JARDEL THALISSON BASTOS

CRIME CIBERNÉTICO E O ESTELIONATO VIRTUAL

Trabalho de conclusão de curso, apresentado ao Curso de Direito, Departamento de Ciências Sociais Aplicadas da Universidade Regional Integrada do Alto Uruguai e das Missões – Campus Erechim.

Orientador: Professor Me. Glauber Serafini

ERECHIM

2016

AGRADECIMENTOS

Quero agradecer em primeiro lugar a Deus, pela força e coragem durante toda esta longa caminhada.

Agradeço também a todos os professores que me acompanharam durante a graduação.

Dedico aos meus amigos e familiares que foram pessoas importantes e fundamentais em todo esse processo de apoio e aprendizado.

RESUMO

O presente estudo busca estabelecer reflexões sobre os crimes virtuais, que tem crescido constantemente, em função da acessibilidade, e facilidade que a internet oferta. Atualmente, é praticamente impossível viver sem acesso à informação, eis que, isso já faz parte do dia-a-dia do ser humano. Todavia, existem pessoas que não fazem o uso correto dessa tecnologia, e se aproveitam de forma maliciosa para obter vantagem ilícita. O estelionato virtual, é o crime cibernético, com o mesmo fim que o estelionato real tipificado no artigo 171 do Código Penal, obter para sim ou para outrem vantagem ilícita em prejuízo alheio, com apenas uma diferença, o *modus operandi*. O estelionato virtual é praticado através de um recurso informático, onde, mantem a vitima em erro, para obter a vantagem ilícita, e a vitima agindo de boa-fé fica no prejuízo. O ordenamento jurídico, aprovou apenas duas legislações que tipificam crimes cibernéticos as Leis nº 12.735 e 12.737, esta ultima conhecida como a Lei de Carolina Dieckmann, onde um individuo, invadiu o computador, furtou os arquivos pessoas da Atriz global, e ainda publicou suas fotos intimas. Apesar das ambas legislações tratarem da tipificação do crime cibernético, em nenhuma delas foi tipificado o estelionato virtual, e não havendo conduta tipificada não crime, assim garante o inciso XXXIX do artigo 5º da Constituição Federal. Dessa forma, é de suma importância que um novo projeto de lei venha ser desenvolvido, para que assim essa conduta seja tipificada, e consequentemente haver o devido processo legal e a condenação do sujeito passivo. A técnica utilizada é em procedimento bibliográfico e pesquisa documental, sob métodos indutivos e procedimento descritivo.

Palavras Chaves: Crime cibernético. Internet. Estelionato. Estelionato Virtual. Fraude.

ABSTRACT

This study seeks to establish reflections on cybercrime, which has grown steadily, due to the accessibility and ease that the internet offer. Currently, it is virtually impossible to live without access to information, behold, it is already part of day-to-day human being. However, there are people who do not make proper use of this technology, and take advantage maliciously to obtain unfair advantage. The virtual larceny, is cyber crime, with the same purpose as the actual larceny typified in article 171 of the Penal Code, to get yes or others unfair advantage in other people's prejudice, with only one difference, the modus operandi. The virtual larceny is committed through a computer resource where, keep the victim in error, to obtain unfair advantage, and the victim acting in good faith is at a loss. The law, adopted only two laws that criminalize cyber crimes Laws No. 12.735 and 12.737, the latter known as the Law Carolina Dieckmann, where an individual, broke into the computer, stole the files people global Actress, and also published the photos intimate. Despite both laws treat the criminalization of cyber crime, in any of them was typified virtual larceny, and there untyped conduct no crime, thus guarantees the item XXXIX of Article 5 of the Federal Constitution. Thus, it is of paramount importance that a new bill will be developed so that such conduct is typified, and consequently be due process and sentencing of the taxpayer. The technique used is in bibliographic and documentary search procedure under inductive methods and descriptive procedure.

Key words: Cybercrime. Internet. Larceny. Virtual larceny. Fraud.

SUMÁRIO

1 INTRODUÇÃO

O presente trabalho trata sobre o crime cibernético e o estelionato virtual, o qual dentro os vários crimes cibernéticos existentes e vieram ser tipificados com as legislações de nº 12.735 e 12.737. A conduta de estelionato virtual estava no projeto de lei nº 84/99, entretanto foi suprimido do texto até o projeto de lei ser sancionado.

Desde o surgimento da informática e da internet, é praticamente impossível o indivíduo sobreviver sem esses avanços tecnológicos. Os crimes cibernéticos têm crescido constantemente nos últimos tempos, e a legislação penal não pode permanecer ante as novas condutas que vêm surgindo.

Em 2014, foi sancionada a Lei nº 12.965, também conhecida como a Lei do Marco Civil da Internet, que trouxe princípios, direitos, garantias e deveres dos usuários da internet.

O crime de estelionato tipificado no artigo 171 do Código Penal brasileiro, obter para si ou para outra vantagem ilícita mediante ardil, artificio, meio fraudulento em prejuízo de outrem. A principal característica do estelionato é manter a vítima em erro e deixá-la no prejuízo.

No que tange o estelionato virtual, a única diferença havida entre o estelionato virtual e o real, é o modus operandi, pois o virtual necessita do uso de um equipamento de informática. Para este não há qualquer tipificação no ordenamento jurídico, a qual não pode haver qualquer condenação.

Ademais o próprio artigo 5º da Constituição Federal, no seu inciso XXXIX, dispõe que não há conduta sem tipificação e não há condenação sem o devido processo legal. Entende-se, portanto, que não havendo tipificação do crime de estelionato virtual no Código Penal, não há que se falar em crime.

Apesar de a Lei nº 12.737, denominada também de Lei Carolina Dieckmann, esta não abrange os crimes de estelionato virtual, justamente pela peculiaridade de manter a vítima ao erro, e pelo binômio de obter a vantagem ilícita em prejuízo de outrem. Sendo assim, é de suma importância o estudo desse tema, para demonstrar o quanto lei penal ainda permanece defasada quanto aos crimes cibernéticos.

O presente trabalho é com base doutrinar de renomados autores como Nucci e Bitencourt, a qual interpreta minuciosamente o crime de estelionato. Ainda Celso Fiorillo e Christiany Conte relatam a respeito dos crimes virtuais no ambiente digital, e Damásio de Jesus, com maestria, apresenta complementos através do manual de crimes informáticos. E demais outros autores renomados complementam a tese dos principais autores citados.

A técnica utilizada é em procedimento bibliográfico e pesquisa documental, sob métodos indutivos e procedimento descritivo.

O presente trabalho divide-se em 3 seções para uma melhor análise e desenvolvimento. A primeira seção, é analisado o surgimento da internet, de uma forma sucinta demonstra-se a sua evolução até ser de fácil acesso para a toda população. Ainda faz uma breve analise da internet com o direito, comenta-se sobre a Lei do Marco Civil da Internet, e leciona sobre os crimes de informática.

Já na segunda seção, aborda-se o crime de estelionato, tipificado no Código Penal, onde faz-se uma breve analise sobre os sujeitos ativos e passivos, o induzimento e a manutenção da vitima ao erro, uma reflexão sobre a obtenção da vantagem ilícita, o que pode ser a vantagem ilícita, e o prejuízo alheio, e ainda comenta-se sobre os crimes de fraudes equiparados ao estelionatos, que estão dispostos nos incisos I ao VI do §2º do artigo 171 do Código Penal.

E por fim, na ultima seção relata-se o estelionato virtual, onde observa-se que não havendo tipificação quanto a essa conduta, o crime é considerado atípico. E ainda faz-se comentários às Leis de n° 12.735 e 12.737, que tipificaram os crimes cibernéticos no ordenamento jurídico.

2 A INTERNET E OS CRIMES VIRTUAIS

De acordo com o artigo 225 da Constituição Federal de 1988, todos têm direito ao meio ambiente ecologicamente equilibrado, bem de uso comum do povo e essencial à sadia qualidade de vida, impondo-se ao Poder Público e à coletividade o dever de defendê-lo e preservá-lo para as presentes e futuras gerações.

Ora, o que tem a haver o meio ambiente com a internet? Tudo. Baseando-se na definição da Lei Federal nº 6.938 de 31 de Agosto de 1981, mais precisamente no seu artigo 3º, inciso I, define o meio ambiente como o conjunto de condições, leis, influências e interações de ordem física, química e biológica, que permite, abriga e rege a vida em todas as suas formas.

