a ação penal (FUX, 2014).

O Ministério Público de São Paulo remeteu os autos para a comarca de Guaranésia, Minas Gerais, entendendo que o crime de estelionato, se consuma no local da obtenção da vantagem indevida. O Ministério Público de Minas Gerais, por seu turno, encaminhou os autos ao Supremo Tribunal Federal para decidir sobre o

conflito negativo de atribuições, alegando que o estelionato, se consumou no local da recusa do pagamento do cheque pelo sacado, que no caso foi em São Paulo (FUX, 2014).

Para Fux (2014) para a resolução da controvérsia imprescindível uma análise aprofundada dos fatos narrados, pois se por um lado, a obtenção da vantagem indevida foi no Estado de Minas Gerais, por outro, o crime de estelionato pela emissão fraudulenta de cheque sem fundos se deu em São Paulo. Avaliando o caso, se verificou que a emissão do cheque sem previsão de fundos, não foi o meio para a consecução da vantagem ilícita, mas tão somente uma forma de assegurar a eficácia da conduta anterior.

Nesses termos o tipo penal é o previsto no art. 171, *caput*, do Código penal, pois a fraude e obtenção do benefício ilícito ocorreu antes da emissão dos cheques. Sendo assim, o segundo fato é apenas um desdobramento do primeiro, sendo mero exaurimento da conduta anterior. Assim, conforme o art. 70 do Código Processo Penal é competente para julgamento do feito o local em que a ação se consumar. Em se tratando do crime de estelionato, a competência para processar e julgar o fato é o juízo do local em que se obteve a vantagem patrimonial ilícita, que no caso em análise, é o local em que foi realizado o depósito na conta corrente do agente, que se deu em Minas Gerais (FUX, 2014).

Considerou o relator e autor da decisão monocrática, que a fraude consumada com a devolução dos cheques pela insuficiência de saldo, foi apenas um desdobramento da ação do autor do crime, para assegurar a eficácia da conduta anterior, que no caso foi a promessa de venda de ingressos e prestação de serviços de hospedagem que sabia que não iria cumprir, consumada com o depósito de quantia pela vítima. Assim, consoante o art. 70 do Código Penal (BRASIL, 1940), o juízo competente para processar a ação penal, é do local em que se consumar a infração, que no caso em análise, foi em Minas Gerais.

Diante de tudo o que fora explorado no presente capítulo, pode dizer em resumo que o crime de estelionato pode ser conceituado como aquele praticado com o fim de se obter vantagem ilícita, para si ou para outrem, em prejuízo da vítima, que é induzida ou mantida em erro pelo agente por artifício, ardil ou qualquer meio fraudulento.

De modo contínuo, o bem jurídico protegido pela tipificação do ato é a inviolabilidade do patrimônio. O sujeito ativo é aquele que emprega a fraude, e com

isso recebe a vantagem ilícita, o sujeito passivo, por sua vez, são todos os que sofrem o prejuízo patrimonial e todos os que foram enganados pelo estelionatário. É crime doloso, pois é necessária a vontade de auferir vantagem indevida, admite tentativa e dar-se-á por consumado no local em que se deu a obtenção da vantagem ilícita.

O estudo que foi aqui realizado auxiliará sobremaneira na solução do problema da pesquisa, já que traçou noções introdutórias de suma importância para a compreensão futura do que se trata o estelionato virtual, que é um desdobramento do estelionato fundamental que aqui se analisou. Dito isto, o próximo capítulo pretende fazer uma observação acerca dos crimes cometidos na internet, os chamados cybercrimes.

3. DOS CYBERCRIMES: UMA OBSERVAÇÃO ACERCA DOS CRIMES COMETIDOS NA INTERNET.

Considerando o estudado no capítulo anterior, o crime de estelionato consuma-se com a ação do sujeito para obter para si ou para outrem vantagem ilícita, em prejuízo da vítima, induzindo ou mantendo esta em erro, mediante artifício, ardil ou outro meio fraudulento. Feitas essas considerações iniciais acerca do crime objeto da pesquisa, buscará no capítulo em questão, entender o que são os cybercrimes.

O estudo que aqui se pretende é de suma importância para alcançar uma solução plausível para o problema proposto, já que é o ponto em que se compreenderá as formas e instrumentos utilizados pelo agente para o cometimento do estelionato virtual, para que após possa se entender se a legislação vigente é suficiente ou não para reprimir a prática do ato.

Destarte, aqui se analisará o conceito de crimes cibernéticos, ou cybercrimes, destacar a existência de várias nomenclaturas possíveis para identificar a ação, conhecer os instrumentos necessários para a prática do ato, as principais classificações, local do crime, dentre outras particularidades acerca da temática. Para atingir o intento do presente capítulo, o autor irá se utilizar de pesquisa bibliográfica, consolidada em doutrinas, artigos e trabalhos já publicados extraídos da internet.

Não se pode olvidar que a internet se tornou uma importante ferramenta no mundo globalizado, pois ao mesmo tempo que proporciona o relacionamento de pessoas e transmissão de informações, também é um meio de comércio. Contudo, a internet, juntamente com os benefícios, traz em mesma proporção uma quantidade infinita de ilícitos, que vêm aumentando assustadoramente (SANTOS et. al., 2017). Nesta senda, muito embora a internet venha sendo uma ferramenta de integração global, proporcionando o relacionamento de pessoas independente da distância, acaba por dar margem ao cometimento de vários delitos.

Com o advento da rede mundial de computadores a pessoa humana perdeu parcialmente sua privacidade, ficando sujeita a riscos decorrentes da exposição excessiva, ou até mesmo de danos a sua moral, embora seja inegável os pontos benéficos, como a integração cibernética, o armazenamento e coordenação

de dados e a facilitação de atividades e processos. Ocorre que, a internet tem contribuído consideravelmente para o aumento do que se chama de delitos informáticos, visto que serve de instrumento para a prática delitiva (SPINIELI, 2018).

