CENTRO UNIVERSITÁRIO ASSIS GURGACZ
ROBERTO PEREIRA ROCHA

ESTELIONATO VIRTUAL: CRESCIMENTO E FALTA DE LEIS ESPECÍFICAS

CASCAVEL
2020

CENTRO UNIVERSITÁRIO ASSIS GURGACZ

ROBERTO PEREIRA ROCHA

O ESTELIONATO VIRTUAL: CRESCIMENTO E FALTA DE LEIS ESPECÍFICAS

Artigo apresentado como requisito parcial para obtenção da aprovação semestral no curso de Direito pelo Centro Universitário FAG.

Professor Orientador: Tiago Vidal Vieira.

CASCAVEL
2020

CENTRO UNIVERSITÁRIO ASSIS GURGACZ

ROBERTO PEREIRA ROCHA

O ESTELIONATO VIRTUAL: CRESCIMENTO E FALTA DE LEIS ESPECÍFICAS

Artigo apresentado ao Curso de Direito do Centro Universitário da Fundação Assis Gurgacz como requisito para obtenção do título de Bacharel em Direito, sob a orientação do Professor Tiago Vidal Vieira.

BANCA EXAMINADORA

_____
Orientador Professor Tiago Vidal Vieira
Centro Universitário da Fundação Assis Gurgacz
titulação

_____
prof. avaliador
Centro Universitário da Fundação Assis Gurgacz
titulação

_____
prof. avaliador
Centro Universitário da Fundação Assis Gurgacz
titulação

Cascavel/PR, 08 de junho de 2020.

O ESTELIONATO VIRTUAL: CRESCIMENTO E FALTA DE LEIS ESPECÍFICAS

ROCHA, Roberto Pereira[1]
VIEIRA, Tiago Vidal[2]

RESUMO

O estelionato é um dos crimes praticados no espaço cibernético que requer a análise da legislação e das formas de combate aos crimes virtuais. O objetivo deste trabalho é analisar o crime de estelionato e sua prática virtual buscando adequar o processo investigativo do delito ao ambiente tecnológico para identificar e punir os criminosos com maior rigor e eficácia. Mediante o método de revisão bibliográfica, foram analisados estudos e jurisprudências que indicam que o Código Penal brasileiro não enquadra especificamente o sujeito que comete crime virtual em seus artigos, identificando os tipos penais de forma geral, assim como, as leis existentes são, ainda, esparsas e não abarcam todas as situações que surgiram com o avanço tecnológico e o uso indevido dessas situações. No entanto, o Código Penal contempla o crime de estelionato, que não difere do delito cometido no espaço digital com relação ao tipo penal. Como a Constituição Federal de 1988 afirma que não existe crime sem lei que o defina, as decisões judiciais baseiam-se, muitas vezes, em analogias jurídicas para julgar a existência ou não de ato ilícito e criminalidade, especialmente no caso do estelionato praticado no ambiente virtual. A análise desses estudos leva a concluir que o combate ao crime virtual requer maior educação dos usuários para que conheçam os riscos e saibam identificar possíveis condutas criminosas, assim como, há necessidade de fortalecer o processo de investigação no mundo virtual em busca de soluções efetivas ao combate a esse delito.

Palavras-chave: Internet. Crime. Estelionato. Direito Penal.

THE VIRTUAL STELLIONATE: GROWTH AND LACK OF SPECIFIC LAWS

ABSTRACT

The fraud is one of the crimes practiced in cyber space that requires analysis of legislation and ways to combat virtual crimes. The objective of this work is to analyze the crime of fraud and its virtual practice, seeking to adapt the investigative process of the crime to the technological environment in order to identify and punish criminals with greater rigor and effectiveness. Through the bibliographic review method, studies and jurisprudence were analyzed that indicate that the Brazilian Penal Code does not specifically fit the subject who commits virtual crime in its articles, identifying criminal types in general, as well as, existing laws are still sparse and do not cover all situations that have arisen with technological advances and the misuse of these situations. However, the Penal Code contemplates the crime of fraud, which

[1] Acadêmico do 9º ano do Curso de Direito pela Faculdade Assis Gurgacz – FAG, campus Cascavel. e-mail: rpereirarocha869@gmail.com.
[2] Professor Orientador. Email: Tiago.vidal.vieira@gmail.com.

does not differ from the crime committed in the digital space in relation to the criminal type. As the Federal Constitution of 1988 states that there is no crime without a law that defines judicial decisions, they are often based on legal analogies to judge the existence or not of an illegal act and criminality, especially in the case of fraud committed in the virtual environment. The analysis of these studies leads to the conclusion that the fight against cyber crime requires greater education of users so that they know the risks and know how to identify possible criminal conduct, as well as, there is a need to strengthen the investigation process in the virtual world in search of effective solutions to fight this crime.

Key-words: Internet. Crime. Larceny. Criminal Law.

1 INTRODUÇÃO

Apesar de a Internet ter propiciado facilidades e comodidades ao dia-a-dia da população, os usuários permanecem expostos a uma gama variada de crimes. É fato que os crimes virtuais, também denominados crimes cibernéticos, digitais ou eletrônicos, vêm crescendo avassaladoramente, o que é justificado pelo avanço crescente nas tecnologias de informação, aliadas à difusão cada vez maior de dados e informações por meio da Internet.

Considerando que grande parte da população faz uso de recursos digitais, os criminosos do meio cibernético encontram alvos fáceis para adquirir vantagem. A falta de legislações específicas que tratem da tipificação de crimes virtuais dificulta a investigação dos casos ocorridos e, por isso, alguns tipos delituosos praticados no meio digital se tornam mais difíceis de serem resolvidos. Entre estes, está o estelionato que, embora tipificado no ordenamento penal, tem levantado discussão doutrinária sobre sua ocorrência no meio virtual para fins de penalização do indivíduo que pratica esse delito utilizando-se do meio eletrônico.

Tendo em vista o crescimento do estelionato praticado no meio digital, este estudo levanta a problemática da dificuldade de localização dos criminosos e investigação desse delito em virtude do *modus operandi*, fato este que tem facilitado o recrudescimento da prática e o surgimento de novas vítimas de estelionatários.

Tal prática torna necessária a intervenção do Direito Penal na evolução das tecnologias digitais e virtuais, com o fim de garantir a aplicação das normas penais de forma eficaz na sociedade da informação. Nesse sentido, este trabalho busca maior conhecimento sobre o estelionato praticado no meio virtual, analisando a prática e a forma como esse delito tem sofrido aplicação penal, com o intuito de buscar e propor soluções possíveis em tornar a investigação e punição dos criminosos virtuais mais eficientes.

Essa finalidade é alcançada mediante o uso do método de pesquisa bibliográfica, que considera uma abordagem qualitativa, buscando a compreensão do problema levantado. As referências a autores como: Wendt e Jorge (2012), Nucci (2013), Cassanti (2014), Almeida (2015), Matos (2016), Bueno e Jorge (2019), entre outros, fornecem a base para a análise do tema em comento, mediante a discussão das possibilidades de investigação e punição do crime de estelionato praticado no ambiente virtual.

Nesse sentido, o objetivo dessa pesquisa é analisar o crime de estelionato e sua prática virtual buscando adequar o processo investigativo do delito ao ambiente tecnológico para identificar e punir os criminosos com maior rigor e eficácia. Dentre os objetivos específicos, busca-se definir o estelionato e sua tipificação no Código Penal; conceituar e compreender o que são crimes virtuais; discorrer sobre a prática do estelionato por meio da Internet; analisar a necessidade de serem criadas leis específicas para tipificar o estelionato praticado no ambiente virtual; discutir formas de combate à prática do estelionato virtual com possibilidades de melhoria no processo investigativo.