Ante a definição de meio ambiente acima, fazendo uma associação com o ambiente digital, (internet) todos têm o direito a uma informação segura, bem como possui o direito de segurança à suas informações, de não serem expostas neste ambiente digital, não é mesmo?

Atualmente, é praticamente impossível viver em um mundo onde não há qualquer tipo de comunicação, principalmente a comunicação virtual, aquela que em apenas um “click” lhe atualiza de tudo o que está acontecendo no mundo.

Fiorillo e Conte (2016), conseguem expressar em sua obra a evolução da sociedade e a necessidade destas para com o meio ambiente digital.

> Inviável discutir o advento da Sociedade da Informação sem colocar em posição de destaque a Internet, bem como seus reflexos na própria realidade jurídica da coletividade. As tecnologias de informação e comunicação, especialmente a Internet, trouxeram a necessidade de um novo olhar sobre velhos direitos, tais como: à informação, à comunicação, à liberdade de expressão e à privacidade, bem como o questionamento sobre o surgimento de novos bens que demandam uma tutela jurídica específica (como no caso da denominada Segurança Informática, que abarca a integridade das informações lançadas na rede mundial de computadores, a disponibilidade de acesso e a confidencialidade das informações).(FIORILLO; CONTE, 2016, p.14)

A internet passou a ser um dos principais instrumentos de trabalho do ser humano, esta não tem a função apenas de relacionar ou interligar as pessoas, ou seja, com a internet veio uma gama de informações, recursos, documentos e serviços que passaram a fazer parte da rotina do indivíduo.

A partir destas informações, passa-se a estudar conceito e a origem da internet, bem como o marco civil desta, e os principais crimes virtuais.

2.1 CONCEITO E ORIGEM

A renomada autora Liliana Minardi Paesani (2013), traz um conceito atual sobre a internet na sociedade:

> Hoje, a Internet é vista como um meio de comunicação que interliga dezenas de milhões de computadores no mundo inteiro e permite o acesso a uma quantidade de informações praticamente inesgotáveis, anulando toda distância de lugar e tempo. (PAESANI, 2013, p. 10-11)

A internet surgiu na década de 60, durante a Guerra Fria, apenas com a intenção militar:

> A Internet surgiu durante os anos 60, nos Estados Unidos, na época da Guerra Fria. O Departamento de Defesa americano pretendia criar uma rede de comunicação de computadores em pontos estratégicos. A intenção era descentralizar informações valiosas de forma que não fossem destruídas por bombardeios se estivessem localizadas em um único servidor. (CÉZAR, 2013)

Como citado acima, a internet surgiu nos Estados Unidos, por uma das subdivisões do Departamento de Defesa, denominado ARPA - *AdvancedResearchProjectsAgency*, como explica os autores Fiorillo e Conte, 2016.

> O experimento financiado pelo Departamento de Defesa dos Estados Unidos e desenvolvido pela Advanced Research Projects Agency (ARPA), através de um de seus departamentos, o Information Processing Techniques Office (IPTO), resultou na primeira forma de comunicação eletrônica entre computadores. Denominada ARPANET, a tecnologia interligou primeiramente os centros universitários da Universidade da Califórnia, em Los Angeles, da Universidade da Califórnia, em Santa Barbara, e da Universidade de Utah, possibilitando a transmissão de telecomunicações on-line. (FIORILLO; CONTE, 2016, p.15).

A ARPANET foi criada para tratar de serviços sigilosos e ainda operava através de diversas privadas, não obstante ainda "possuía a capacidade de conectar os militares e os investigadores sem que eles estivessem em um local fixo, podendo ser encontrados em qualquer lugar que houvesse cobertura a referida tecnologia.", é assim que define, Luiz Guilherme de Matos Feitoza, (FEITOZA, 2012, p. 27).

Na década de 70, a ARPANET foi disponibilizada nas universidades, e na década de 80, o Departamento de Defesa criou a MILNET, pois estava preocupado com as possíveis falhas do sistema de segurança.

> Durante toda a década de 70, a ARPANET foi aperfeiçoada com a ajuda de cientistas e disponibilizada inicialmente para as universidades, até que, em 1983, preocupado com possíveis falhas de segurança, o Departamento de Defesa optou por dividir os objetivos da rede e criou a MILNET, que possuía a mesma função. Enquanto esta teria seu uso reservado ao serviço militar, a primeira permaneceria no uso acadêmico, transformando-se em ARPA-INTERNET. Outras fases de evolução se passaram, como a criação e posterior imposição do protocolo de controle de transmissão TCP/IP. (FIORILLO; CONTE, 2016, p.15)

Como exposto a MILNET foi criada com uma proposito, de dividir as funções de uso de dados com a ARPANET. E na década de 80 foi o fenômeno midiático, que num período de quatro anos atingiu cerca de 50 milhões de pessoas, conforme a informação de Fernando Cézar em 2013.

> Foi o maior fenômeno midiático já criado, em torno de 4 anos a internet atingiu cerca 50 milhões de pessoas. National Science Foundation Network

> era o conjuto de redes universitárias interconectadas, tinha 56 kilobits de por segundo, depois a velocidade passou a ser de 1,5 megabit por segundo. Tanto o HTML (linguagem de marcação e hipertexto), ENQUIRE quanto o World Wide Web foram criados por Tim Berners-Lee da Organização Europeia para Pesquisa Nuclear (CERN), os dois se baseiam no armazenamento de dados e hiperligações. Para saber um pouco mais sobre a importância de Tim Bermers-Lee [...]. (CÉSAR, 2013).

Já no Brasil, a internet chegou de forma lenta, e foi um longo período até ser acessível para a população, entretanto com a aprovação da Lei da Informática - Lei nº 7.232 de 29 de Outubro de 1984,"referendou os princípios básicos de capacitação tecnológica e reserva de mercado e democratizou o processo decisório através da criação do Conselho Nacional de Informática e Automação (CONIN)", é o que conta o autor Paulo Bastos Tigre (TIGRE apud FEITOZA, 2013, p. 33.).

2.2 INTERNET E O DIREITO

A internet passou a ser uma ferramenta de uso importante para o indivíduo, e com isso fez-se necessário que o Direito olhasse de uma outra maneira e evoluísse em relação a essa nova era. Frisa que esta evolução é tão importante para que não se perca a sua real função de disciplinar as relações sociais e impor condutas.

> Vivemos numa sociedade marcada pela denominada Revolução Digital. Conceitos como Internet, aldeia global, espaço virtual e eliminação de fronteiras marcam a realidade social do século XXI. Nesse contexto de realidade virtual, novas relações se consolidam a cada instante, necessitando, dessa maneira, de tutela jurídica, a fim de garantir efetividade e segurança para tais relações. (FIORILLO; CONTE, 2016, p.17)

Ora, a internet permite que as pessoas comuniquem-se de qualquer parte do mundo, e através das redes sociais como *Facebook, Twitter, Orkut,* etc., conheçam novas pessoas e culturas, mas que utilizem esse campo de uma forma sadia.

Com a internet surge um campo chamado ciberespaço, ou seja, é o meio ambiente digital que mencionou-se no inicio deste capitulo, onde neste ciberespaço há um trafego muito rápido de informações sem limite de fronteiras.

Em 1997 o Ministério da Ciência e Tecnologia, pretendia garantir o desenvolvimento do Pais, com a inserção deste no programa da Sociedade da Informação, como narra Fiorillo e Conte:

> O Brasil, por meio do Ministério da Ciência e Tecnologia, estabeleceu, no ano de 1997, um Programa para a Sociedade da Informação, que resultou na edição do Livro Verde da Sociedade da Informação, por meio do qual foram indicadas diversas metas com o fito de inserir o Brasil no contexto da Sociedade da Informação, bem como, dessa forma, garantir o desenvolvimento do País. (FIORILLO; CONTE, 2016, p.19)

Fez-se então necessário a criação de regras, para este ciberespaço, para proteger e garantir os usuários dos seus direitos e deveres, e assim ser um ambiente de uso saudável. Atualmente há duas Leis Federais, que regulam os crimes com a utilização de meios informáticos e outros dispositivos. Essas leis serão tratadas na ultima seção deste trabalho.

Neste instante tratar-se-á do Marco Civil da Internet (MCI), que trouxe, princípios, garantias, direitos e deveres para os usuários da intenet.