Com o surgimento e popularização da internet, o ser humano, como bem destacado pelo autor, perdeu parcialmente sua privacidade, e mesmo que tenha trago consigo uma série de benefícios, como a integração de pessoas, o armazenamento e coordenação de dados e a facilitação das atividades diárias, ela tem contribuído consideravelmente com o aumento de número de crimes, servindo como um verdadeiro instrumento da prática delitiva.

O Grupo de Combate aos Crimes Cibernéticos, da Procuradoria da República no Estado de São Paulo (BRASIL, 2006), acrescenta que muitas coisas podem ser feitas com o auxílio da Internet, é possível pagar contas, trocar mensagens, participar de conversas em salas de bate-papo, fazer downloads de arquivos, comprar produtos, solicitar a realização de serviços, acessar informações de interesse. Mas todas essas atividades oferecem riscos ao usuário, pois em algum momento podem se deparar com alguém mal-intencionado que se aproveita da velocidade e da escala em que a troca de informações ocorre para cometer crimes.

Dessa maneira, mesmo que a internet, auxilie em inúmeras atividades e facilite a vida do ser humano, ela traz consigo riscos em igual proporção, pois não se pode desconsiderar em qualquer momento a existência de pessoas que se utilizam do meio eletrônico para a execução de práticas delitivas.

Completam Maues et. al (2018) que a internet trouxe inúmeros resultados positivos para o mundo globalizado, seja na perspectiva política, econômica, social ou cultural. Ocorre que foram trazidas também algumas mazelas, como por exemplo, a proliferação dos chamados crimes cibernéticos, tais como, a pornografia infantil, práticas de racismo, fraudes em contratos eletrônicos, crimes contra a honra, furtos, dentre outros crimes virtuais. Ratificam os autores que a internet tem sido o instrumento utilizado para a prática e proliferação dos chamados crimes cibernéticos, ou cybercrimes, que vão desde crimes contra a honra, a crimes de maior dimensão social, como a pornografia infantil.

Não há na doutrina uma nomenclatura sedimentada acerca dos crimes cometidos na internet, contudo, independentemente do nome utilizado, há uma caracterização única, posto que para esses crimes será observado o uso de dispositivos informáticos, a utilização de rede de transmissão de dados para

delinquir, e o bem jurídico lesado deverá ser uma conduta típica, antijurídica e culpável (SILVA, 2015). Isto posto, embora não haja um posicionamento doutrinário consolidado acerca da nomenclatura dos crimes cometidos na internet, esses se consumam sempre da mesma maneira, ou seja, o infrator se utiliza de equipamentos informáticos, da internet, para cometer ato ilícito.

Na mesma linha Jorge e Wendt (2012) verberam crimes digitais, crimes eletrônicos, ciber crimes, crimes cibernéticos, dentre outras nomenclaturas possíveis, procuram dar nome à atividade criminosa realizada com a utilização de um computador e mediante o acesso à rede. Confirmando, a visão anterior, os autores, alertam que independente da terminologia utilizada, de um modo geral, todas dizem respeito ao ato criminoso realizado com o apoio de um dispositivo informático e mediante o acesso à rede de transmissão de dados.

Segundo conceituação atribuída pela Secretaria da Mulher de Pernambuco crime cibernético é aquele em que ocorre a invasão de um equipamento eletrônico ou a violação de uma rede social objetivando a obtenção, adulteração, destruição de informações ou danos pessoais sem a autorização ou permissão do seu proprietário. No crime em questão inclui-se a instalação de softwares maliciosos que estabelecem vulnerabilidades de acesso a informações pessoais não autorizadas (BRASIL, 2017).

Segundo o disposto, os crimes cibernéticos, podem ser conceituados como a invasão de um equipamento eletrônico, ou violação de perfil em rede social, com a finalidade de obter, adulterar, destruir dados ou informações pessoais, sem a autorização ou permissão do titular da conta. O crime abrange, também, a conduta de instalar softwares maliciosos para criar vulnerabilidades de acesso a informações não autorizadas.

Rossini (2004) utilizando a terminologia “delito informático”, conceitua a ação como sendo a conduta típica e ilícita, que se constitui em crime ou contravenção penal, dolosa ou culposa, por ação ou omissão, praticada por pessoa física ou jurídica, com a utilização dos meios de informática, em ambiente conectado a rede ou fora dele e que ofenda direta ou indiretamente, a segurança da informática, que tem os seguintes elementos: integridade, disponibilidade e confidencialidade.

Nos termos da citação retro, os delitos informativos, são aqueles em que o autor pessoa física ou jurídica, pratica conduta típica e ilícita, caracterizada como

crime ou contravenção penal, seja o ato doloso ou culposo, comissivo ou omissivo, com o uso de equipamentos de informática, em ambiente de rede ou fora dele, com o fim de ofender direta ou indiretamente, a integridade, disponibilidade e confidencialidade da informática.

Desmembrando essa conceituação para melhor compreensão, percebe-se que os cybercrimes, muito embora sejam usualmente praticados por pessoas físicas, especialmente pelos chamados *hackers*, a ação pode ser praticada também por pessoas jurídicas. A conduta praticada por quaisquer das pessoas mencionadas deve ser típica, ilícita e caracterizada como crime ou contravenção penal.

Destaca-se, outrossim, que a conduta poderá ser dolosa, que é aquela intencional, cujo resultado era planejado pelo autor do fato ou culposa, aquela que é resultado de negligência, imprudência ou imperícia do sujeito, comissiva ou omissiva. Por fim, a última parte conceitual dispõe que a ação será praticada com o auxílio de equipamentos de informática, tais como celulares, computadores e dispositivos correlatos, na rede mundial de computadores ou fora dela, com o fim de se ofender seja direta ou indiretamente a segurança da informática. Percebe-se que de acordo com essa conceituação, o ponto alvo não é a internet, pois de acordo com o autor, os crimes informáticos podem ser praticados sem ela, o ponto de atenção é a utilização de dispositivos de informática.

Os crimes cibernéticos possuem inúmeras classificações adotadas pelas doutrinas, mas destas, destacam-se duas, uma faz referência a crimes cibernéticos puros, mistos e comuns, e a outra classifica as infrações em próprios e impróprios (MATSUYAMA e LIMA, 2016).