2 DESENVOLVIMENTO

2.1 SURGIMENTO DA INTERNET E OS CRIMES VIRTUAIS

A Internet, como é conhecida atualmente, teve seu início em meados do século XIX, porém, seu histórico está ligado ao início da Revolução Industrial, que ocorreu no final do século XVIII na Inglaterra e se espalhou no início do século XIX por toda a Europa, período em que houve uma crescente evolução da ciência e da tecnologia, especialmente no campo das tecnologias da comunicação. Isso possibilitou a criação de um sistema global de informatização que mudou a sociedade, causando impacto nas relações sociais, políticas e financeiras do mundo e contribuindo para a globalização (BUENO e JORGE, 2019).

De acordo com Wendt e Jorge (2013), a construção do primeiro computador digital, chamado de ENIAC (*Electronic Numerical Integrator and Computer*), em 1946, deu início à expansão da informática no mundo. Em 1957, o presidente dos Estados Unidos, John Kennedy, propôs a criação da Agência de Investigação de Projetos Avançados (*Advanced Research Project Agency* – ARPA), com a intenção de criar um sistema de defesa e enviar um americano à lua, em vista do fato da antiga União Soviética ter lançado o primeiro satélite artificial no

espaço. No ano seguinte, 1958, foi também criada a Administração Nacional da Aeronáutica e do Espaço (*National Aeronautics & Space Administration* – NASA), que trabalhava com tecnologia mais avançada, utilizando computação interativa e sistemas de tempo compartilhado. A necessidade de conectar informações além das fronteiras, integrando computadores e transmitindo dados que abarcassem diferentes lugares do mundo, levou à criação de uma tecnologia mais específica, capaz de fazer conexões internacionais. Assim foi criada a Agência de Pesquisas em Projetos Avançados na Rede (*Advanced Research Projects Agency Network* – ARPANET).

A ARPANET realizou sua primeira conexão internacional em 1973, interligando a Inglaterra e a Noruega, utilizando o protocolo de comutação de pacotes, chamado de Protocolo de Controle de Rede (*Network Control Protocol* – NCP). Ao final da década de 1970, esse protocolo foi substituído pelo Protocolo de Controle de Transmissão, ou Protocolo de Interconexão (*Transmission Control Protocol/Internet Protocol* – TCP/IP), tornando-se a linguagem básica de comunicação utilizada até os dias atuais. Em 1986, foi criada a Teia Mundial (*World Wide Web* – WWW), um conjunto de documentos em hipermídia que utiliza a Linguagem de Marcação de Hipertexto (*HyperText Markup Language* – HTML), que possibilita a produção de páginas visualizáveis por programas de computados (*browsers*). Então, a ARPANET passou a ser chamada de Internet (WENDT e JORGE, 2013).

Segundo expõe Rutherford (2010), o desenvolvimento da Internet teve como principal objetivo a comunicação entre as bases militares dos Estados Unidos da América, no início da "guerra fria". O governo americano pretendeu criar uma rede de computadores que funcionasse de forma contínua e ininterrupta, mesmo diante de um provável bombardeio. Em 1987, tendo em vista a difusão da tecnologia entre universidades e laboratórios pelo mundo, os EUA liberaram o uso da Internet para diferentes usos, sendo que, na década de 1990, surgiram diversas empresas provedoras de acesso à rede, popularizando essa tecnologia.

Assim, a Internet passou a fazer parte da sociedade mundial, tornando-se uma ferramenta necessária e indispensável a praticamente todos os atos da vida comum. De uma função puramente militar, considerada um meio seguro de comunicar dados sem riscos de estes serem transmitidos ao inimigo, a Internet passou a interligar milhões de computadores, num conglomerado de redes que permitem o acesso a todo tipo de informação e transferência de dados (CASSANTI, 2014; PACHECO, 2019).

No Brasil, a Internet foi introduzida a partir de 1988, pelo Laboratório Nacional de Computação Científica do CNPQ, que conseguiu acesso a uma rede de computadores americana chamada Bitnet, e pela Fapesp, que efetuou a primeira conexão com protocolo de

comunicação. Porém, somente no ano de 1995 foi liberada a Internet para fins comerciais e para o público em geral (MATOS, 2016).

Os benefícios da Internet são destacados por Pinheiro (2007, p. 16), para quem

> A internet veio possibilitar não apenas o encurtamento das distancias com maior eficiência de custos, mas, sobretudo, a multicomunicação, ou seja, transmissão de texto, voz e imagem. A multicomunicação, associada à capacidade de respostas cada vez mais ágeis, permite que a internet se torne o mais novo veículo de comunicação a desafiar o modo como nos relacionamos.

Entretanto, em contrapartida às mudanças sociais, econômicas, políticas e culturais positivas trazidas pelo uso da Internet, que possibilitaram o envio e recebimento de informações, facilitando a vida das pessoas, a Internet passou a facilitar também o cometimento de crimes e delitos diversos, com consequências que chamam a atenção do mundo jurídico. Conforme Jesus e Milagres (2016, p. 17), "a internet é rica, e onde há riqueza, existe crime". Portanto, as facilidades trazidas pela Internet, em especial por proporcionar um certo anonimato e a sensação de impunidade, passaram a estimular a prática de alguns delitos, gerando os chamados "crimes virtuais".

Feitoza (2012), também assinala essa questão, afirmando que:

> [...] o mundo cibernético tem sido alvo da atuação crescente de criminosos, que encontram na internet um meio fácil de cometer crimes, muitas vezes, aproveitando-se do anonimato, o que é vedado pela Constituição Federal, e da falsa impressão de que são impunes, ou pela falta de legislação específica, ou pela dificuldade na investigação criminal em encontrar os autores. É importante ressaltar que os usuários facilitam muito a prática destes ilícitos, tornando-se presas fáceis, pois ao acessar informações bancárias utilizando dados sigilosos, bem como a exposição da imagem, sem os devidos cuidados, acabam por favorecer a criminalidade cibernética (MARTINS, 2010 *apud* FEITOZA, 2012, p. 49).

De fato, evidencia-se que a internet consiste em um meio que possibilita o fácil acesso e transferência de informações pessoais que, sendo utilizadas para fins criminosos, trazem prejuízos aos usuários.

2.2 CRIMES VIRTUAIS: DEFINIÇÃO, CLASSIFICAÇÃO E INSERÇÃO LEGISLATIVA

Os crimes virtuais, também chamados de crimes cibernéticos, digitais ou eletrônicos[3], consistem em atividades delituosas praticadas por meio de rede de computadores e/ou internet, ou dispositivos informáticos em geral (WENDT e JORGE, 2013; CASSANTI, 2014).

Essa definição requer que se reconheça o conceito de crime, para o Direito Penal, que, conforme Nucci (2013) se apresenta numa concepção formal, que é a criminalização de uma conduta mediante a materialização de um tipo penal, o qual é definido em lei, respeitando-se o princípio da legalidade ou reserva legal. Além do conceito formal, a concepção de crime apresenta um conceito analítico, que define o crime como:

> [...] uma conduta típica, antijurídica e culpável, vale dizer, uma ação ou omissão ajustada a um modelo legal de conduta proibida (tipicidade), contrária ao direito (antijuridicidade) e sujeita a um juízo de reprovação social incidente sobre o fato e seu autor, desde que existam imputabilidade, consciência potencial de ilicitude e exigibilidade e possibilidade de agir conforme o direito. (NUCCI, 2013, p. 180).

A problemática dos crimes cometidos pela Internet não foge dessa definição com relação à conduta do criminoso, contudo, a forma como o crime é praticado se diferencia grandemente, posto que o objeto do crime não é somente o bem jurídico em si, mas também a subjetividade da pessoa.

Contudo, os crimes praticados através do meio digital são recentes, com relação ao Código Penal. Conforme Matos (2016), historicamente, os primeiros relatos de crimes realizado por meio da internet datam da década de 1960, sendo estes caracterizados pela manipulação de dados informatizados. Na década de 1970, surge o *hacker*, indivíduo com altas habilidades em programas computacionais e que, à época, não atuava com a intenção de ocasionar danos ao usuário da rede/computador, mas, sim, expor as falhas de segurança dos diferentes sistemas de informação. Nos anos subsequentes, com a popularização e a difusão da internet, sobretudo a partir dos anos 90, observou-se uma elevação crescente no número e na variedade dos delitos cometidos por meio do computador. Tais práticas se tornaram tão difundidas que foi necessário criar legislações para definir e caracterizar os crimes virtuais.