2.3 MARCO CIVIL

O Marco Civil da Internet é o nome da Lei federal nº 12.965, de 23 de abril de 2014, a qual regula os direitos de uso, princípios e deveres para os usuários da rede de internet. O projeto de Lei foi aprovado pela Câmara dos Deputados e logo após, foi aprovada pelo Senado Federal, sendo o projeto sancionado, pela então Presidente da República.

A Constituição Federal Brasileira de 1988, já garantia o direito à informação, mais precisamente no artigo 220 caput: “A manifestação do pensamento, a criação, a expressão e a informação, sob qualquer forma, processo ou veículo não sofrerão

qualquer restrição, observado o disposto nesta Constituição.”(BRASIL, Constituição Federal Brasileira, 1988)

A Lei Federal, veio apenas para regularizar os princípios, garantias, direitos e deveres. No artigo 3º da referida Lei, estão os princípios que disciplinam o uso da internet.

> Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:
> I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;
> II - proteção da privacidade;
> III - proteção dos dados pessoais, na forma da lei;
> IV - preservação e garantia da neutralidade de rede;
> V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;
> VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei;
> VII - preservação da natureza participativa da rede;
> VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei. (BRASIL, LEI FEDERAL, 2014)

São princípios que já estão preservados na Constituição Federal, mas que foram regulamentados na Lei Federal para serem inseridos e adaptado no ambiente digital, mas que de forma alguma irá minimizar os princípios exposto na Constituição Federal, assim comenta o autor Celso Fiorillo (2015), ao comentar o parágrafo primeiro do artigo mencionado em supra. Veja:

> O parágrafo único do art. 3o da Lei n. 12.965/2014 procura adaptar o § 2o do art. 5o de nossa Constituição Federal às “especificidades” do uso da internet no Brasil. Verdadeiramente despiciendo, a exemplo de outros dispositivos da lei ora comentada, conforme estamos tendo a oportunidade de aduzir, deve ser observado de qualquer forma em face da supremacia de nossa Carta Constitucional, que prevalece sempre sobre todo e qualquer tratado internacional, conforme já decidiu o Supremo Tribunal Federal (FIORILLO, 2015, p. 39)

O artigo 8º da Lei nº 12.965/2014, trata da garantia ao direito a liberdade de expressão, bem como à privacidade, o qual também está devidamente regularizada

na Constituição Federal, há uma ressalva a ser feita, que consta no parágrafo primeiro do mesmo artigo, o qual declara ser nulas de pleno direito clausulas contratuais que violam o caput do artigo 8º.

Fiorillo e Conte, comentam o artigo 10, §3º da Lei do Marco Civil da Internet, já no seu aspecto penal, onde permite ao Ministério Publico e outras autoridades policiais, o acesso a informações sem uma ordem judicial.

> O art. 10, § 3o, do MCI permite o acesso a dados cadastrais (qualificação pessoal, filiação, endereço) de usuários da rede pelo Ministério Público, pela autoridade policial ou por outras autoridades administrativas, sem necessidade de ordem judicial. Tal possibilidade de acesso já existia para o MP e para a autoridade policial em virtude das leis de lavagem de dinheiro (art. 17-B da Lei n. 9.613/98) e do crime organizado (Lei n. 12.850/2013). (FIORILLO; CONTE, 2016, p. 228)

Não obstante não bastam apenas garantias, princípios, direitos e deveres se não há respeito. Existem indivíduos que se aproveitam da vulnerabilidade da informação na rede, para cometer crimes. A partir desde instante passa-se estudar alguns de tantos crimes virtuais que ocorrem com frequência.

2.4 CRIMES VIRTUAIS

De tudo que foi exposto até o momento, percebe-se que essa evolução da tecnologia, no que diz respeito a informatização, já faz parte do indivíduo, sendo praticamente impossível viver sem essa tecnologia, é como se isso estivesse preso na pessoa não havendo qualquer possibilidade de libertá-lo.

Entretanto, apesar de ser um beneficio para a população, há sujeitos que se aproveitam da vulnerabilidade da informação de dados, e de usuários, e cometem crimes tão gravosos quanto aqueles que empregam o uso da força, é assim que o autor Paulo Marco Ferreira Lima narra em sua obra.

> Todavia, tais benefícios, infelizmente, não apareceram sozinhos, trazendo consigo os crimes e criminosos da era digital, que aumentam em proporção alarmante por todo o mundo. O potencial prejuízo econômico à privacidade e a outros tantos bens jurídicos penalmente tutelados é indiscutível; os computadores adentraram de tal forma em nossa vida cotidiana que se torna irreversível nossa libertação dessa tecnologia. (LIMA, 2011, p.7)

Ainda o referido autor, explana que os criminosos são ocultos, e que os crimes podem afetar diversas pessoas e países.

> Ademais, os criminosos não podem ser facilmente vistos e ouvidos – ocultos estão em um terreno virtual e pouco explorado –, cabendo ainda ressaltar que alguns crimes cometidos por intermédio de computadores podem vir a afetar diversos países e vítimas, por diversas nacionalidades e distintas legislações, sem que o agente criminoso nem ao menos se desloque da segurança de sua casa e covil. (LIMA, 2011, p.7)

Ainda explica que o computador não é perverso, que é apenas um instrumento, possuindo uma pena diferenciada, e tendo uma tipificação especifica.

A preocupação em destaque, é que a norma penal, não é uma norma atual, e "há algo além de uma nova ferramenta, de um novo meio, de um novo modus operandi para cometimento de crimes: estamos também diante de novas condutas não tipificadas." (LIMA, 2011, p. 11).

> Vislumbra-se que uma série de bens jurídicos penalmente tutelados parece ser vítimas de criminalidade informática sem que seja objeto de uma figura típica específica; são ações efetivadas contra a liberdade individual, o direito à intimidade ou ao sigilo das comunicações, entre outras. A nova tecnologia de informação veio expor esses bens de forma mais ampla e abrupta, os dados constantes em um documento eletrônico restam mais desprotegidos que quando restavam somente em um fino pedaço de papel. (LIMA, 2011, p. 11-12)

Pode-se caracterizar os crimes virtuais, como crimes de colarinho branco, ou seja, somente uma pessoa com um amplo conhecimento de informática, é que

possui competência técnica para praticar esse tipo de conduta ilícita, muitas vezes a conduta ilícita está relacionada com o trabalho do criminoso, ou seja, é praticada do próprio instrumento de trabalho.

> São também crimes que começam a se tornar muito sofisticados e relativamente frequentes no âmbito militar, trazendo não só preocupações quanto ao âmbito financeiro, pois é possível imaginar o que a presença de uma conduta maligna em uma central de controles de bombas atômicas poderia fazer. (LIMA, 2011, p. 15)

Os crimes virtuais são sofisticados e vem acontecendo com grande freqüência. Assim o que era um meio para facilitar a vida da população, passou a ser usado como forma de cometer crimes.

Ora, pelo fato de se tratar de crime virtual, é fundamental que o sujeito ativo tenha conhecimentos avançados a respeito das funções e programas da informática, selecionando dessa forma o indivíduo que praticou a conduta ilícita.

2.4.1 Classificação dos Crimes Virtuais

Existem diversas maneiras de cometer um crime virtual, a mais maliciosa é a instalação de vírus, gerando um perigo para as informações no sistema computacional e computadores ligados pela rede.

> O vírus de computador é o malware mais conhecido pelas pessoas, a forma mais conhecida de se cometer ilícitos através da internet. Como o próprio nome sugere, um vírus de computador é um software que infecta o sistema computacional e gera perigo para quem usa máquinas infectadas, contudo não são os únicos malwares existentes. Outros malware bastante comuns são os *trojan horses, os pywares*e os worms. (grifos do autor) (SAMPAIO, 2014, p.18)

Além destes crimes maliciosos, que põem em risco as informações resguardas no sistema computacional, existem crimes praticados contra a moral de

individuo, o mais conhecido é o crime de racismo, havendo também homofobia e humilhações, é uma classificação conhecida como cyberbullying. Entretanto, há também a existência de pornografia infantil, e da pirataria, quando baixa os conteúdos online e depois é comercializado.

Há, também, outras classificações, como por exemplo, os Crimes Econômicos:

- Fraude por manipulação de um computador contra um sistema de processamento de dados;
- Espionagem informática;
- Furto de tempo;
- Intrusão de Sistema;
- Ofensas Tradicionais.

Não pode-se deixar de fora, os crimes de Fraude, executados também de um computador, que afetam a privacidade do cidadão mediante a cumulação, arquivos ou divulgação indevida de dados que estão guardadas no sistema computacional.