De acordo com a primeira classificação, os crimes cibernéticos podem ser puros, mistos ou comuns. O crime cibernético puro é aquele em que o infrator objetiva especificamente atacar o sistema computacional e seus componentes, o agente tem o objetivo de atingir o equipamento físico, o sistema informático e as informações constantes nos bancos de dados, aqui toma-se como exemplo a invasão a servidores e sites (MATSUYAMA e LIMA, 2016).

O crime cibernético misto, por seu turno, se consolida pela ação criminosa essencialmente condicionada ao uso da Internet para atingir o intento delituoso. O agente não dirige sua conduta ao sistema computacional nem a seus componentes, mas a tecnologia é a ferramenta para atingir seu intento. Cita-se como exemplo, a retirada de valores monetários em contas bancárias via *homebanking*. Os comuns

são aqueles em que a internet é apenas o instrumento para a consumação de crimes já tipificados no Código Penal, como os crimes contra a honra praticados na internet (MATSUYAMA e LIMA, 2016).

Pela segunda classificação os crimes cibernéticos podem ser próprios ou impróprios. Os crimes cibernéticos próprios, caracterizam-se pela sua autonomia, e distinção das condutas já consolidadas no Código Penal, daí a dificuldade ou impossibilidade na criminalização de tais ações. Os impróprios, são aqueles em que é possível a aplicação da norma penal às condutas, pois o agente se vale de recursos informáticos como instrumento para a consumação de crimes já previstos no Código Penal (MATSUYAMA e LIMA, 2016).

Monteiro (2010) na mesma linha disciplina que a classificação mais adotada é a que divide os crimes eletrônicos em puros e impuros. Os puros são aqueles que os dados e os sistemas eletrônicos se constituem como o objeto do delito. Os impuros seriam aqueles em que os meios eletrônicos servem como ambiente para a prática do ato e o objeto jurídico tutelado já encontra respaldo legislativo em algum dispositivo penal.

Há também uma outra classificação que os divide em duas espécies, comuns e específicas. Nas condutas comuns, os meios informáticos são utilizados para praticar condutas consideradas puníveis pela legislação vigente, ao passo que as condutas específicas seriam aquelas enquadradas em situações que ainda não encontram respaldo jurídico, como o mero acesso indevido a um sistema computacional em que haja dano decorrente do ato ou desenvolvimento de vírus no sistema (MONTEIRO, 2010).

No que se refere às características da prática delitiva aqui desenvolvida é a volatilidade da materialidade desses atos. Por não se tratarem de dados estáticos ou que se localizam em um único local, estes podem ser facilmente alterados ou apagados, mesmo que sem intenção. Apesar de quase sempre ser possível resgatar os dados, mesmo que tenham sido deslocados intencionalmente, a maioria das investigações é interrompida por não se conseguir informações suficientes para delimitar a materialidade e autoria da infração (MONTEIRO, 2010).

Verbera o autor que os cybercrimes possuem uma característica que muitas vezes podem incidir em impunidade, a volatilidade da materialidade dos atos praticados, vez que por ser um crime mutável, vários dos seus registros podem ser facilmente alterados ou apagados, mesmo que de modo não espontâneo, e muito

embora alguns destes possam vir a ser recuperados, a maioria tem impedido o prosseguimento das investigações.

Outra característica visível nos crimes informáticos é que esses não delimitam fronteiras, ou seja, eles não se restringem a determinada região geográfica. Os autores do fato podem estar em um país, o objeto tutelado em outro e o resultado ser produzido em um terceiro país. Essa natureza peculiar dos crimes informáticos, são extremamente interessantes no âmbito jurídico, tendo em vista a necessidade de se delimitar fronteiras para o processamento adequado do delito (MOTTEIRO, 2010).

Naturalmente a maior parte dos delitos demanda um tempo no espaço para ser delimitado e reconstruído. Os crimes eletrônicos, por sua vez, funcionam de modo diverso. Estes podem acontecer em frações de segundos ou mesmo em horas seguidas, sendo assim a determinação do local do crime e a aplicação do princípio da extraterritorialidade podem encontrar alguns desafios. Alguns países tendem a aplicar a teoria da ubiquidade, ou seja, a competência é determinada pelo local em que qualquer fase do crime ocorreu. O Brasil adota tal teoria, principalmente em relação a delitos que não acontecem em território nacional. Mas se aplicada tal teoria vários países podem ser competentes para o processamento do crime (MONTEIRO, 2010).

Pelas citações acima afere-se que outra característica dos cybercrimes é o fato de que estes não possuem fronteiras, não há determinação geográfica para ocorrerem. De modo geral, o autor do fato pode estar em um país, o objeto tutelado pode estar em outro e o resultado ocorrer em local diverso dos dois primeiros. Ante essa dificuldade o Brasil tem adotado a teoria da ubiquidade para determinar a competência de julgamento do crime. Pela teoria a competência será determinada pelo local em que ocorreu quaisquer das fases mencionadas, sendo que o ato fracionado será considerado como o todo do crime.

Shimabukuro (2017) explica que com a popularização do acesso a internet os crimes digitais assumiram números assustadores no Brasil. De acordo com dados da SaferNet no ano de 2017, que controla a Central Nacional de Denúncias, foram recebidas e processadas mais de 115 mil denúncias referentes a crimes contra direitos humanos no ano de 2016. Os crimes envolvendo fraudes bancárias não ficaram pra trás, com prejuízo de cerca de R\$ 1,8 bilhão só em 2015. Os crimes bancários envolvem também roubo de senhas e kits boletos,

exclusividade do Brasil. Além dos crimes em epigrafe, destacam-se, a pornografia infantil, o bullying, a violação a direitos autorais, racismo e casos recentes de ciberterrorismo.

De acordo com a citação acima após a internet se tornar mais popular no Brasil, os índices de cometimento de crimes digitais assumiram índices assustadores. Salieta que de acordo com a SaferNet, órgão que controla a Central Nacional de Denúncias, foram contabilizadas mais de 115 mil denúncias envolvendo crimes contra os direitos humanos na internet, só no ano de 2016. Os crimes envolvendo fraudes bancárias também tomaram uma grande proporção, tanto que os bancos brasileiros chegaram a perderem R\$ 1,8 bilhão de reais só no ano de 2015. Além dos crimes mencionados, destaca, ainda, crimes envolvendo pornografia infantil, bullying, violação de direitos autorais, racismo, e até mesmo ciberterrorismo.