Conforme explica Matos (2016), os crimes cometidos via Internet têm, em geral, a ação dos chamados *crackers*, os quais surgiram concomitantemente aos *hackers*, porém, são considerados os verdadeiros criminosos, por praticarem atividades ilegais por meio do computador, usando técnicas que visam ludibriar as vítimas, que acreditam na veracidade das

[3] Doravante, neste trabalho, considera-se apenas a expressão “crimes virtuais” contemplando as demais expressões.

informações fornecidas pelo criminoso executando ou fornecendo dados vindo, com isso, a sofrer prejuízos ou danos.

Os *crackers*, em geral, utilizam-se de uma técnica conhecida como engenharia social, a qual é conceituada por Wendt e Jorge (2012, p. 1), como "um conjunto de ardis e técnicas utilizadas para ou convencer a vítima a oferecer suas informações sensíveis ou executar algo em seu computador de modo a permitir que o criminoso obtenha alguma vantagem e/ou proporcione algum prejuízo com isso".

Visando coibir a ação de criminosos no meio virtual, em 1999 foi proposto um projeto de lei, PL 84/99, chamado de Projeto Azeredo, cujo teor foi objeto de discussão, críticas, emendas e alterações, até que o texto foi, finalmente, aprovado e transformado na Lei n. 12.735/2012, com vetos, restando apenas 6 dos 22 artigos propostos originalmente. Segundo Feitoza (2012, p. 64), esses vetos se devem ao fato de "algumas condutas extrapolarem os limites da proporcionalidade e razoabilidade exigidas constitucionalmente [...]".

A criação de uma lei que abarque os crimes cibernéticos tem sido objeto de reflexão doutrinária e jurídica em razão de diversos aspectos que permeiam o limite às condutas praticadas no ambiente virtual. Lima (2014), afirma que a criação da Lei n. 12.735/2012 resultante do PL 84/99, foi uma resposta a uma série de ataques de *hackers* e *crackers* a sites oficiais do governo e a empresas públicas, em 2011. Influenciou também nessa criação alguns fatos ocorridos com celebridades que tiveram sua conta hackeada, a exemplo da atriz Carolina Dieckmann. Embora fortemente influenciada pela mídia, confirmou-se, assim, a necessidade de uma legislação específica que combatesse os crimes virtuais.

Na perspectiva de tipificar as condutas ilícitas realizadas no meio virtual, a referida lei, assim como a Lei n. 12.737, também criada em 2012 para normatizar aspectos concernentes a condutas praticadas no meio digital, alterou o Código Penal de 1940, em virtude das mudanças produzidas na sociedade ao longo do tempo e, especialmente, nas últimas décadas, com o evento da Internet, incluindo a tipificação criminal de delitos informáticos, preenchendo algumas lacunas legislativas concernentes à falta de tipificação dos atos ilícitos praticados por meio da Internet e meios digitais (LIMA, 2014).

Contudo, salienta Pinheiro (2007), que não ocorreram mudanças importantes no Código Penal com relação à tipificação de crimes virtuais, já que o conceito de crime, delito, ato e efeito, sejam estes praticados no meio digital ou no meio social, não é diferente no Direito Penal ou no Direito Penal Digital. Segundo o autor, as principais inovações jurídicas percebidas no âmbito do Direito Penal Digital se referem à territorialidade e à investigação probatória; há,

também, a necessidade de tipificar adequadamente algumas condutas, as quais, pela sua peculiaridade, devem ter uma tipificação penal apropriada.

Assim sendo, da mesma forma como ocorre no Direito Penal, os crimes cometidos no meio digital são classificados em dois tipos principais: próprios e impróprios, diferenciando pelo meio como estes são praticados.

Conforme Matos (2016, p. 23), crimes virtuais impróprios podem ser compreendidos como "toda conduta ilícita nas quais o computador serviu de instrumento para o cometimento de um delito, sem, contudo, lesar a inviolabilidade do sistema de informação". Ou seja, o computador ou a rede de internet consistem na ferramenta utilizada para consumar o crime.

Wendt e Jorge (2013) asseveram que tais delitos não requerem um conhecimento de informática mais avançado, razão pela qual são considerados de fácil execução. Estes autores ainda classificam os crimes virtuais impróprios em crimes cibernéticos abertos, que são aqueles delitos que podem ser realizados com ou sem o uso de computadores.

Dentre os crimes virtuais impróprios (ou crimes cibernéticos abertos), destacados por Matos (2016), é possível citar:

- Crimes contra a honra: previstos nos artigos 138 a 140 do Código Penal, envolvem os casos de calúnia, difamação e injúria. São crimes facilmente cometidos na internet, principalmente por conta da possibilidade de anonimato nas redes sociais e da rapidez na disseminação das informações;

- Crimes contra a liberdade individual: envolve os delitos de ameaça (artigo 147 do Código Penal) e violação de correspondência (artigo 151 do Código Penal), sendo aplicáveis em casos de interceptação de e-mails e mensagens;

- Crimes patrimoniais: destacam-se os crimes de furto mediante fraude (artigo 155 do Código Penal) e estelionato (artigo 171 do Código Penal), foco deste estudo, a ser abordado de forma específica nas seções posteriores;

- Crime de pornografia infantil: diz respeito à produção, comercialização e publicação de fotos ou vídeos de crianças e adolescentes em cenas eróticas na internet, entre outros.

Já os crimes virtuais próprios são "aqueles em que o bem jurídico protegido é a inviolabilidade dos dados informatizados [...]" (MATOS, 2016, p. 31), ou seja, só podem ser praticados por meio de um dispositivo com acesso à internet. Destacam-se:

- Invasão de dispositivo informático: envolve a "violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização [...] do titular do dispositivo ou instalar vulnerabilidade para obter vantagem ilícita" (BRASIL, 2012a);

- Criação e divulgação de programas de computador destrutivos: diz respeito à produção, à distribuição e à venda de dispositivos ou programas de computador com a finalidade de invadir dispositivos informáticos;

- Interceptação telemática legal: envolve a interceptação de comunicações telefônicas e de informática sem autorização judicial ou com objetivos não previstos em lei;

- Falsificação informática: popularmente conhecido como "pirataria digital", diz respeito à reprodução ilegal de programas de computador com fins comerciais sem que o proprietário autorize a realização de tal prática.

É essencial ressaltar que, apesar das situações acima expostas estarem devidamente descritas nas jurisprudências e doutrinas brasileiras, o rápido avanço da internet – em conjunto com o aprimoramento dos crimes virtuais – levam, em muitos casos, à impunidade.

Inellas (2009) discorre sobre tal problemática e afirma que os criminosos atuam de forma mais acelerada que os legisladores – o que não é uma exclusividade do Direito brasileiro. De fato, considerando a falta de legislação específica para cada um dos crimes virtuais, muitos operadores de Direito utilizam o Código Penal para solucionar esses casos, haja vista que "a grande maioria das infrações penais cometidas através da internet pode ser capitulada nas condutas criminosas previstas no Código Penal" (INELLAS, 2009, p. 100).

É certo que, a Lei nº 12.735/2012 determinou, entre outros aspectos, a criação de setores responsáveis pelo combate a ações criminosas provenientes do ambiente virtual (BRASIL, 2012b). De igual forma, a Lei n. 12.695/2014, chamada de Marco Civil da Internet, foi criada com o objetivo de estabelecer princípios, garantias, direitos e deveres para o uso da internet no Brasil tendo em vista respaldar a ação penal sobre a matéria (BRASIL, 2014).