E assim se dividem, conforme a Classificação de Lima explica:

> **a) fraudes da matéria corporal, ou dos hardwares:**são as ações criminosas que atingem a integridade física do próprio computador;
> **b) fraudes no nível do input:** também chamadas de manipulação do input, que se revelariam na conduta do agente em alterar dados, omitir ou ingressar dados verdadeiros ou introduzir dados falsos, em um ordenador;
> **c) fraudes no nível do tratamento:** nas quais o delinquente modifica apenas os programas, sem alterar de nenhuma forma os dados eletrônicosali existentes. É tambémpossível interferir no correto processamento da informação, alterando o programa original ou adicionando ao sistema programas especiais que o próprio criminoso introduz;
> **d) fraudes no nível do output:** é o ato de falsear o resultado, inicialmente correto, obtido por um ordenador.(grifos do autor) (LIMA, 2011, p. 19-20)

Não obstante ainda se classificam como puros ou próprios, e impuros ou impróprios, onde sob os ensinamentos de JESUS e SMANIO (JESUS e SMANIO

apud LIMA 2011, p. 20), os puros “seriam aqueles delitos praticados por computador que se realizem ou se consumem também em meio eletrônico; o sujeito ativo visa especificamente danos ao sistema de informática em todas as suas formas (softwares, hardwares, dados e sistemas).”

Já os impuros ou impróprios “seriam aqueles em que o agente se vale do computador como meio para produzir resultado naturalístico que ofenda o mundo físico ou o espaço “real”, ameaçando ou lesando outros bens, não computacionais ou diversos da informática;” (JESUS e SMANIO apud LIMA 2011, p. 20).

Além disso, não se pode deixar de mencionar a classificação do renomado autor mexicano, JulioTellez Valdez (VALDEZ apud LIMA, 2011, p. 20) o qual classifica quanto ao instrumento ou meio, “para o autor, encontram-se as condutas criminais que se valem dos computadores como método, meio para o cometimento do ilícito, exemplificando com a falsificação de documentos via computadorizada (cartões de crédito, cheques etc.);”

E a outra classificação deste autor, é sobre as condutas praticadas contra as máquinas computadorizadas, que são “as condutas criminais que vão dirigidas contra os computadores, seus acessórios ou programas como entidade física, exemplificando com programação de instruções que produzem um bloqueio total ao sistema; destruição de programas por qualquer método;” (Valdez apud Lima, 2011, p. 21).

Tendo um breve conhecimento da história da internet, bem como a origem de crimes cibernéticos e algumas classificações, passa-se, portanto, para o próximo capítulo, para abordar as leis e projetos de leis que regulamente os crimes de internet evidenciar de fato qual o tipo criminal cibernético que se equipara ao crime de estelionato.

3 ESTELIONATO

A origem da palavra estelionato surgiu há vários séculos atrás e era comparado com o réptil Camaleão, animal proveniente da África que tem a sua principal característica a mudança de cor para enganar seus predadores e capturar as suas presas.

Cezar Roberto Bitencourt, 2015, de uma forma técnica, adota o conceito de estelionato das Ordenações Filipinas, o Código Criminal do Império 1830, do Código Penal Republicano de 1890.

O crime de estelionato está tipificado no Código Penal Brasileiro no artigo 171 caput, com a seguinte redação:

> 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 1 (um) a 5 (cinco) anos, e multa.(BRASIL, Código Penal Brasileiro, 1940)

Nota-se que o crime de estelionato é binômio, pois ao mesmo tempo que o autor obtém a vantagem ilícita ele deixa outrem em prejuízo, pois obviamente que se a vantagem fosse licita não seria caracterizado estelionato e sim outros meios maliciosos, ou até mesmo configura uma conduta atípica.

Houve uma evolução nas relações sociais, e consequentemente a vulnerabilidade de informações, dados e bens. O ser humano, maliciosamente, passa-se a se aproveitar descaradamente e ilicitamente, desta vulnerabilidade, causando prejuízo a outrem.

De acordo com Damásio de Jesus (2016, p. 791), o crime de estelionato apenas se configura se “o sujeito empregar engodo para induzir ou manter a vítima em erro, com o fim de obter um indevido proveito patrimonial.”.

Em um conceito mais sociológico, como definir o conceito de criminalidade, ou violência? O autor Antonio Sergio Spagnol, 2013, explana desta maneira:

> O dicionário descreve como crime, segundo um conceito formal, a violação culpável da lei penal, e, segundo o conceito substancial, a ofensa de um bem jurídico tutelado pela lei penal. E também qualquer ato que suscita a reação organizada da sociedade. A criminalidade, portanto, seria o ato do criminoso. (SPAGNOL, 2013, p. 131).

Obviamente, que o crime de estelionato não tem emprego de força e ameaça, entretanto, possui outros meios ardilosos, que o resultado pode ser mais grave que um crime com um emprego de força. Obter uma vantagem ilícita sobre outrem, é tão grave quanto um crime de furto.

Tanto é que a sua pena pode chegar a 5 anos de reclusão, conforme está tipificado no Código Penal Brasileiro.

3.1 SUJEITOS ATIVOS E PASSIVOS

Quem pode ser o sujeito ativo do crime de estelionato? De acordo com o entendimento de Bitencourt (2015), qualquer pessoa pode ser praticante de um crime de estelionato, sem qualquer condição especial.

Assim como já fora mencionado no capitulo anterior, de acordo com o entendimento de Paulo Marco Ferreira Lima (2011), os crimes de computadores, são crimes que exigem um conhecimento técnico do sujeito passivo, podendo inclusive ser denominado como crime de colarinho branco.

Ou seja, se o estelionato for de modo virtual, obviamente que não pode ser praticado por qualquer pessoa. Salienta-se que não se quer desmerecer a capacidade do ser humano, pois no mundo atual, a sociedade está se surpreendendo com o que o indivíduo é capaz, entretanto, quando se trata de um estelionato virtual, é necessário que se tenha um conhecimento técnico de informática bem como as artimanhas para enganar o sujeito passivo.

Sendo assim, para o estelionato virtual, não cabe o entendimento do renomado autor Bitencourt (2014), sendo este um crime de colarinho branco, conforme entendimento de Lima (2011).

Agora, em se tratando de sujeito passivo, este sim pode ser qualquer pessoa, tanto física quanto jurídica, desde que possua capacidade e discernimento, para que seja caracterizado a fraude e consequentemente o crime de estelionato.

De acordo com Cezar Roberto Bitencourt (2015) pode haver dois sujeitos passivos no crime de estelionato:

> Sujeito passivo pode ser, igualmente, qualquer pessoa, física ou jurídica; deve-se destacar que pode haver dois "sujeitos passivos", quando, por exemplo, a pessoa enganada for diversa da que sofre o prejuízo (o empregado sofre o golpe (fraude) do agente, mas quem suporta o prejuízo da ação é o empregador). (BITENCOURT, 2015, p. 834).

Ademais, não se pode esquecer que o bem jurídico protegido é o patrimônio, e o sujeito passivo é o dono deste patrimônio e é este quem sofre a lesão, e ainda deve estar reconhecido o nexo causal entre o crime o patrimônio lesado.

3.2 ADEQUAÇÃO TIPICA DO ESTELIONATO

O caput do artigo 171 do Código Penal Brasileiro dispõe que o crime de estelionato é praticado através de meio ardil, artifícios, meios fraudulentos, manter o sujeito passivo em erro para assim conseguir vantagem ilícita.

Cezar Roberto Bitencourt, interpreta o crime de estelionato desta forma:

> A característica fundamental do estelionato é a fraude, utilizada pelo agente para induzir ou manter a vítima em erro, com a finalidade de obter vantagem patrimonial ilícita. No estelionato, há duplarelação causal: primeiro, a vítima é enganada mediante fraude, sendo esta a causa e o engano o efeito; segundo, nova relação causal entre o erro, como causa, e a obtenção de vantagem ilícita e o respectivo prejuízo, como efeito. (BITENCOURT, 2015, p. 836)

E ainda menciona os requisitos fundamentais para a configuração do crime de estelionato: "1) emprego de artifício, ardil ou qualquer outro meio fraudulento; 2)

induzimento ou manutenção da vítima em erro; 3) obtenção de vantagem patrimonial ilícita em prejuízo alheio (do enganado ou de terceiro).” (BITENCOURT 2015, p. 836).