Assim como os crimes comuns se aperfeiçoam com o tempo, os crimes virtuais também têm tomado novas formas por meio do avanço da tecnologia, a qual tem permitido e facilitado suas práticas. Com o aumento do número de usuários, que já ultrapassa os 3 bilhões é cada vez mais difícil identificar os agentes que cometem crimes na internet. No período de 11 anos, a Safernet Brasil, registrou o recebimento e processamento de 3.861.707 denúncias anônimas, o que demonstra o alto índice de crimes virtuais (PAGNOZZI, 2018). Assim, a popularização da internet no Brasil, tem facilitado e permitido o aumento e avanço dos cybercrimes, que nos últimos anos estão atingindo índices alarmantes.

Os primeiros crimes eletrônicos conhecidos datam os anos 60, onde práticas caracterizadas como estelionato aconteceram. Os primeiros trabalhos nesse sentido, datam a década de 70, onde alguns cenários interessantes foram alvos de argumentação. Vários crimes aconteceram na década de 80, sistemas inteiros de bancos, tráfico aéreo, pagamento, prisionais, foram prejudicados, causando danos em diferentes países. Já nessa época, experimentou-se grandes prejuízos financeiros que já alcançavam a casa dos milhões. Entretanto, o diferencial dos crimes cometidos na época encontra-se no fato de poderem ser considerados como românticos da criminalidade informática, já que figurava apenas uma pessoa reclusa em uma sala escura obtendo proveito próprio, hoje em dia existem organizações criminosas transnacionais, cuidando da prática do fato (MONTEIRO, 2010).

Consoante a citação acima os crimes cibernéticos, ficaram conhecidos em meados dos anos de 1960, momento em que alguns crimes enquadrados como

estelionato ocorreram. Os primeiros trabalhos acerca da temática são datados da década de 1970. Em 1980 vários cybercrimes ocorreram e sistemas inteiros de bancos, controles de tráfego aéreo, pagamentos, prisionais foram prejudicados, causando danos em diversos países, já nessa época os prejuízos decorrentes da ofensa já alcançavam as casas dos milhões.

Muito embora as práticas já fossem conhecidas desde estas épocas, como salienta o autor, esses anos podem ser considerados como os românticos na criminalidade na informática, pois até então os infratores cometiam os delitos em pequenas salas escuras e em proveito próprio, exclusivamente. Nos tempos modernos com a evolução dos sistemas de informática e popularização da internet, vêm aparecendo, inclusive organizações criminosas que dominam os ambientes em que as infrações acontecem.

Deste modo, a modernização e popularização das redes informatizadas, têm sido um ambiente ideal para o cometimento de crimes cibernéticos, até porque, em várias situações o usuário não tem pleno conhecimento do sistema que utiliza e acaba por ficar em um campo vulnerável.

Segundo dados levantados pela Safernet Brasil, considerando os anos de 2006 e 2011, averiguou-se um crescimento significativo nos casos de cybercrimes no Brasil, é o que demonstra o quadro abaixo.

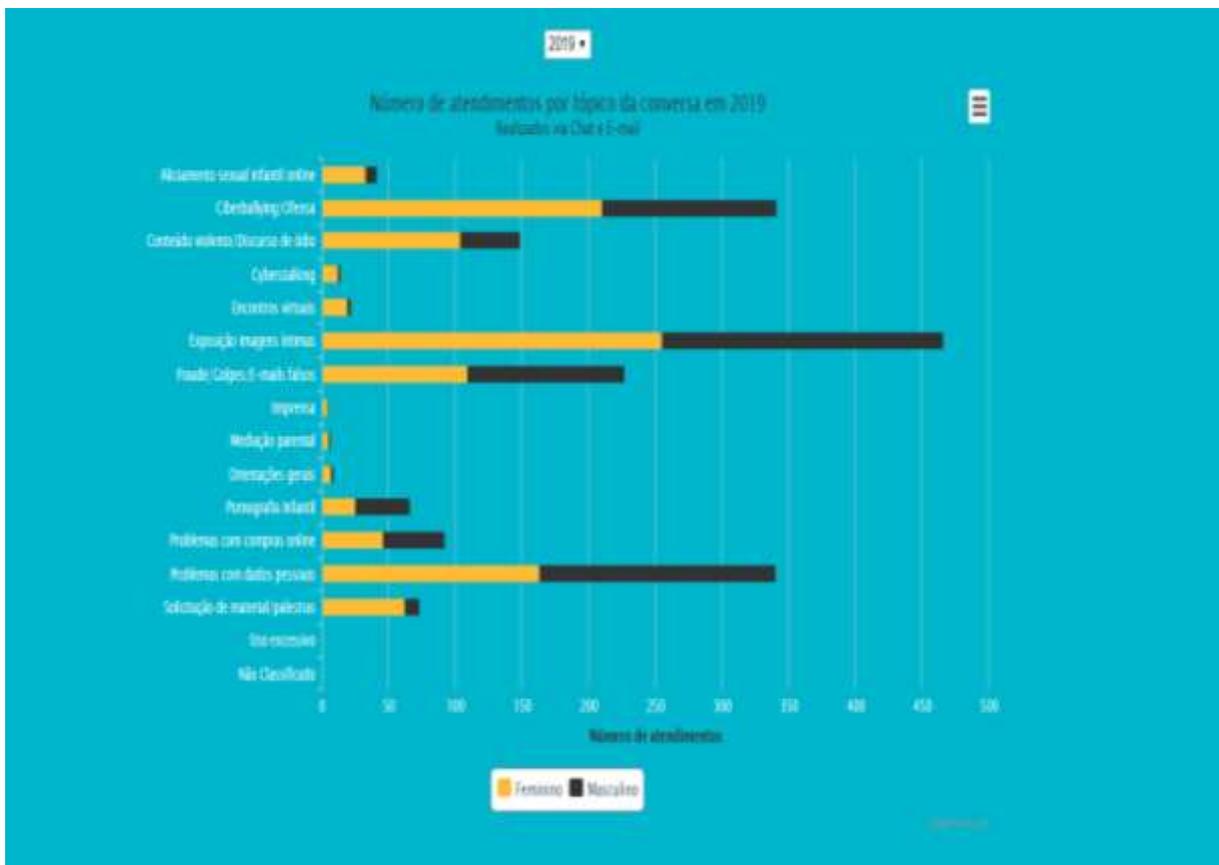
QUADRO 1 – PERIGO NA REDE: Páginas na internet denunciadas no Brasil