Conforme Teixeira e Chaves (2019), as leis criadas em 2012 que dispunham sobre crimes virtuais tentavam fazer uma alteração no Código Penal visando o combate aos crimes digitais impróprios, que possuem características de crimes comuns envolvendo um *modus operandi* com aparatos tecnológicos. O artigo 4º da Lei n. 12.735/2012 previu uma estruturação da polícia judiciária voltada ao combate à ação delituosa virtual, do que derivou a criação de delegacias especializadas sobre crimes virtuais. Já a Lei n. 12.737/2012 trouxe uma alteração importante no Código Penal, inserindo os artigos 154-A e 154-B em seu texto, tipificando a "invasão de dispositivo informático".

No tocante às alterações trazidas pela Lei n. 12.695/2014, os autores consideram que esta regulou e amparou de modo mais eficiente o uso e os atos cometidos no meio digital, tanto dos seus usuários quanto das pessoas jurídicas que utilizam a Internet. Desse modo, essa lei

possibilitou uma melhor relação entre pessoas físicas e jurídicas, especialmente quanto à proteção do usuário da Internet (TEIXEIRA e CHAVES, 2019).

Contudo, a Lei n. 12.695/2014 não tipificou os crimes cometidos no ambiente virtual, vistos como o principal entrave do problema, consoante as considerações de Silva (2017), embora tenha abordado pontos de relevância no que diz respeito a direitos e garantias constitucionais no âmbito de crimes virtuais. Ademais, embora a legislação brasileira tenha, de certa forma, buscado em alguns momentos agir frente à problemática dos crimes virtuais, entretanto, isso não ocorreu com a mesma destreza observada nos avanços da tecnologia.

Nesse sentido, este autor comenta que, embora essas iniciativas tenham sido empreendidas no campo jurídico brasileiro, ainda há falta de regulamentações e normativas que atuem de forma eficaz no combate aos criminosos virtuais, especialmente pelo fato da dificuldade de investigar e punir os criminosos, o que traz aos usuários da rede a sensação de impunidade e de violação de seus direitos. Um dos delitos que tem aumentado e que chama a atenção na atualidade é o estelionato, em especial porque as fraudes foram facilitadas pela Internet a usuários mal-intencionados.

E, levando em conta as palavras de Cassanti (2014, p. 22), que afirma: “Não haverá o mínimo de possibilidade em obter êxito na luta contra os crimes virtuais se quem pretender vencê-lo primeiramente não puder entendê-lo”, é importante compreender o que é o estelionato, sua tipificação no Direito Penal e sua prática no contexto digital, para, então, analisar possíveis articulações entre o processo investigativo e a efetiva penalização dos indivíduos que cometem esse delito no espaço da Internet.

2.3 O CRIME DE ESTELIONATO E SUAS PARTICULARIDADES

O termo estelionato provém do latim *stellionatus*, que vem de *stellio*, espécie de lagarto africano conhecido como camaleão, e significa trapaceiro, enganador, referindo-se a uma prática criminosa que ocorre quando alguém vende, hipoteca ou cede alguma coisa para mais de uma pessoa, enganando a ambas (CASSANTI, 2014).

O estelionato é uma prática conhecida desde a antiguidade. De acordo com Marques (2009, *apud* FEITOZA, 2012, p. 13), rumores de egípcios que comercializavam animais falsos, simulando peso e tamanho com o intuito de ludibriar ricos e nobres foram constatados por volta de 500 anos antes de Cristo.

Greco (2010, p. 228), afirma que a prática do estelionato existe desde que surgiram as relações sociais, sendo utilizada "para dissimular seus verdadeiros sentimentos e intenções para, de alguma forma, ocultar ou falsear a verdade, a fim de obter vantagens que, em tese, lhe seriam indevidas". O crime de estelionato, assim, se caracteriza por uma conduta que visa obter vantagem ilícita em prejuízo alheio.

Na legislação brasileira, tal delito foi introduzido pelo Código Penal no Título II da parte Especial, referente aos Crimes contra o Patrimônio, compreendendo os artigos 155 ao 183. O estelionato, propriamente dito, é descrito no artigo 171, com o seguinte teor: "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, 1940).

Os sujeitos envolvidos na prática do estelionato são os sujeitos ativo e passivo. Conforme Mirabete (2004), o sujeito ativo do estelionato é a pessoa, ou mais pessoas, que efetiva o delito enganando a vítima para conseguir vantagem sobre ela. Já o sujeito passivo é a pessoa que sofre o dano patrimonial, mediante engano. O autor ainda comenta que o prejuízo pode não necessariamente atingir a vítima, estendendo-se a outros, daí a lei falar em prejuízo alheio e proteger o patrimônio, não exatamente a pessoa em si.

Greco (2017) comenta que, o ordenamento jurídico protege o patrimônio, por ser o bem jurídico tutelado frente ao estelionato. O bem jurídico é o objeto material, composto pelo patrimônio alheio, sejam eles bens móveis ou imóveis, direitos, e outros que possam constituir o objeto do delito material. Já Nucci (2013, p. 796) explica que o objeto material do crime de estelionato "é a vantagem obtida ou a coisa alheia, bem como a pessoa que incide em erro".

Os conceitos trazidos pelo artigo 171 são comentados por Masson (2016), o qual explica que, a vantagem ilícita de que fala o citado artigo, tem relação com o fator econômico, patrimonial, enquanto o prejuízo alheio remete ao prejuízo econômico da vítima. Segundo ele,

> Vantagem ilícita precisa possuir natureza econômica, uma vez que o estelionato é crime contra o patrimônio. É ilícita porque não corresponde a nenhum direito. De fato, se a vantagem for lícita o estelionato cede espaço para o delito de exercício arbitrário das próprias razões. [...] Prejuízo alheio é o dano patrimonial. Não bastando, portanto, a obtenção de vantagem ilícita ao agente. Exige também o prejuízo ao ofendido. (MASSON, 2016, p. 597).

Sobre os demais aspectos, este autor explica que, o artifício pode ser entendido como fraude material, em que o agente engana a vítima utilizando algum instrumento ou objeto, ou um método para disfarçar ou falsificar o produto ou o negócio. Quanto ao ardil, o autor afirma

que este nada mais é que a fraude moral, em que o agente faz uso de uma conversa enganosa, usa de esperteza ou sagacidade para convencer a vítima. Pode, também, ocorrer o estelionato mediante outros meios, sendo estes quaisquer comportamentos ou atitudes que provoquem a vítima ao erro, ou a mantenham no erro, devendo o agente obter a vantagem ilícita e causar dano patrimonial (MASSON, 2016).

Ressalta Feitoza (2012, p. 16), 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. 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.

Ainda sobre os elementos objetivos que compõe o tipo penal estelionato, Nucci (2013) afirma que existem diversas formas de se cometer o delito, sendo a obtenção de vantagem indevida, por indução ou manutenção de alguém em erro a previsão genérica do *caput* do artigo 171. O autor explica que o estelionatário obtém um benefício ou lucro ilícito sobre a vítima, a qual, enganada por aquele, colabora sem perceber que está sofrendo o engano.

Nessa perspectiva, o crime de estelionato somente pode ser praticado mediante dolo, como afirma Greco (2017, p. 488): "o delito de estelionato somente pode ser praticado dolosamente, não havendo previsão para a modalidade de natureza culposa". Essa prática se caracteriza pela fraude, mediante a dissimulação e engano, sem o uso de ameaça ou violência.

Nesse sentido, portanto, o delito de estelionato pode ser classificado de modo sucinto da seguinte maneira:

> Estelionato é um crime comum tanto com relação ao sujeito ativo como sujeito passivo; doloso; material; comissivo e omissivo; (tendo em vista ser possível esse raciocínio através da conduta de manter a vítima em erro); de forma livre (pois que qualquer fraude pode ser usada como meio para a prática do crime); instantâneo (podendo, ocasionalmente, ser reconhecido como instantâneo de efeitos permanentes, quando houver, por exemplo, a perda ou destruição da coisa obtida por meio de fraude); de dano; monossubjetivo; plurissubsistente, transuente ou não transuente (dependendo da forma como o delito é praticado). (GRECO, 2017, p. 487).