De acordo com Julio Fabbrini Mirabete, o emprego meio artificio, é quando o sujeito passivo muda o aspecto material da coisa. Veja:

> O artificio existente quando o agente se utiliza de um aparato que modifica, ao menos aparentemente, o aspecto material da coisa, figurando entre esses meios o documento falso outra falsificação qualquer, o disfarce, a modificação por aparelhos mecânicos ou elétricos, filmes efeitos de luz, etc. (MIRABETE, 2003, p 1348).

Bitencourt (2015, p. 836) conceitua o meio artificio de uma forma mais simples, “é toda simulação ou dissimulação idônea para induzir uma pessoa em erro, levando-a à percepção de uma falsa aparência da realidade;”.

No que tange ao meio ardil o mesmo autor, conceitua este como “a trama, o estratagema, a astúcia; qualquer outro meio fraudulento é uma fórmula genérica para admitir qualquer espécie de fraude que possa enganar a vítima.” (Bitencourt 2015, p. 836).

Nas palavras de Nucci o meio ardil significa:

> é também artifício, esperteza, embora na forma de armadilha, cilada ou estratagema. No exemplo dado anteriormente, o agente prepara um local com a aparência de ser uma agência de venda de veículos, recebe o cliente (vítima), oferece-lhe o carro, recebe o dinheiro e, depois, desaparece. Trata-se de um ardil. (NUCCI, 2015, p. 530.)

E ainda não se pode esquecer o meio fraudulento, que nas palavras de Mirabete (2003) caracteriza da seguinte forma:

> Discute-se, na aferição da idoneidade do meio empregado, se deve ser levada em consideração a prudência ordinária, o discernimento do homo medius, ou a pessoa da vítima, concluindo os doutrinadores por esta ultima

> hipótese. Embora já se tenha decidido que as manobras fraudulentas devem ser suficientes para embair a média argúcia, a prudência normal, aquele mínimo de sagacidade que a pessoa comum usa em seus negócios, é francamente predominando a jurisprudência de que a idoneidade do meio deve ser pesquisada no caso concreto, inclusive, tendo-se em vista as condições pessoais da vítima. (MIRABETE, 2003, p.304).

Não obstante o resultado do estelionato é dúplice, como já foram mencionado no inicio desta seção, onde obtém-se a vantagem ilícita o prejuízo alheio, Damásio de Jesus, conceitua de uma forma didática essa teoria

> É necessário que o sujeito, obtendo a vantagem ilícita, venha a causar prejuízo a terceiro. É possível que o sujeito apenas obtenha a vantagem ilícita, mas não cause prejuízo a terceiro. Neste caso, não se pode dizer que ocorreu o resultado do estelionato, respondendo por tentativa do crime. Trata-se de vantagem patrimonial, uma vez que o estelionato é delito contra o patrimônio. A vantagem deve ser ilícita. Se lícita, em regra pode haver o delito do art. 345 do CP. (JESUS, 2015, p.483)

Ora, o meio fraudulento deve ser idôneo para o induzimento da vitima ao erro, pois se o meio fraudulento for relativamente inidôneo pode configurar tentativa de estelionato, e se for absolutamente inidôneo caracteriza crime impossível por absoluta ineficácia ao meio.

3.2.1 Induzimento e/ou manutenção da vítima em erro

De ante mão frisa que apesar de o verbo “induzir” possui o significado de criar uma ideia na cabeça da vítima, ou seja, possuir o mesmo sentido nos crimes praticados contra a vida, este verbo no caso do estelionato é apenas de manter o a vitima em erro.

De acordo com Nucci, (2015, p. 561), o erro no estelionato “é a falsa percepção da realidade. O agente coloca – ou mantém – a vítima numa situação enganosa, fazendo parecer realidade o que efetivamente não é.”.

Bitencourt explica que esta conduta pode ser caracterizada de duas formas

> Na primeira hipótese, a vítima, em razão do estratagema, do ardil ou engodo utilizado pelo agente, é levada ao erro; na segunda, aquela já se encontra em erro, voluntário ou não, limitando-se a ação do sujeito ativo a manter o ofendido na situação equivocada em que se encontra. Em outros termos, a obtenção da vantagem ou proveito ilícito decorre da circunstância de o agente induzir a vítima ao erro ou de mantê-la no estado de erro em que se encontra. Enfim, é possível que o agente provoque a incursão da vítima em erro ou apenas se aproveite dessa situação em que a vítima se encontra. De qualquer sorte, nas duas modalidades comete o crime de estelionato. Mas, parece-nos importante destacar, mesmo na segunda hipótese, a conduta é comissiva, pois para "manter" o agente deve agir positivamente. (BITENCOURT, 2015, p. 837).

Verifica-se que o agende induzindo ou promovendo a manutenção da vitima em erro é crime, mas é importe verificar em qual modalidade o agente utiliza, verificando a ação positivamente.

A característica principal do crime de estelionato é o induzimento e a manutenção do sujeito passivo ao erro, este deve estar agindo de boa-fé em relação à conduta do sujeito ativo.

3.2.2 Vantagem ilícita e prejuízo alheio

O caput do artigo 171, não foi claro ao definir a categoria vantagem ilícita, a doutrina entretanto entende que vantagem ilícita será no seu amplo sentido, ou seja abrange todo e qualquer tipo de vantagem, pode ser de cunho econômico ou não.

Assim afirma Luiz Regis Prado

> Prevalece o entendimento doutrinário de que a referida vantagem não necessita ser econômica, já que o legislador não restringiu o seu alcance como o fez no tipo que define o crime de extorsão, no qual empregou a expressão indevida vantagem econômica. (PRADO, 2002. p. 523)

Como já exposto no tópico anterior, é necessário a caracterização da vantagem ilícita, bem como o prejuízo alheio, sob a hipótese de descaracterizar o crime de estelionato.

Abordando o entendimento de Luiz Regis Prado acima, e analisando os comentários de Cezar Roberto Bitencourt do Código Penal, que também adota o entendimento do autor citado, compara a vantagem ilícita do crime de estelionato com o crime de extorsão mediante sequestro.

Que pelo fato de não estar descrito na norma, qual seria a vantagem (tanto no crime de extorsão, quanto no estelionato), e que isso pode não ter sido um erro do legislador, mas sim um proposito e deixou a expressão “qualquer vantagem” no crime de extorsão e “vantagem ilícita” no crime de estelionato, para se tratar de qualquer vantagem, podendo ser econômica ou patrimonial.

Alias, apesar de ambos fazerem parte do titulo das disciplinas de crimes contra o patrimônio, uma coisa não tem nada a ver com a outra, assim define Bitencourt.

> O argumento de que a natureza econômica da vantagem é necessária, pelo fato de o estelionato estar localizado no Título que disciplina os crimes contra o patrimônio, além de inconsistente, é equivocado. Uma coisa não tem nada que ver com a outra: os crimes contra o patrimônio protegem a inviolabilidade patrimonial da sociedade em geral e da vítima em particular, o que não se confunde com a vantagem ilícita conseguida pelo agente. Por isso, não é a vantagem obtida que deve ter natureza econômica; o prejuízo sofrido pela vítima é que deve ter essa qualidade. (BITENCOURT, 2015, p. 839).

No que diz respeito ao prejuízo alheio, esse além de ser cunho patrimonial, obrigatoriamente deve ser concreto, de acordo com Magalhães Noronha (NORONHA apud BITENCOURT, 2015), prejuízo significa dano, e por se tratar de crime contra o patrimônio, o prejuízo deve ser patrimonial.

> Prejuízo patrimonial não quer dizer somente prejuízopecuniário: a disposição tomada pode consistir na entrega de uma soma em dinheiro, de uma coisa, móvel ou imóvel, de um direito e também de um trabalho que se entenda retribuído, ou de um serviço tarifado. Pode também consistir na renúncia a um direito que positivamente se tem. Deve tratar-se, em todo caso, de um valor economicamente apreciável, sobre o qual incida o direito de propriedade no sentido amplo em que tal direito é entendido pela lei penal. (SOLER apud BITENCOURT, 2015, p. 839)

Não se pode esquecer que a vantagem ilícita é o elemento subjetivo especial do crime de estelionato, onde o principal objetivo para tal é obter a vantagem ilícita para si ou para outrem, ou seja, é querer, é na modalidade dolosa, não admite-se a modalidade culposa para o estelionato.