De acordo com os dados apresentados no quadro acima houve um aumento considerável de 2006 para 2011 nos crimes de racismo, pornografia infantil, apologia e incitação a crimes contra a vida, homofobia, maus tratos contra animais, intolerância religiosa, xenofobia e neonazismo. O crime de tráfico de pessoas que antes foi considerado junto a outros delitos, ganhou espaço próprio. Em termos gerais, de um total de 519 registros, passou para 2.001, ou seja, a demanda de 2011 chegou a quase quatro vezes às registradas em 2011.

Os índices de 2019 são igualmente alarmantes, registrou o atendimento de homens e mulheres, em diferentes tópicos, dentre eles: aliciamento sexual infantil online, *ciberbullying*, discursos de ódio, *cyberstalking*, encontros virtuais, exposição de imagens íntimas, fraudes e golpes, imprensa, mediação parental, orientações gerais, pornografia infantil, problemas com compras online, problemas com dados pessoais.

QUADRO 2 – Número de atendimentos por tópico da conversa em 2019



Fonte: Safernet Brasil. Indicadores. <http://indicadores.safernet.org.br/indicadores.html>.

De acordo com o gráfico acima, os crimes de maior incidência no meio virtual são a exposição de imagens íntimas, o *ciberbullying* e aqueles relacionados a problemas com dados pessoais. Em todas estas verificam-se uma certa equivalência no número de denúncias em razão do gênero da vítima, sugerindo que os crimes virtuais não têm opção entre homem ou mulher.

Num geral, o surgimento da internet foi um grande avanço para o mundo globalizado, oferecendo facilidades, como a execução remota de atividades, bem como ampliando o campo de interação das pessoas. Contudo, ao mesmo tempo que trouxe incontáveis benefícios, tem submetido os usuários a uma perda parcial de privacidade, os deixando a mercê de pessoas mal-intencionadas que aproveitam-se das facilidades decorrentes da internet para causar dano a outrem, o que tem se intitulado de cybercrimes.

Portanto, o estudo aqui elaborado auxilia na solução do problema da pesquisa, tendo em vista que trata dos cyber crimes de um modo geral, o que são, como são consumados, dispositivos utilizados para tal feito e principais crimes cometidos no meio eletrônico. Em sendo assim, o próximo capítulo irá analisar um crime cibernético específico, o estelionato virtual.

4. DO CRIME DE ESTELIONATO VIRTUAL.

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 utiliza de artifício, 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 capítulo procurará traçar algumas considerações acerca do crime de estelionato virtual, propriamente dito, destacando especialmente a ausência de norma específica que regule a espécie e os projetos de lei em tramitação que cuidam da matéria. Para a melhor compreensão do estudo que aqui se realizará, o capítulo 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.

4.1 DO CRIME DE ESTELIONATO VIRTUAL NO ORDENAMENTO JURIDICO BRASILEIRO

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 capítulo 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 certa 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 Ataíde (2017) ocorre crime de estelionato virtual quando os infratores criam links, e-mails, etc., falsos, com o objetivo de não ser identificado e conseqüentemente 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 casa, 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 específico, 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 legítima 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 benefício 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 induzir a vítima em erro para que essa efetue pagamento antecipado para a compra de produtos, na ilusão de que irá recebê-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 enganá-las 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 prática 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 específica. 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 específicas que cuidem dos crimes cibernéticos.

Segundo Feitoza (2012) a ausência de legislação específica acerca do tema acaba por induzir os criminosos a praticarem a infração, pois confiam na impunidade devido a falta do instrumento normativo específico. 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 específica 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 específica 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 específicas, 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, não

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 específica 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 Ataíde (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.

O Direito como uma ciência normativa não deveria permanecer inerte frente a tantas modificações no contexto social, nessa perspectiva, as condutas fraudulentas merecem tipificação penal específica, já que essas ilicitudes lesam ofendem bens de suma importância para a sociedade. Assim sendo, muitas reflexões têm sido realizadas no âmbito do direito penal, com o objetivo de proporcionar a atualização dos tipos penais previstos no ordenamento jurídico brasileiro. Seguindo esse raciocínio, é evidente a dificuldade do Direito em adaptar-se ao contexto social que modifica-se constantemente, não conseguindo acompanhar principalmente o avanço proporcionado pelas novas tecnologias, sendo a internet um ambiente completamente livre e sem fronteiras, do qual os agentes se aproveitam da possibilidade de anonimato e ausência de regras (FEITOZA, 2012).

O Direito como uma ciência normativa, não poderá conforme considerado na citação retro, permanecer estático, devendo, pois, atender a todas as mudanças decorrentes da evolução da sociedade, e as condutas fraudulentas demandam tipificação penal, já que atingem bens de extrema importância para a sociedade. Dessa forma tem surgido inúmeras reflexões no âmbito do direito penal, destacando as dificuldades do Direito em se adaptar ao atual contexto social. O Direito, não tem conseguido acompanhar o rápido avanço das novas tecnologias, especialmente da internet, que é um ambiente livre e acessível, local propício ao cometimento de novas modalidades de crimes, por pessoas que se aproveitam da possibilidade de anonimato e ausência de regras.