O estelionato somente se configura quando se consuma, sendo necessário que a vítima sofra a perda patrimonial. Desse modo, a tentativa da prática do delito é possível, mas a

penalização do ato tem dividido a opinião de doutrinadores e juristas. A favor se posicionou o Superior Tribunal de Justiça, em julgamento do RHC 17.106, entendendo que a tentativa de estelionato não consumada, mas tendo a vítima sido ludibriada, é possível de ser penalizada (PINHEIRO, 2011).

Contudo, a doutrina diverge a respeito. Enquanto Masson (2016) afirma que a tentativa de estelionato pode ser penalizada, estando presente a fraude, o meio fraudulento, o engano e a obtenção de vantagem ilícita, sem, no entanto, causar prejuízo patrimonial, Bitencourt não vê possibilidade de pena na tentativa do delito se não houver o engano da vítima, já que, "quando o agente não consegue enganar a vítima, o simples emprego de artifício ou ardil caracteriza apenas a prática de atos preparatórios, não se podendo cogitar de tentativa de estelionato" (BITTENCOURT, 2008, *apud* PINHEIRO, 2011, p. 11).

Há ainda que comentar sobre a torpeza bilateral, que é a fraude existente em ambas as partes, com ambos os envolvidos querendo obter a vantagem indevida, o que dificulta a análise da existência do delito, mas não o afasta, apesar de ser clara a torpeza da vítima também. Contudo, avalia Masson (2016, p. 551), se a má-fé do agente é verificada, sendo assim, ele deve ser punido, em vista que, enquanto "a reparação civil do dano interessa tão somente à vítima, enquanto a punição do estelionatário interessa a toda a coletividade".

Em vista do exposto, convém ainda diferenciar brevemente o crime de estelionato do crime de furto mediante fraude, em virtude de que essas figuras típicas são confundidas facilmente por terem características semelhantes, especialmente pelo elemento comum a ambas, a fraude, não tendo, no entanto, o mesmo caráter e essência, especialmente no que diz respeito à conduta do criminoso, conforme se analisa a seguir.

2.3.1 Estelionato X furto mediante fraude

Muitos autores comparam o furto praticado mediante fraude com o estelionato. Pinheiro (2011), afirma que, "os traços distintivos são muito sutis e requerem uma detida análise do intérprete para a correta adequação típica da conduta.".

A prática do furto mediante fraude é comparável ao estelionato quando sua prática se utiliza da confiança que alguém tem no agente, ao que este abusa da confiança nele depositada. Esse entendimento advém do artigo 155, parágrafo 4º, II, que qualifica o delito se este for praticado "com abuso de confiança, ou mediante fraude, escalada ou destreza".

Conforme conceito dado por Nucci (2013, p. 749),

> A fraude é uma manobra enganosa destinada a iludir alguém, configurando, também, uma forma de ludibriar a confiança que se estabelece naturalmente nas relações humanas. Assim, o agente que criar uma situação especial, voltada a gerar na vítima um engano tendo por objetivo praticar uma subtração de coisa alheia móvel, incide na figura qualificada.

A fraude, assim, é comum aos dois tipos criminais. Contudo, o furto mediante fraude utiliza-se do engano da vítima, podendo ser empregada tanto para se assenhorear da coisa quanto para dela se apossar. Nesse caso, a vítima não percebe que está sendo furtada, enquanto que, no estelionato, ela é iludida ou enganada, entregando por esse meio seu patrimônio ao agente (PINHEIRO, 2011).

Essa diferença é ressaltada pela Ministra Laurita Vaz, do Superior Tribunal de Justiça, que assim se posiciona:

> O furto mediante fraude não se confunde com o estelionato. A distinção se faz primordialmente com a análise do elemento comum da fraude que, no furto, é utilizada pelo agente com o fim de burlar a vigilância da vítima que, desatenta, tem seu bem subtraído, sem que se aperceba; no estelionato, a fraude é usada como meio de obter o consentimento da vítima que, iludida, entrega voluntariamente o bem ao agente. (BRASIL, 2007).

Dessa forma, embora o furto mediante fraude possa ser qualificado como estelionato, deste se diferencia pela subtração da coisa, sem que haja consentimento ou presunção da vítima, enquanto no estelionato a vítima transfere a coisa ao agente por indução ao erro, entregando o bem voluntariamente, mediante o engodo.

É importante afirmar que, apesar das definições apresentadas, cada delito tipificado como sendo um estelionato deve ser minuciosamente avaliado, a fim de que seja possível determinar sua veracidade e, dessa forma, punir os criminosos. Feitoza (2012), salienta que, embora o Código Penal mencione o crime de estelionato, nada se aborda nele sobre a sua prática por meio de um computador ou outro dispositivo eletrônico conectado à internet.

Entretanto, em virtude de a prática do estelionato ter se estendido aos meios virtuais mediante os avanços técnicos e científicos proporcionados pela expansão da Internet, deve esta ser analisada para obter maior eficácia em sua investigação e consequente punição.

2.4 PRÁTICA DO ESTELIONATO ATRAVÉS DA INTERNET – “ESTELIONATO VIRTUAL”

No gênero crimes virtuais existem várias possibilidades delituosas, sendo uma delas a fraude eletrônica, a qual consiste em enganar a vítima mediante o uso de dispositivos de informática com a intenção de obter vantagens ilícitas e causar transtornos patrimoniais para a vítima com o enriquecimento ilícito do fraudador. Para Wendt e Jorge (2012), as incidências mais comuns de fraudes eletrônicas são: o estelionato (art. 171 CP), o furto qualificado mediante fraude e concurso de agentes (art. 155, §4º, II CP) e a extorsão (art. 158 CP).

Destaca Feitoza (2012) que, assim como ocorre com o crime tipificado no Código Penal, no estelionato virtual é essencial que alguns requisitos estejam presentes, tais como: a denominação legal do crime; a conduta do autor, que deve ser comissiva, omissiva ou dolosa (a conduta culposa não se aplica ao caso do estelionato, já que o estelionatário age sempre com intenção de levar à vítima ao erro); a existência de um dano à vítima. O "estelionato virtual" se diferencia, portanto, do estelionato real, pelo *modus operandi*, que é realizado por meio da internet e não no mundo físico.

Como já comentado anteriormente, os crimes virtuais são realizados por pessoas que possuem um nível de conhecimento mais elevado dos recursos disponibilizados pelas tecnologias de informação e da rede de Internet e que, por conta disso, faz uso de meios mais elaborados para ludibriar suas vítimas (como os *crackers*, por exemplo). Mas, no caso do estelionato, Nauata (2018) chama a atenção para outros tipos mais leigos, que não possuem tanto conhecimento sobre a rede, que também fazem uso desse meio para praticar fraudes.

Jesus e Milagres (2016, p. 57) também alertam para o fato de que "o crime cibernético no Brasil está menos técnico e muito mais criativo", em razão de que os criminosos aproveitam-se da ignorância dos usuários para praticar os delitos.

No ambiente virtual, o estelionatário faz uso de algumas condutas consideradas típicas, como, por exemplo, "encaminhar para um usuário qualquer um e-mail com conteúdo falso", como, por exemplo, a atualização de dados cadastrais bancários, de modo a levar esse usuário a crer que o link é confiável. Tal conduta é amplamente utilizada com a finalidade de se adquirir informações pessoais ou confidenciais do usuário (MARTINS, 2017, p. 23).

Outro exemplo muito utilizado é a venda de produtos *online*. De acordo com Ramos Junior (2008, p. 41), "[...] comete o crime de estelionato o agente que cria a página na internet ou faz anúncios por intermédio de *sites* [...], simulando a venda de produtos com o objetivo de induzir a vítima em erro" e, assim, obtém vantagem econômica a partir de um meio fraudulento. Nesses casos, a fraude é representada por falsas páginas de comércio eletrônico e as vítimas são atraídas pelos baixos preços dos produtos, efetuam o pagamento (normalmente na forma de boletos ou depósitos antecipados), mas nunca chegam a receber o bem adquirido.