3.3 EQUIPARAÇÃO AO ESTELIONATO

O parágrafo 2º do artigo 171 do Código penal, elenca nos incisos uma serie de atos ilícitos que se equiparam ao crime de estelionato:

> § 2º - Nas mesmas penas incorre quem:
> **Disposição de coisa alheia como própria**
> I - vende, permuta, dá em pagamento, em locação ou em garantia coisa alheia como própria;
> **Alienação ou oneração fraudulenta de coisa própria**
> II - vende, permuta, dá em pagamento ou em garantia coisa própria inalienável, gravada de ônus ou litigiosa, ou imóvel que prometeu vender a terceiro, mediante pagamento em prestações, silenciando sobre qualquer dessas circunstâncias;
> **Defraudação de penhor**
> III - defrauda, mediante alienação não consentida pelo credor ou por outro modo, a garantia pignoratícia, quando tem a posse do objeto empenhado;
> **Fraude na entrega de coisa**
> IV - defrauda substância, qualidade ou quantidade de coisa que deve entregar a alguém;
> **Fraude para recebimento de indenização ou valor de seguro**
> V - destrói, total ou parcialmente, ou oculta coisa própria, ou lesa o próprio corpo ou a saúde, ou agrava as conseqüências da lesão ou doença, com o intuito de haver indenização ou valor de seguro;
> **Fraude no pagamento por meio de cheque**
> VI - emite cheque, sem suficiente provisão de fundos em poder do sacado, ou lhe frustra o pagamento. (BRASIL, Código Penal Brasileiro, 1940).

A partir deste instante, far-se-á uma breve análise de cada uma das disposições especiais para melhor entendimento.

3.3.1 Disposição de coisa alheia como própria

Disposto no inciso I do parágrafo 2º do artigo 171 do Código penal, é indispensável que esteja presente os mesmo elementos que no estelionato, como a fraude, o mantimento da vitima em erro, a vantagem ilícita e o prejuízo alheio.

Assim como está expresso no texto do inciso, os incidentes incriminadores são vender, permutar, dar em pagamento, locação ou em garantia a coisa alheia. É dispor da coisa alheia como se fosse própria. Bitencourt (2015, p. 842) afirma que "exige-se a má-fé do sujeito ativo e correspondente boa-fé do sujeito passivo; no caso, o comprador é enganado, além do proprietário, é claro."

3.3.2 Alienação ou oneração fraudulenta de coisa própria

Disposto no inciso II do parágrafo 2º do artigo 171 do Código Penal, a diferença entre o inciso I e o inciso II é o objeto material, o que antes era coisa alheia, agora é coisa própria.

Damásio de Jesus (2015), aponta que o sujeito ativo é quem vende permuta, dá em garantia ou em pagamento os objetos materiais da coisa própria móvel ou imóvel, e o sujeito passivo é quem sofre a lesão patrimonial.

As incriminadoras estão gravadas com a inalienabilidade

> Quando "todos os direitos" imanentes ao direito de propriedade reúnem-se na pessoa do proprietário fala-se em dominium plenum. Nem sempre, porém, o dono da coisa dispõe de todos esses atributos da propriedade, sendo uma das restrições possíveis a inalienabilidade, que pode decorrer de lei, convenção ou testamento. Outra restrição ao direito de propriedade, especialmente importante para o direito penal, é a indisponibilidade de coisa gravada de ônus, que nada mais é do que o desmembramen- to de alguns dos direitos que compõem o dominium. (BITENCOURT, 2015, p. 842).

Jesus (2015), define que o crime está no ato do sujeito silenciar sobre a promessa da venda anterior, e não na venda.

3.3.3 Defraudação de penhor

Nesse caso ocorre o estelionato no momento em que o devedor pignoratício, aquele que esta na posse do bem empenhado, defrauda mediante a alienação não consentida pelo credor a garantia empenhada. Defraudar é o mesmo que lesar, privar ou tomar o bem de outrem.

Cezar Roberto Bitencourt ainda complementa:

> A defraudação do penhor para aperfeiçoar-se em sua anatomia jurídica, geralmente prescinde do exame pericial; a exigência, além de estimular a impunidade, seria verdadeira contradicta in reipsa, considerando-se que é da natureza desse ilícito penal o desaparecimento da garantia real representada pelo penhor. O consentimento do ofendido, representando a ausência do elemento normativo do tipo, afasta a tipicidade da conduta do sujeito ativo. (BITENCOURT, 2015, p. 843).

Aqui também há a necessidade do dolo, não existe a modalidade culposa, e principalmente o não consentimento do ofendido, caso contrario o crime torna-se atípico.

3.3.4 Fraude na entrega da coisa

Disposto no inciso IV, do § 2º do artigo 171 do código penal, neste caso o estelionato se configura na fraude da entrega da coisa, ou seja, não se configura da defraudação, mas sim na entrega do bem para o credor. A defraudação ocorre na qualidade ou na quantidade da coisa.

Nucci, no comentário da referido inciso, explana de uma maneira didática este estelionato especial

> [...] substância é a matéria que compõe alguma coisa (ex.: substituir uma joia de diamante por uma de zircônio); qualidade significa a propriedade ou atributo que algo possui (ex.: substituir uma pedra preciosa pura por outra, contendo impurezas); quantidade é a medida em unidades de alguma coisa (ex.: entregar um colar de pérolas, faltando alguns glóbulos). (NUCCI,2015, p. 570)

Nesta modalidade também admite-se apenas como dolosa. Não havendo as prerrogativas impostas, o crime deixa de ser típico deste artigo, e passa a estar tipificado no artigo 275 do Código Penal.

3.3.5 Fraude para o recebimento de indenização ou valor de seguro

Disposto no inciso V do parágrafo 2º do artigo 171, aqui o bem protegido, é o patrimônio do segurador, Paulo José da Costa Junior apud Bitencourt (2015. p. 844) destaca que há duas fraudes executadas com o objetivo de defraudar o seguro: "(1) destruição ou ocultação da coisa própria; (2) lesão do corpo, agravamento de lesão ou moléstia de que esteja acometido."

Nucci faz analise do núcleo do tipo, com as elementares, destruição, ocultação, lesão e agravar.

> [...] destruir significa fazer desaparecer, aniquilar ou extinguir; ocultar quer dizer encobrir ou esconder; lesar significa ofender fisicamente; agravar quer dizer aumentar ou piorar. O tipo é misto alternativo, ou seja, o autor pode destruir, ocultar, lesar ou agravar, além de poder também praticar mais de uma das condutas típicas, como ocultar coisa própria, destr0uindo-a, em seguida, redundando num único delito. (NUCCI,2015,p. 571)

Neste caso o objeto ativo é aquele que possui o objeto ou o corpo segurado, e o sujeito passivo é a seguradora. Assim como nos anteriores, esta modalidade não admite a forma culposa, e o objeto jurídico é o patrimônio do sujeito passivo.

3.3.6 Fraude no meio de pagamento por cheque

Disposto no inciso VI do paragrafo 2º do artigo 171 do Código Penal, sendo esta a ultima modalidade de fraude que se equipara ao crime de estelionato. De acordo com Damásio de Jesus (2015, p. 491), este delito pode ser cometido por intermédio de duas condutas "1.a) emitir cheque sem suficiente provisão de fundos em poder do estabelecimento bancário sacado; 2.a) frustrar o seu pagamento."

Na primeira hipótese o sujeito coloca o cheque em circulação como forma de pagamento, entretanto não há saldo suficiente no banco, já na segunda modalidade, o sujeito até possui a quantia suficiente depositada, entretanto saca esse valor antes mesmo do cheque entrar. É nesse sentido a analise do núcleo do tipo, nas palavras de Nucci:

> [...] emitir cheque significa pôr em circulação o título de crédito; frustrar o pagamento quer dizer iludir ou enganar o credor, evitando a sua remuneração. Esta última conduta pode se realizar de variadas formas: desde a retirada dos fundos existentes na conta, passando pelo encerramento da conta antes da apresentação do cheque até chegar a ponto de determinar a sustação do título de crédito. Note-se que emitir não é equivalente a endossar. Portanto, o beneficiário que, ciente da ausência de fundos, passa adiante o cheque, deve responder por estelionato na modalidade prevista no caput do art. 171. Entretanto, se desde o início estão em conluio emitente e tomador, é natural que haja, nesse caso, concurso de pessoas, e ambos responderão pela figura do inciso VI. O avalista, por sua vez, responde como partícipe, se obrar com má-fé (cf. DIRCEU DE MELLO, Aspectos penais do cheque, p. 122-123 e 125). (NUCCI, 2015, p. 572)

Qualquer pessoa pode ser sujeito ativo, tanto quem emite o cheque, quanto quem frustra, e o sujeito passivo pode ser qualquer pessoa credora. É necessário o dolo.