O Plano Nacional de Informática e Automação, a Lei nº 7.232/84, foi umas das primeiras leis a tratar da informática no Brasil e versava acerca das diretrizes informáticas em solo Brasileiro. Logo depois, a Lei nº 7.646/87, foi revogada dando espaço à Lei nº 9.609/98. Há, também, a Lei nº 12.965/14, conhecida como o marco civil da internet, e veio para regular os direitos e deveres, como também estabelecer os princípios e garantias aos usuários da Internet (ATAIDE, 2017).

A internet chegou ao Brasil em 1988, iniciando-se por São Paulo e Rio de Janeiro, até ganhar espaço nos demais Estados, e desde a sua concepção houveram alguns instrumentos normativos, como a Constituição Federal de 1988, que trata das proteções dos dados e ainda anterior à Carta Magna, a Lei nº 7.232/84, que dispõe sobre a Política Nacional de Informática e outras providências. Fora estas, até o ano de 2012 não havia qualquer outra lei zelando pelos direitos e responsabilidades com a utilização da internet (CRUZ e RODRIGUES, 2018).

As leis que surgiram a partir de 2012, decorreram de grande pressão da mídia sobre o poder legislativo, a promulgação da lei foi subsequente a fotos íntimas da atriz Carolina Dieckmann, serem divulgadas na internet, na época os indivíduos, localizados, foram indiciados por extorsão qualificada, furto e difamação. T tamanha foi a repercussão do fato que seis meses após a divulgação das fotos, foram publicadas na mesma data as Leis nº 12.735/12 e 12.737/12 (CRUZ e RODRIGUES, 2018).

Cruz e Rodrigues (2018) verberam que está claro que pela lei promulgada o legislador não se ateuve a necessidade de previsão dos cybercrimes em espécie, mas sim com o momento, no qual uma pessoa com fama publica, teve fotos íntimas divulgadas na mídia. Os demais crimes praticados na internet continuam sendo processados conforme o efeito danoso provocado pelos infratores. O real problema nessa insuficiência normativa não é a falta de lei que os classifica e os pune, mas de questões técnicas de como se chegar no autor do fato e na competência para julgamento.

Consoante a citação acima, afere-se que até que ocorresse uma situação de decorreu em grade mídia, o legislador não havia se preocupado com os cybercrimes em espécie, foi necessário que uma pessoa famosa tivesse fotos íntimas divulgadas para que isso ocorresse. Já os demais crimes praticados na internet, permanecem sem o devido suporte legislativo e continuam a ser julgados com base nos efeitos do ato danoso praticado pelo agente. Necessário salientar o

real problema dos crimes cibernéticos, não se encontra na ausência de lei que classifica o crime e pune, mas nas questões técnicas a ele inerentes, como o modo de se chegar ao infrator e a competência de julgamento.

Em suma, o crime de estelionato virtual, não possui legislação específica 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 inexistente 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 específica do delito em questão.

4.2 DOS PROJETOS DE LEI SOBRE O TEMA

Verificado no item anterior que inexistente norma que trate de forma específica do crime de estelionato virtual, apresentará no presente espaço, os projetos de lei acerca do tema. O estudo que aqui se pretende será sustentado principalmente na avaliação ao Projeto de Lei do Senado nº 76/2000, ao Projeto de Lei do Senado nº 137/2000 e ao Projeto de Lei da Câmara nº 89/2003.

Segundo Feitoza (2012) o delito de estelionato virtual merece atenção especial pelo legislativo brasileiro, tendo em vista o alto grau de danos que vem causando a sociedade, e por isso, não se pode protelar projetos que se encontram em tramitação do Congresso Nacional e que dependem da aprovação dos deputados e senadores em suas respectivas casas. Diariamente, novos usuários se tornam vítimas destes criminosos que se aproveitam da inexistência da norma para fraudar as vítimas, lhes oferecendo bens e serviços, e não cumprindo a obrigação pactuada, gerando prejuízos irreparáveis.

Como salientado na citação retro transcrita o crime de estelionato virtual deve ser objeto de atenção pelos legisladores, pois tem provocado grande impacto na sociedade, assim, não se pode mais retardar os projetos em tramitação. A cada

dia sobem os casos de pessoas que se tornam presas fáceis para esses criminosos, aproveitando-se estes últimos da inexistência de lei regulamentadora para causar prejuízos às vítimas.

Nas palavras de Feitoza (2012) o estelionato cometido por meio da internet está inserido em alguns projetos de lei que se presta, a tipificar as condutas e puni-las. O projeto de lei, assim como seu substitutivo ao PLS/2000, PLC 89/2003 e PLC 173/2000, pleiteiam a alteração da lei, abrindo espaço para a inclusão de um parágrafo segundo ao art. 171 do Código Penal, apresentando a definição de estelionato virtual e a maneira com a qual deverá ser punido, aumentando sua pena.

O crime de estelionato virtual estava sendo tema de três projetos de lei que visam tipificar esta e outras condutas e puni-las de maneira mais correta. Almeja-se que seja inserido um outro parágrafo no art. 171 do Código Penal, que tratará especificadamente do crime de estelionato virtual e como deverá ser punido, sendo considerado uma causa de aumento de pena a utilização de meios de tecnologia da informação na prática de estelionato.

Partindo para a análise em ordem cronológica do Projeto de Lei do Senado nº 76/2000, Projeto de Lei do Senado nº 137/2000 e Projeto de Lei da Câmara nº 89/2003. Verifica-se que aprovada a redação final do PLC nº 89/03, reataram prejudicados os Projetos de Lei do Senado nº 76 e nº 137, ambos de 2000, os quais foram para arquivo de 10 de setembro de 2008 (BRASIL, 2000).

A situação atual do Projeto de Lei sobrevivente, em consulta ao site oficial, indica que a sua tramitação está encerrada, transformada em norma jurídica com veto parcial em 01 de setembro de 2014 e encaminhada a secretaria de arquivo em 18 setembro de 2014 (BRASIL, 2003).

Consoante o disposto, afere-se que muito embora, tenham havido tentativas para tipificar a conduta de estelionato virtual propriamente dita, não se obteve êxito, até então, permanecendo inalterado o texto do Código Penal, e sem qualquer norma específica que veio para tratar especificadamente do assunto.