Como é possível perceber, os meios eletrônicos provocaram uma mudança na percepção do crime, passando de uma realidade sentida e constatada fisicamente para uma realidade virtual, mais relacionada com os sentimentos das pessoas, contudo, refletida na realidade social, familiar e financeira. Esse tipo criminal é de mais difícil detecção, mas tem causado impacto significativo na sociedade (BUENO e JORGE, 2019).

Imprescindível, portanto, reconhecer a necessidade de uma legislação específica voltada a abranger os crimes virtuais em sua tipificação e punição adequadas. Nesse sentido, no tópico seguinte essa necessidade legislativa é analisada com a intenção de avaliar se a legislação brasileira tem alcançado adequadamente os crimes de fraude eletrônica de modo a facilitar o combate ao estelionato virtual.

2.5 DA (DES)NECESSIDADE DE LEGISLAÇÃO ESPECÍFICA AO COMBATE DO ESTELIONATO VIRTUAL

Com relação aos crimes virtuais, há um debate acerca da necessidade de tipificação dos mesmos para que ocorra a devida punição dos criminosos. A simples adequação dos delitos à tipificação penal do Código Penal brasileiro, como salienta Inellas (2009), não é suficiente, em muitos casos, quando se trata de práticas virtuais.

Contudo, é comum aos operadores do direito valerem-se de analogias ou de adaptações nas leis vigentes para conseguir julgar os casos de estelionato virtual, contudo isso não é possível em todas as situações. Ocorre que, em virtude de, até 2012 não existir uma norma voltada à prática de crimes virtuais no ordenamento brasileiro, essa analogia é justificável, apesar de que, muitos delitos cometidos no meio virtual não estão totalmente em conformidade com os tipos penais encontrados no Código Penal.

A analogia do Código Penal aplicada aos crimes virtuais abarca alguns tipos penais, tais como os citados por Carneiro (2012): calúnia (art. 138); difamação (art. 139); injúria (art. 140); ameaça (art. 147); furto (art. 155); dano (art. 163); apropriação indébita (art. 168); estelionato (art. 171); violação ao direito autoral (art. 184), entre outros contemplados em diferentes legislações brasileiras.

No caso específico da prática do estelionato (art. 171 CP), a doutrina tem entendido que o tipo penal não requer nova tipificação, já que constitui crime contra o bem jurídico, seja realizado na forma física tradicional ou no mundo cibernético, havendo apenas a diferença do *modus operandi* que atua com aparatos tecnológicos (TEIXEIRA e CHAVES, 2019).

Matos (2016, p. 26) afirma que

> O estelionato praticado em ambiente virtual amolda-se perfeitamente na tipificação já prevista em lei, uma vez que a conduta descrita no verbo é realizada pelo infrator, entretanto, este usa dos meios de comunicação disponíveis na internet para convencer a vítima a realizar tarefa que venha a lhe proporcionar vantagem econômica de maneira ilícita, sem manter contato pessoal com a mesma.

A jurisprudência brasileira também tem se posicionado nesse sentido, como demonstra o parecer decisório do Superior Tribunal de Justiça sobre a questão:

> ESTELIONATO. VENDA DE PRODUTO PELA INTERNET. ENVIO DE E-MAIL COM FALSA COMPROVAÇÃO DE PAGAMENTO. CONSUMAÇÃO DO DELITO [...] 1. Situação em que a vítima vendia mercadoria pela internet e, após receber uma falsa confirmação de pagamento por e-mail, remeteu a mercadoria para o endereço do estelionatário, que foi preso em flagrante quando a recebia do agente dos Correios. 2. Nos termos do art. 70 do CPP, a competência será de regra determinada pelo lugar em que se consumou a infração e o estelionato, crime material tipificado pelo art. 171 do CP, consuma-se no momento e lugar em que o estelionatário aufere proveito econômico em prejuízo da vítima. (BRASIL, 2018).

Vale ressaltar que, o Superior Tribunal de Justiça tem feito distinção entre o crime de fraude e o estelionato, considerando que, a venda fraudulenta feita por meio da Internet caracteriza o crime de fraude e, quando ocorre uma operação simples de compra e venda que seja feita mediante fraude isso é tipificado como estelionato. Assim, percebe-se que, mesmo a "jurisprudência deste tribunal superior da justiça comum reflete a dificuldade de estabelecer critério seguro e eficaz quando se está diante de crimes praticados no ambiente virtual, e mais precisamente vinculados à relação de consumo" (TEIXEIRA e CHAVES, 2019, p. 1).

Não obstante, a tipificação dos delitos permanece em conformidade com o estabelecido pelo Código Penal de 1940, levando em conta apenas a diversidade do *modus operandi*. E, nesse sentido, Souza (2018) comenta que, o Código Penal se aplica aos diversos crimes comuns cometidos pela Internet em razão de que o Direito Penal visa a proteção dos cidadãos usuários da Internet e punição do criminoso virtual, este sendo um indivíduo que comete um delito (estelionato), que atua mediante uma conduta ilícita, a de se aproveitar da tecnologia para a prática de crimes já absorvidos pelo Código Penal.

Feitas essas considerações sobre a tipificação e a desnecessidade de nova legislação sobre o estelionato virtual, torna-se ainda essencial discorrer sobre as possibilidades de investigação do crime de estelionato praticado no ambiente virtual. Assim sendo, analisa-se o papel da polícia investigativa e possíveis formas de combate a esse delito, haja em vista seu crescimento e as dificuldades que existem com relação à localização do criminoso, a questões

ligadas ao conhecimento dos usuários e à necessidade de preparo dos profissionais que atuam no processo investigativo, bem como, a melhoria da estrutura de combate ao crime virtual.

2.6 FORMAS DE COMBATE À PRÁTICA DO ESTELIONATO VIRTUAL

Conforme já comentado anteriormente, os criminosos que se utilizam da Internet para praticar o crime tipificado no artigo 171 do Código Penal brasileiro se aproveitam da boa-fé, da vulnerabilidade e, mesmo, da falta de experiência com os recursos digitais. Souza (2018) comenta que não é raro a própria vítima contribuir com o criminoso virtual, pelo seu pouco conhecimento ou falta de preparo sobre o mundo virtual. Dessa maneira, os criminosos fazem uso de *sites* de anúncios, das redes sociais, de aplicativos, entre outros, que facilitam o acesso às vítimas, que, confiantes, não percebem, na maioria das vezes, que estão sendo alvo. Os criminosos, por sua vez, sentem-se protegidos pelo aparente anonimato da rede e pelo fato de que os meios de investigação, nesse ambiente, ainda são morosos ou precários.

Os casos de estelionato em meio virtual são de difícil resolução em virtude de diversos aspectos, podendo-se destacar a dificuldade de localizar o estelionatário em razão da possibilidade de anonimato no uso da Internet. Nesse sentido, Bueno e Jorge (2019, p. 1) analisam os impactos negativos do anonimato da rede, que, diante do novo fenômeno criminal, acaba facilitando a impunidade “pela potencialização dos danos aos bens jurídicos visados, pela facilidade do aprendizado de técnicas criminosas, e pelo favorecimento da cooperação entre indivíduos com propósitos desviantes”.

Outro aspecto que acaba dificultando a investigação dos crimes e localização do criminoso é a questão da territorialidade. Segundo Bueno e Jorge (2019), ao mesmo tempo em que a rede mundial de computadores está presente em todo o mundo, a criminalidade nesse meio alcançou características únicas, de transnacionalidade, universalidade e ubiquidade, haja vista que os delitos cibernéticos podem ser cometidos em qualquer país e em qualquer sistema ou rede computacional, quer sejam estes públicos ou privados.

Dessa forma, dificulta-se a determinação do local da ocorrência do crime, fator considerado de relevância para a instauração de um processo judicial, que preconiza a necessidade de se delimitar o território onde ocorre o crime.