Em resumo, estelionato é obter a vantagem ilícita, para si ou para outrem em prejuízo de outrem, observou-se, os vários tipos de fraudes que se esquiparam ao crime de estelionato, entretanto há um tipo de crime que está tomando força, os chamados crimes virtuais, e que algumas ilicitudes praticadas se equiparam ao crime de estelionato, é o que trata-se no próximo capítulo.

4 ESTELIONATO VIRTUAL E A APLICABILIDADE DA NORMA PENAL

No capitulo anterior, relatou-se a respeito do estelionato real, tipificado no artigo 171 do Código Penal, bem como os crimes de fraudes que se equiparam ao estelionato. No entanto a partir deste momento, passa-se a relatar sobre o estelionato virtual, um ato ilícito que vem ganhado força na área virtual, e pelo fato de não estar tipificado, inibe o sujeito ativo de praticá-lo.

4.1 ESTELIONATO VIRTUAL

Como verificou-se, no primeiro capitulo, os crimes virtuais vêm crescendo constantemente. A internet é um meio hábil e fácil para o acesso à informação, neste sentido a velocidade dos avanços tecnológicos estão permitindo de certa maneira uma acessibilidade fácil á computadores, e a população sente a necessidade de estar ligada a esse meio informático, usufruindo e compartilhando todo e qualquer tipo de informação.

Embora a tecnologia da informatização tenha vindo para facilitar e agilizar a vida social e profissional do ser humano, há pessoas que se aproveitam da vulnerabilidade da informação e através de meios ardilosos e fraudulentos, obter para si uma vantagem ilícita em prejuízo de outrem.

O Direito por ser uma ciência social aplicada, não pode permanecer inerte ante as condutas virtuais ilícitas, que vem ocorrendo. O Direito deve adaptar-se e trazer novas tipificações a respeitos das condutas virtuais.

Paulo Marcos Ferreira Lima, leciona nesse sentido

> Levando-se em conta também a gravidade que implicam os delitos informáticos, é necessário que o Código Penal inclua figuras delitivas que contenham os crimes de computador, já que a consequência direta de não fazê-lo será a ausência de figuras concretas que possam ser aplicadas nessa matéria, o que pode levar à ausência de punição aos autores desses fatos, ou a obrigar os tribunais a aplicarem preceitos que não se ajustem de forma perfeita à natureza dos fatos cometidos.(LIMA, 2011, p.4)

No capitulo anterior abordou-se a respeito do crime de estelionato, aquele tipificado no artigo 171 do Código Penal, onde o sujeito obtém para si vantagem ilícita em prejuízo do sujeito passivo sob meios artificio, ardil, qualquer outro meio fraudulento.

Entretanto, agora quer-se tratar a respeito do estelionato virtual, crime este executado no ambiente virtual, e que vem crescendo constantemente. Todavia não tipificação expressa a respeito do estelionato virtual, alias a própria legislação penal se mostra inerte quanto a essa questão.

O inciso XXXIX do artigo 5º da Constituição Federal de 1988, garante não há crime sem previsão legal e não há pena sem condenação previa. Entretanto a natureza jurídica deste dispositivo limita a pretensão punitiva estatal, e pelo fato de não existir a tipificação do estelionato virtual no ordenamento jurídico, o sujeito ativo é absolvido da conduta praticada.

Veja como Cezar Roberto Bitencourt, leciona sobre esta interpretação do principio da legalidade:

> O princípio da legalidade ou da reserva legal constitui efetiva limitação ao poder punitivo estatal. Feuerbach, no início do século XIX, consagrou o princípio da reserva legal por meio da fórmula latina nullum crimen, nulla poena sine lege. O princípio da reserva legal é um imperativo que não admite desvios nem exceções e representa uma conquista da consciência jurídica que obedece a exigências de justiça; somente os regimes totalitários o têm negado.(BITENCOURT, 2015, p. 109)

Nesse norte, é necessário também três requisitos essenciais para a composição do fato típico, ou seja, o crime deve ser típico, ilícito e culpável. Ademais, entre a conduta e o dano deve haver o nexo causal. Rogerio Greco, de forma didática explica a respeito do nexo de causalidade:

> O nexo causal, ou relação de causalidade, é aquele elo necessário que une a conduta praticada pelo agente ao resultado por ela produzido. Se não houver esse vinculo que liga o resultado à conduta que levada a efeito pelo agente, não se pode falar em relação de causalidade e, assim, tal resultado

> não poderá ser atribuído ao agente, haja vista não ter sido ele seu causador. (GRECO, 2009, p.294)

Neste sentido, o nexo causal é a relação entre a conduta do sujeito ativo e o dano do sujeito passivo. Faz-se necessário destacar que os crimes de informáticas não são praticáveis por qualquer pessoa, mas sim por quem tem um vasto conhecimento de programas informáticos, que possuem capacidade técnica para esse tipo de conduta.

Fazendo uma breve comparação entre o estelionato virtual e o real, a diferença entre ambos é apenas o *modus operandi*, o qual o virtual emprega o uso de um meio informático. Apenas.

Guilherme Feitoza demonstra como ocorre o estelionato no modo virtual:

> Uma das formas mais recorrentes do estelionato no ciberespaço é a invasão do correio eletrônico da vítima, em particular o daquelas pessoas que possuem o costume de consultar seus saldos e extratos bancários pelo computador. Nesta situação, o estelionatário (*crackler*) encontra alguma maneira de clonar a página legítima do internet banking do usuário e fazer com que ele tente fazer o acesso, sem saber que os dados que estão sendo inseridos serão interceptados por um terceiro de má-fé que irá usá-los indevidamente. (FEITOZA, 2012, p. 48).

Este primeiro meio, é quando estelionatário invade o correio eletrônico da vítima e encontra o meio de clonar a pagina que o sujeito passivo consulta os seus saldos bancários, e deixa esta página para a vítima, induzindo ela ao erro, e assim permite-se que esta disponibilize os dados de acesso acreditando ser a página acessada verdadeira.

A segunda modalidade de estelionato virtual que Guilherme Feitoza narra é a seguinte:

> Outro tipo de estelionato muito comum e executado por pessoas com menor conhecimento informático que o *crackler*são pertinentes a correntes de sorte ou de crenças populares, onde o autor envia inúmeros e-mails para suas vítimas em potencial e conta uma breve história, onde ao final, pede que seja depositada certa quantia em dinheiro para que aquilo versado anteriormente se torne realidade, e garantindo posteriormente o

> ressarcimento do valor dispensado, o que, de fato, não ocorre.(FEITOZA, 2012, p. 48).

A segunda modalidade apresentada, é parecido com o “conto do bilhete”, a maioria das pessoas idosas, caem nas historias contadas pelo sujeito ativo.

4.2 NORMAS DOS CRIMES CIBERNÉTICOS

Com o que fora demonstrado até o momento, viu-se que a legislação encontra-se defasada quantos aos crimes virtuais, que são inúmeros os crimes praticados pela internet.

Tratou-se, brevemente no capitulo anterior, a respeito o Marco Civil da internet, projeto de lei que foi sancionado em 23 de abril de 2014, para garantir os direitos de uso, princípios e deveres dos usuários. Além do Marco Civil da Internet, existem outras duas legislações, que regularizam os crimes virtuais, ambas foram sancionadas em 2012, são as Leis de nº 12. 735 e 12.737.

O crime de estelionato virtual, não foi tipificado em ambas as legislações acima mencionadas. Geralmente o crime de estelionato virtual ocorre na fraude da não entrega da coisa, sendo dessa forma equiparado com o inciso IV do artigo 171 do Código Penal.

Fato, é que a tecnologia virtual vem crescendo constantemente, e a legislação permanece estagnada, sendo necessário que ocorra uma relevante mudança, na atual legislação penal.

4.2.1 Lei Federal nº 12.735

A Lei nº 12.735 de 30 de novembro de 2012, adveio do Projeto de Lei nº 84/99, e promoveu mudanças no Código Penal, bem como no Código Penal Militar. Apesar de no seu preambulo tipifica condutas realizadas mediante o uso de sistema eletrônico, digital, similar, não acrescentou qualquer tipo penal no ordenamento jurídico.