5 CONSIDERAÇÕES FINAIS

A partir da pesquisa realizada, pode-se afirmar que a internet é tida como um grande avanço no mundo globalizado, contando com inúmeras facilidades para o mundo moderno, como a execução de atividades remotas e interação de pessoas. Contudo, embora ofereça inegáveis benefícios, traz consigo uma série de problemas, decorrentes da perda parcial de privacidade pelos usuários, que são alvos fáceis de pessoas mal-intencionadas que aproveitam-se da internet para causar mal a outrem.

Não se pode olvidar que com os avanços promovidos com o surgimento da internet, houveram também variações no modo de execução de alguns crimes. A dificuldade de constatação do autor do crime, bem como as demais facilidades que a internet proporciona levaram a uma elevação significativa do número de casos dos chamados cybercrimes.

No decorrer da pesquisa constatou-se, inicialmente, que o crime de estelionato é conceituado como toda ação praticada com o intuito de obter para si ou para outrem vantagem patrimonial em prejuízo da vítima, utilizando-se o autor do fato de artifício, ardil ou qualquer meio fraudulento, que leve a vítima em erro ou a se manter em erro. Após constatou-se que os crimes virtuais são aqueles praticados em ambiente virtual, com a utilização de equipamentos eletrônicos e acesso a rede mundial de computadores.

Conjugando essas duas conceituações, aferiu-se que o crime de estelionato virtual é aquele em que o sujeito utilizando-se de equipamentos tecnológicos e acesso à internet, induz ou mantém alguém em erro, por meio de artifício, ardil, ou qualquer meio fraudulento, com o fim de obter vantagem ilícita, em benefício próprio ou de outrem, e em prejuízo da vítima.

Descobriu-se, outrossim, que inexistente no ordenamento jurídico brasileiro, legislação específica que trate do crime de estelionato virtual, sendo os agentes processados pelo crime de estelionato, conforme tipificado no art. 171 do Código Penal. Entretanto, a ausência de norma específica tem causado alguns problemas no que tange a punição do agente infrator, tendo em vista dificuldades na sua localização, definição do local do crime e competência, fatos que levam a uma

sensação de impunidade. Aferiu-se que chegaram a tramitar três projetos de lei acerca do assunto, mas ambos não prosperaram, persistindo, portanto, essa lacuna que impede a correta punição do infrator.

De posse do exposto, há por satisfeitos todos os objetivos da monografia, e tendo-se o seguinte problema de pesquisa: “Sabendo que inexistente legislação específica que trate sobre o estelionato virtual, pode-se afirmar que as normas gerais previstas no art. 171 do Código Penal, são suficientes para reprimir a prática do ato?”, chega-se ao resultado de que as normas gerais prescritas pelo art. 171, do Código Penal, que trata do crime de estelionato, é insuficiente para reprimir a prática de estelionato virtual, especialmente porque a norma não é eficaz para ter a correta definição do autor do delito, não traz diretrizes para a fixação do local do crime e da competência, o que tem desencadeado uma sensação de impunidade.

Atingir tal resultado, foi relativamente complicado, tendo em vista a insuficiência de pesquisas a respeito, o que foi surpreendente em razão das altas taxas de incidência do crime. Imaginou-se que por ser um problema recorrente, existiria, ao menos projetos de lei em tramitação, o que se viu não ser verdade, pois todos os projetos propostos, não atingiram o intuito de tipificar especificamente o crime de estelionato virtual.

Os resultados aqui obtidos, servem de alicerce para a exigência de ações efetivas do poder legislativo, para que diante da gravidade e crescimento dos crimes cibernéticos, atue para reprimir e prevenir condutas em que o autor se utiliza da internet para causar dano a outrem. Ademais, serve de base para pesquisas semelhantes, pois se sabe que nenhum estudo é satisfativo e consegue abordar, sozinho todas as nuances do tema.

REFERÊNCIAS

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

ATAÍDE, Amanda Albuquerque de. **Crimes Virtuais**: uma análise da impunidade e dos danos causados às vítimas. Maceió, 2017. Disponível em:< http://www.faaiesa.edu.br/aluno/arquivos/tcc/tcc_amanda_ataide.pdf>. Acesso em: 20 abr. 2020.

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

BRASIL. Conselho Nacional de Justiça. **CNJ Serviço**: qual a diferença entre crime e contravenção?. Disponível em:< <https://www.cnj.jus.br/cnj-servico-qual-a-diferenca-entre-crime-e-contravencao/>>. Acesso em: 20 abr. 2020.

_____. **DECRETO-LEI N° 2.848, DE 7 DE DEZEMBRO DE 1940**: Código Penal. Disponível em:< http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm>. Acesso em: 19 fev. 2020.

_____. **LEI N° 12.737, DE 30 DE NOVEMBRO DE 2012**. Disponível em:< http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 19 fev. 2020.

_____. Procuradoria da República no Estado de SP. **Crimes cibernéticos**: manual prático de investigação. 2006. Disponível em:< <https://egov.ufsc.br/portal/conteudo/crimes-cibern%C3%A9ticos-manual-pr%C3%A1tico-de-investiga%C3%A7%C3%A3o>>. Acesso em: 20 abr. 2020.

_____. **Projeto de Lei da Câmara nº 89, de 2003**. Altera o Decreto-Lei nº 2848, de 07 de dezembro de 1940 - Código Penal e a Lei nº 9296, de 24 de julho de 1996, e dá outras providências. Disponível em:< <https://www25.senado.leg.br/web/atividade/materias/-/materia/63967>>. Acesso em: 23 maio 2020.

_____. **Projeto de Lei da Câmara nº 137, de 2000**. Estabelece nova pena aos crimes cometidos com a utilização de meios de tecnologia de informação e telecomunicações. Disponível em:< <https://www25.senado.leg.br/web/atividade/materias/-/materia/44045>>. Acesso em: 23 maio 2020.

_____. **Projeto de Lei do Senado nº 76, de 2000.** Define e tipifica os delitos informáticos, e dá outras providências. Disponível em:< <https://www25.senado.leg.br/web/atividade/materias/-/materia/43555>>. Acesso em: 23 maio 2020.