> Para a aplicação da regra da territorialidade é necessário, que se esclareça o lugar do crime, que de acordo com a doutrina penalista e a previsão do art. 6º do Código Penal, corresponde ao local em que o crime tiver sido praticado ou àquele local em que tenha ocorrido o resultado. Portanto, nosso Código Penal, adotou a teoria da ubiquidade, pela qual se entende como lugar do crime, tanto o local da conduta como o do resultado. (ALMEIDA, 2015 p. 11).

Nesse sentido, considerando que, na rede de Internet, o conceito de território foi modificado em vista do comentado acima, e pelo fato da interação entre as pessoas não requerer o espaço físico, a definição do lugar do crime é dificultada, em especial porque não se pode fugir muito da noção de territorialidade, que pressupõe que o crime deve ser consumado no Brasil ou iniciado em território brasileiro com resultado em pais estrangeiro.

Como agravante à resolução de casos de estelionato virtual, Pinheiro (2011) acrescenta o fato de muitos usuários da internet não deterem conhecimentos sobre a ferramenta para transmitir informações essenciais às autoridades, situação agravada pela escassez de recursos para a investigação de crimes do gênero e, sobretudo, pela falta de legislações específicas que tratem do tema em tela.

Nessa perspectiva, considerando o aumento dos crimes virtuais, não apenas do estelionato, embora este seja o objeto em comento, Bueno e Jorge (2019, p. 1) avaliam acertada a preocupação do legislador em "incrementar e qualificar a atividade investigativa – controle social formal de primeira seleção – reconhecendo-a como medida determinante para o eficaz combate aos crimes praticados por meios eletrônicos", responsabilizando também os provedores.

A polícia investigativa, no entanto, se depara com a falta de um sistema legal atualizado e contextualizado com as especificidades tecnológicas, assim como, com equipamentos e dispositivos de ponta, que facilitariam em muito o trabalho de investigação dos crimes e dos criminosos. Bueno e Jorge (2019) acreditam que, para o enfrentamento do crime virtual há necessidade de se exigir do Estado a incrementação de mecanismos de controle social mais eficazes no que diz respeito ao combate a esse fenômeno, bem como, deve-se buscar novas técnicas de percepção, detecção e enfrentamento dos delitos virtuais.

A legislação criada em 2012 contribuiu para que o combate aos crimes virtuais ocorresse com maior desenvoltura, a exemplo da Lei n. 12.735/2012, que, no seu artigo 4º, propôs a estruturação da polícia judiciária criando as delegacias especializadas sobre crimes virtuais, e a Lei n. 12.737/2012, que tipificou "invasão de dispositivo informático" nos artigos 154-A e 154-B. Contudo, Silva (2017) afirma que essas leis, ao lado do Marco Civil da Internet, representam

pouco diante da necessidade de eficácia na atuação ao combate aos criminosos virtuais, em especial devido à dificuldade de investigar e punir os criminosos.

As leis supracitadas são um passo importante, embora ainda débil, em direção à melhoria do processo investigativo de crimes virtuais. O artigo 4º da Lei n. 12.735/2012 dispõe que "os órgãos de polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado" (BRASIL, 2012b).

E o artigo 10 da Lei nº 12.965/2014 assevera a possibilidade de os provedores fornecerem os registros de conexão e de acesso a aplicações pessoais, mediante representação judicial pelo delegado de polícia ou do Ministério Público, assim também, a informação de qualificação pessoal com relação a dados cadastrais pelos provedores, sem necessidade de ordem judicial (BRASIL, 2014).

A responsabilização dos provedores é um passo considerado importante ao processo investigativo dos criminosos virtuais. Nauata (2018) afirma que, para identificar o infrator, é necessário ter o endereço de protocolo de Internet, que é obtido junto aos provedores de acesso. Dados e localidade de acesso também podem ser obtidos junto aos provedores de informações. Contudo, a aquisição de informações junto aos provedores de acesso é complexa e demorada, principalmente em virtude de os provedores entenderem que as informações e dados relacionados aos clientes são sigilosas, preservadas constitucionalmente.

Ainda Nauata (2018) apresenta como um meio de investigação relevante o laudo pericial que, conforme o autor, "é um elemento de grande importância para a concretização dos fatos, sendo que em grande parte dos casos é a única prova palpável do delito". Comenta Nauata que a ineficácia do procedimento de averiguação dos delitos virtuais se deve à falta de responsabilização dos provedores, que deixam de colaborar com a investigação por não guardarem em sua base de informações os dados relacionados a acessos de clientes.

Bueno e Jorge (2019) consideram ser de grande importância para o combate ao crime de estelionato virtual a educação dos usuários da Internet. Afirmam que, para minimizar e combater os crimes no ambiente virtual é imprescindível que se faça um estudo da vítima e seus fatores de vulnerabilidade, aliado ao incremento de políticas públicas voltadas à proteção e garantias de seus direitos.

Em corroboração aos autores citados, Wendt e Jorge (2012), já salientavam que, uma forma eficaz para diminuir a incidência de fraudes eletrônicas é a realização de um trabalho de educação digital dos usuários de computadores e dispositivos de acesso às redes, trabalho este que deve ser feito pela sociedade civil organizada, pelos órgãos públicos e por pessoas

capacitadas. A educação é considerada um meio de combate por proporcionar o conhecimento sobre as principais ameaças que envolvem o uso dos meios digitais, aumentando, assim, os procedimentos preventivos e a segurança no uso da internet.

E, em conclusão ao contexto apresentado, Bueno e Jorge (2019) afirmam que os órgãos de persecução criminal precisam atuar para identificar e responsabilizar os autores de crimes virtuais tomando cuidados para que estes não reincidam. Ao aumentar a possibilidade de identificação da autoria delitiva, é importante que sejam oferecidas capacitações aos integrantes dos órgãos investigativos dos crimes digitais com vistas a potencializar sua atuação de enfrentamento da criminalidade no espaço digital.

3 CONSIDERAÇÕES FINAIS

A análise do tipo penal estelionato cometido em ambiente virtual leva a crer que, em virtude de ser tipificado pelo Código Penal de 1940, não há necessidade de ser criar uma nova tipologia, haja vista que o delito, em si, não se modificou mas sim, a forma e o meio como ele é praticado. A conduta do criminoso continua a ser a mesma tipificada no Código Penal.

A pesquisa demonstra que as leis que tratam dos crimes virtuais, de modo geral, não são, ainda, suficientemente eficientes para abranger todas as condutas, e, nesse sentido, nem todos os tipos delituais persistem no ordenamento jurídico pátrio como passíveis de serem analisados analogicamente. Isso indica que, ainda há necessidade de se refletir o assunto e estudar possíveis legislações que tipifiquem os crimes cometidos no meio digital e auxiliem o processo investigativo dos mesmos.

Consoante ao crime de estelionato, igualmente aos demais crimes virtuais, o processo investigativo dos delitos e dos agentes criminosos é previsto na legislação de 2012, contudo, existe uma grande dificuldade em investigar e, consequentemente, punir os criminosos com rigor e eficácia. Apesar da previsão de uma estrutura policial investigativa dos crimes virtuais, na prática, esta carece, ainda de aprimoramento legal e estrutural para que as ações investigativas sejam realizadas com vias a combater os criminosos que atuam nesse meio.

Dentre os procedimentos que podem facilitar o combate ao crime virtual está a educação dos usuários para que conheçam os riscos e saibam identificar possíveis condutas criminosas. Em especial no caso do estelionato virtual, este ocorre, muitas vezes, com a conivência do usuário, que pode contribuir para a prática por querer tirar alguma vantagem. Mas, geralmente, os criminosos aproveitam-se da boa-fé da vítima.

A aparente impunidade que faz com que aumentem os crimes virtuais deriva do anonimato e da dificuldade de se investigar adequadamente o criminoso. Em grande parte, os provedores de acesso deixam de contribuir para o processo investigativo, resultando em demora na aquisição de dados e informações sobre os estelionatários.