_____. SaferNet. **Institucional.** 2020. Disponível em:< <https://new.safernet.org.br/content/institucional#mobile>>. Acesso em: 20 abr. 2020.

_____. Secretaria da Mulher de Pernambuco. **Crimes Cibernéticos.** Recife, 2017. Disponível em:< <http://estaticog1.globo.com/2017/12/28/CartilhaCrimeCiberneticoSecMulherPernambuco.pdf>>. Acesso em: 20 abr. 2020.

_____. Supremo Tribunal Federal. **Ação Cível Originária 2.361 São Paulo.** Autor: Ministério Público de Minas Gerais. Réu: Ministério Público de São Paulo. Relator: Min. Luiz Fux. Acórdão em: 12/08/2014. Disponível em: <<http://portal.stf.jus.br/processos/downloadPeca.asp?id=250796864&ext=.pdf>>. Acesso em: 22 fev. 2020.

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

COELHO, Yuri Carneiro. **Curso de Direito Penal Didático.** vol. único, 2ª ed. – São Paulo: Atlas, 2015.

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: 19 fev. 2020.

FEITOZA, Luis Guilherme de Matos. **Crimes Cibernéticos:** o Estelionato Virtual. Brasília, 2012. Disponível em:< https://egov.ufsc.br/portal/sites/default/files/crimes_ciberneticos_o_estelionato_virtual.pdf> Acesso em: 19 fev. 2020.

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: 19 fev. 2020.

FUX, Luiz. Decisão. In. BRASIL. Supremo Tribunal Federal. **Ação Cível Originária 2.361 São Paulo.** Autor: Ministério Público de Minas Gerais. Réu: Ministério Público de São Paulo. Relator: Min. Luiz Fux. Acórdão em: 12/08/2014. Disponível em:

<<http://portal.stf.jus.br/processos/downloadPeca.asp?id=250796864&ext=.pdf>>.
Acesso em: 22 fev. 2020.

GOMES, Luiz Flávio. **Direito penal: parte geral: volume 2.** – São Paulo: Editora Revista dos Tribunais, 2007.

GONÇALVES, Victor Eduardo Rios. **Direito penal esquematizado: parte especial do Código Penal.** - 8. ed. – São Paulo: Saraiva Educação, 2018.

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

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

MATSUYAMA, Keniche Guimarães; LIMA, João Ademar de Andrade. **Crimes Cibernéticos: atipicidade dos delitos.** 2016. Disponível em:<http://www.cedipe.com.br/3cbpj/docs/artigos_pdf/11_crimes_ciberneticos_atipicidade_dos_delitos.pdf>. Acesso em: 20 abr. 2020.

MAUES, Gustavo Brandão Koury et. al. **Crimes Virtuais: uma análise sobre a adequação da legislação penal brasileira.** 2018. Disponível em:<https://www.unirios.edu.br/revistarios/media/revistas/2018/18/crimes_virtuais.pdf>. Acesso em: 20 abr. 2020.

MONTEIRO, Renato Leite. **Crimes eletrônicos: uma análise econômica e constitucional.** Fortaleza, 2010. Disponível em:< <http://www.dominiopublico.gov.br/download/teste/arqs/cp142465.pdf>>. Acesso em: 20 abr. 2020.

MOREIRA, Rômulo de Andrade. **Conflito negativo de atribuições entre os membros do MP.** 2010. Disponível em:< <https://www.migalhas.com.br/depeso/107045/conflito-negativo-de-atribuicoes-entre-membros-do-mp> >. Acesso em: 22 fev. 2020.

NAUATA, Felipe Machado. **Crimes virtuais: estelionato.** 2018. Disponível em:<<https://jus.com.br/artigos/65242/crimes-virtuais-estelionato>>. Acesso em: 19 fev. 2020.

PAGNOZZI, Isadora Marina Catelan de Almeida. **Crimes Virtuais: uma abordagem jurídica acerca das limitações no combate aos crimes cibernéticos.** Curitiba, 2018.

Disponível em:< <https://www.unicuritiba.edu.br/images/tcc/2018/dir/ISADORA-MARINA-CASTELAN-DE-ALMEIDA-PAGNOZZI.pdf>>. Acesso em: 20 abr. 2020.

RIBEIRO, Eliete da Silva. **Crime de Estelionato** – Uma análise da evolução sob a égide da impunidade na cidade de Manaus. 2019. Disponível em: https://semanaacademica.org.br/system/files/artigos/crime_de_estelionato_-_uma_analise_da_evolucao_sob_a_egide_da_impunidade_na_cidade_de_manaus_eliete_da_silva_ribeiro_0.pdf>. Acesso em: 19 fev. 2020.

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

SANTOS, Liara Ruff dos et. al. **Os crimes cibernéticos e o direito a segurança jurídica**: uma análise da legislação vigente no cenário brasileiro contemporâneo. Santa Maria, 2017. Disponível em: < <http://coral.ufsm.br/congressodireito/anais/2017/7-7.pdf>>. Acesso em: 20 abr. 2020.

SHIMABUKURO, Adriana. **Cibercrime**: quando a tecnologia é aliada da lei. São Paulo, 2017. Disponível em:< https://www.trf3.jus.br/documentos/emag/Midias_e_publicacoes/Cadernos_de_Estudos_Crimes_Ciberneticos/Cadernos_de_Estudos_n_1_Crimes_Ciberneticos.pdf>. Acesso em: 20 abr. 2020.

SILVA, Patrícia Santos da. **Direito e crime cibernético: análise da competência em razão do lugar no julgamento de ações penais**. Brasília: Vestnik, 2015.

SPINIELI, André Luiz Pereira. **Crimes informáticos**: comentários ao projeto de Lei nº 5.555/2013. Brasília, 2018. Disponível em:< http://www.mpf.mp.br/atuacao-tematica/ccr2/publicacoes/coletaneas-de-artigos/coletanea_de_artigos_crimes_ciberneticos>. Acesso em: 20 abr. 2020.

WENDT, Emerson; JORGE, Higor Vinícius Nogueira. **Crimes cibernéticos**: Ameaças e procedimentos de investigação. Rio de Janeiro: Brasport, 2012.