Nessa perspectiva, considera-se necessário que o sistema legal seja atualizado e contextualizado com a tecnologia, bem como, sejam disponibilizados aos investigadores equipamentos e dispositivos de ponta, capacitação adequada e acesso rápido aos provedores de acesso e à justiça, de modo que o combate ao crime virtual e, especificamente, ao estelionato virtual, seja mais eficaz.

REFERÊNCIAS

ALMEIDA, M. P. C. **A evolução no combate aos crimes virtuais**. 2015. 18f. Artigo de Conclusão de Curso (Pós-Graduação em Magistratura) – Escola de Magistratura do Estado do Rio de Janeiro, Rio de Janeiro-RJ, 2015.

BRASIL. **Decreto-Lei nº 2.848**, de 07 de dezembro de 1940. Código Penal. Diário Oficial da União, Rio de Janeiro, RJ, 1940.

BRASIL. **Conflito de competência nº 67.343**. GO (2006/0166153-0). Relatora: Ministra Laurita Vaz. Brasília (DF), 28 de março de 2007. Disponível em: <http://www.mpf.mp.br/ccr2/stj_cc67343_go.pdf>. Acesso em: 07 abr. 2020.

BRASIL. **Lei nº 12.737**, de 30 de novembro de 2012. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências. **Diário Oficial da União**, Brasília, DF, 2012a.

BRASIL. **Lei nº 12.735**, de 30 de novembro de 2012. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências. **Diário Oficial da União**, Brasília, DF, 2012b.

BRASIL. **Lei nº 12.965**, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União, Brasília, DF, 2014.

BRASIL. **Jurisprudência**. Estelionato. S3. Terceira Seção DJe 27/08/2018 – Conflito de Competência CC 160053 SP 2018/0194677-4 STJ. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/busca?q=INTERNET.+ESTELIONATO+(ART.+171%2C+%C2%A7+3%C2%BA%2C+CP)>. Acesso em: 28 abr. 2020.

BUENO, G. M. G.; JORGE, H. V. N. Investigação criminal tecnológica e direitos fundamentais das vítimas de crimes. **Canal Ciências Criminais**, dez. 2019. Disponível em: <https://canalcienciascriminais.com.br/investigacao-criminal-tecnologica-e-direitos-fundamentais/>. Acesso em: 28 mar. 2020.

CARNEIRO, A. G. Crimes virtuais: elementos para uma reflexão sobre o problema na tipificação. **Âmbito Jurídico**, Rio Grande, 15, n. 99, abr. 2012. Disponível em: <https://ambitojuridico.com.br/edicoes/revista-99/crimes-virtuais-elementos-para-uma-reflexao-sobre-o-problema-na-tipificacao/>. Acesso em: 28 abr. 2020.

CASSANTI, M. O. **Crimes virtuais, vítimas reais**. Rio de Janeiro: Brasport, 2014.

FEITOZA, L. G. M. **Crimes Cibernéticos**: o estelionato virtual. 2012. 70f. Monografia (Graduação em Direito) - Universidade Católica de Brasília, Brasília, DF, 2012.

GRECO, R. **Curso de direito penal**: parte especial, v. III. 7. ed. Niterói: Impetus, 2010.

_____. **Código penal**: comentado. 11. ed. Niterói, RJ: Impetus, 2017.

INELLAS, G. C. Z. **Crimes na Internet**. 2. ed. São Paulo: Juarez de Oliveira, 2009.

JESUS, D. de; MILAGRES, J. A. **Manual de crimes informáticos**. São Paulo: Saraiva, 2016.

LIMA, S. P. **Crimes virtuais**: uma análise da eficácia da legislação brasileira e o desafio do direito penal na atualidade. 2014. Disponível em: <https://ambitojuridico.com.br/cadernos/direito-penal/crimes-virtuais-uma-analise-da-eficacia-da-legislacao-brasileira-e-o-desafio-do-direito-penal-na-atualidade/>. Acesso em: 30 mar. 2020.

MARTINS, A. B. S. **Crimes Virtuais**. 2017. 44f. Monografia (Graduação em Direito) – Faculdade de Sabará, Sabará, 2017.

MASSON, C. **Direito penal esquematizado**: parte especial. v. 2. 9. ed. rev. e atual. Rio de Janeiro: Forense: São Paulo, 2016.

MATOS, F. **Crimes Virtuais**: uma análise à luz do ordenamento jurídico pátrio. 2016. 62f. Monografia (Graduação em Direito) – Universidade de Passo Fundo, Lagoa Vermelha, RS, 2016.

MIRABETE, J. F. **Manual de direito penal**. 22. ed. São Paulo: Atlas, 2004.

NAUATA, F. M. Crimes Virtuais: estelionato. **Jus Brasil**, abr. 2018. Disponível em: <https://jus.com.br/artigos/65242/crimes-virtuais-estelionato>. Acesso em: 28 out. 2019.

NUCCI, G. de S. **Manual de direito penal**. 9. ed. rev.at. e ampl. São Paulo: Revista dos Tribunais, 2013.

PACHECO, W. E. P. **Manual de Responsabilização Penal dos Hackers, Crackers, e Engenheiros Sociais**. Disponível em: <https://egov.ufsc.br/portal/conteudo/manual-deresponsabilizacao-penal-de-hackers-crackers-e-engenheiros-sociais>
Acesso em: 15 de set. 2019.

PINHEIRO, P. P. **Direito Digital**. 4. ed. São Paulo: Saraiva, 2007.

PINHEIRO, T. R. **Furto mediante fraude x estelionato**: aspectos penais e repercussão da fraude civil no âmbito criminal. Artigo (Pós-Graduação). Escola de Magistratura do Estado do Rio de Janeiro. Rio de Janeiro, 2011.

RAMOS JUNIOR, H. S. **Estudo sobre a aplicabilidade das leis penais aos crimes informáticos no Brasil**. Rio de Janeiro: ABEAT, 2008.

RUTHERFORD, M. Crimes na internet: falta de normatização, dificuldades na regulamentação e entendimentos sobre o assunto. **JusBrasil**, 2010. Disponível em: <https://mikhail.jusbrasil.com.br/artigos/234313175/crimes-na-internet-falta-de-normatizacao-dificuldades-na-regulamentacao-e-entendimentos-sobre-o-assunto>. Acesso em: 27 mar. 2020.

SILVA, W. C. **A ausência de segurança jurídica na legislação brasileira mediante aos crimes cibernéticos**. 2017. 74f. Monografia (Graduação em Direito) – Fundação Universidade Federal de Rondônia, Cacoal, RO, 2017.

SOUZA, A. P. de. **Internet: a moderna ferramenta para a prática do crime de auxílio ao suicídio.** Trabalho de Conclusão de Curso (Graduação em Direito) - Universidade Paulista. 2018. Disponível em: <https://monografias.brasilescola.uol.com.br/direito/internet-moderna-ferramenta-para-pratica-crime-auxilio-ao-suicidio.htm>. Acesso em: 28 abr. 2020.

TEIXEIRA, F. S.; CHAVES, F. B. **Os crimes de fraude e estelionato cibernéticos e a proteção ao consumidor no e-commerce**. 2019. Disponível em: <https://jus.com.br/artigos/73480/os-crimes-de-fraude-e-estelionato-ciberneticos-e-a-protecao-ao-consumidor-no-e-commerce>. Acesso em: 30 mar. 2020.

WENDT, E.; JORGE, H. V. N. Considerações sobre fraudes eletrônicas e engenharia social. **ASDEP**, 2012. Disponível em: < http://asdep.com.br/artigos-detalhe/consideracoes-sobre-fraudes-eletronicas-e-engenharia-social-autores-del-pol-rs-emerson-wendt-e-del-pol-sp-higor-vinicius-nogueira-jorge>. Acesso em: 01 abr. 2020.

_____. **Crimes cibernéticos**: ameaças e procedimentos de investigação. 2. ed. Rio de Janeiro: Brasport, 2013.