A Lei referida, no artigo 5º, altera o inciso II do parágrafo 3º do artigo 20 da Lei 7.716/89, acrescentando a expressão “eletrônicas ou da publicação de qualquer meio”, ampliando dessa forma outros os meios virtuais como meios para praticar o crime de racismo e discriminação, como refere o caput do artigo.

O Projeto de Lei, desde a sua criação até a votação levou 12 anos, nesse percurso, vários tipos penais que estavam no projeto foram sendo alterados, assim definem Damásio de Jesus e José Antônio Milagres (2016).

Para Fiorillo e Conte (2016), 17 dos 23 artigos que estavam no Projeto de Lei 84/99, foram excluído por trata-se de questões dúbias e polêmicas, e até mesmo por permitir interpretações abrangentes que restringindo a liberdade de uso da Internet. O texto original até o momento de ser sancionado obteve diversas criticas

> O Substitutivo, em seu texto original, recebeu diversas críticas. Ademais, algumas autoridades no assunto afirmavam que, mesmo sendo o projeto aprovado, teríamos outras dificuldades para colocá-lo em prática, uma delas seria a questão da existência de delegacias especializadas, isso porque somente 6 dos 26 Estados da Federação possuem delegacias especializadas em crimes desse tipo. O delegado Ubiraci da Silva, da Delegacia de Crimes Eletrônicos de São Paulo, nesse sentido, é outro crítico do projeto: “a solução não é aumentar a duração das penas, mas melhorar a cooperação entre polícia e provedores.” (FIORILLO; CONTE, 2016, p. 217-218).

Apesar das criticas, o projeto 89/03 foi reativado por meio do acordo de um novo projeto de lei.

> Tal Substitutivo, que parecia estar fadado ao arquivamento, após duas décadas de tramitação sem o apoio necessário para sair do Congresso, finalmente, voltou a ganhar destaque, por meio do acordo proposto em virtude do surgimento de um novo projeto de lei (PL n. 2.793/2011), apresentado pela Câmara. O indicativo mais evidente de que a proposta legislativa do Senador Azeredo não vingaria, em forma de lei, nos foi expressamente declarado pela própria Câmara dos Deputados, haja vista a aprovação, em 15 de maio de 2012, do Projeto de Lei n. 2.793/2011, que tipificava novos crimes cibernéticos. (FIORILLO; CONTE, 2016, p. 218-219)

Como exposto desde o momento da elaboração do projeto até ser sancionado, foram suprimidos diversos artigos, justamente pelo tempo que levou-se para ser aprovado, por causar ambiguidade, e causar interpretações que limitam o uso da internet.

A tipificação do estelionato foi uma das tipificações que foi suprimida o projeto.

> [...] o delito de estelionato, previsto no art. 171 do Código Penal, também seria alterado, para inserir uma disposição relativa àquele que difundisse, por qualquer meio, código malicioso com intuito de facilitar ou permitir acesso indevido à rede de computadores, dispositivo de comunicação ou sistema informatizado. A pena seria a mesma do caput. (JESUS; MILAGRES, 2016, p. 80).

Ora, a inserção do estelionato virtual, não foi recepcionado, por estar tipificado no Código Penal.

4.2.2 Lei Federal 12.737

Conhecida como a Lei de Carolina Dieckmann, foi um projeto de lei que obteve a tramitação mais rápida pelo Congresso Nacional. A Lei dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências.

A Lei acresceu os artigos 154-A e 154-B no Código Penal.

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
> Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos.” (BRASIL, LEI FEDERAL, 2012)

A grosso modo, essa legislação veio para tipificar os crimes cibernéticos, o que já vinha sendo requerido a muito tempo pela população em geral, eis que diversas intimidades já vieram ser protegida, como destaca Eudes Quintino de Oliveira Junior:

> A lei ora apresentada veio com certa demora. A sociedade reclamou a tutela penal da intimidade cibernética durante muito tempo. E com razão. Muitas outras intimidades foram protegidas, tais como a inviolabilidade de domicílio, o sigilo epistolar, o sigilo das correspondências e das comunicações, sigilos das comunicações telefônicas, sigilo bancário e outros. E no mundo digitalizado há a mesma necessidade de se erguer muros protetores. (JUNIOR, 2013)

A impressão que se tem é de que a Lei somente foi sancionada, pois a atriz global, Carolina Dieckmann, teve o seu computador invadido, e seus arquivos pessoais subtraídos, inclusive com a publicação de suas fotos intimas pela rede de internet. Ora, por se tratar de uma pessoa que tem relevância em um mundo artístico, e um nome a zelar, o processo de votação deste projeto de lei acelerou após o fato ocorrido.

Apesar de a lei nº 12.737 inserir dois artigos no Código Penal, Jesus e Malheiros, (2016) entendem que a legislação, na verdade, veio para atender uma demanda no setor financeiro, que foi duramente impactado em virtude dos golpes e fraudes eletrônicas.

Interpretando o caput do artigo 154-A, entende-se que o crime de estelionato virtual está incluído por esta legislação. Todavia, o bem protegido desta conduta é a privacidade, a intimidade a vida privada do sujeito passivo, já no estelionato, o bem protegido é o patrimônio. Ademais, o estelionato exige que o sujeito que o sujeito passivo seja lesado, e o artigo 154-A, não há esta exigência.

Ante esses impasses, evidencia-se que o estelionato virtual não está tipificado na legislação vigente, havendo a extrema necessidade que novas legislações que venham suprir esta lacuna legislativa existente.

5 CONCLUSÃO

No presente trabalho abordou-se a respeitos dos crimes cibernéticos e estelionato virtual, o qual é uma conduta que atualmente não encontra-se tipificada no ordenamento jurídico. Refletiu-se a respeito desta análise, a respeito do principio da legalidade disposto no artigo 5º da Constituição Federal de 1988, mais precisamente no inciso XXXIX, onde está disposto que não há crime sem conduta e não há condenação sem o devido processo legal.

Os objetivos propostos foram de alguma forma cumpridos, onde analisou-se brevemente o surgimento e a evolução da internet, bem como a relação entre a internet e o direito, mencionando a Lei Marco Civil da Internet, e destacando alguns crimes virtuais. Após tratou-se a respeito do crime de estelionato, tipificado no código penal, bem como ressaltou-se os sujeitos ativos e passivos, e equiparação das fraudes ao crime de estelionato.

E o destaque principal do presente trabalho, foi o crime de estelionato virtual, uma conduta virtual, que vem crescendo constante, e não está tipificado no Código Penal. De acordo com o inciso XXXIX do artigo 5º da Constituição Federal, garante que não há crime sem lei, e não há condenação sem o devido processo legal, dessa forma entende-se que o crime de estelionato virtual é um crime atípico.

Fez-se também uma verificação a respeito das leis nº 12.735 e 12.737, ambas sancionadas em novembro de 2012, esta ultima mencionada, também conhecida como lei de Carolina Dieckmann, a qual teve o seu computador invadido, subtraindo seus arquivos pessoais e tendo suas fotos intimas publicadas.

A lei 12.737, alterou o código penal e acrescentou os artigos 154-A e 154-B, em que nestes tipificam a conduta de invasão ao dispositivo informático, para obter, furtar informações e obter vantagem ilícita, contudo a vantagem ilícita não é em prejuízo de outrem, não havendo qualquer possibilidade de enquadrar o estelionato virtual neste tipo penal.

Necessita-se, portanto, de novos projetos de lei, para tipificar as condutas virtuais, que não enquadram-se no artigo 154-A, assim como o estelionato virtual,

que atualmente é um crime atípico, pois cada dia que passa o sujeito ativo encontra novos meios e métodos para infracionar.

Em resumo não há crime sem lei, e não há condenação sem o devido processo legal.

REFERÊNCIAS

BRASIL, **Constituição Federal 1988**, São Paulo: Saraiva, 2016.

BRASIL, **Código Penal Brasileiro 1940**. Disponível em, www.planalto.gov.br, com acesso em 16 de setembro de 2016.

BRASIL, **Lei Federal n° 6.938 de 31 de agosto de 1981**. Disponível em, www.planalto.gov.br, com acesso em 16 de setembro de 2016.

BRASIL, **Lei Federal nº 7.232 de 29 de Outubro de 1984**. Disponível em, www.planalto.gov.br, com acesso em 16 de setembro de 2016.

BRASIL, **Lei Federal nº 12.735 de 30 de Novembro de 2012**. Disponível em, www.planalto.gov.br, com acesso em 16 de setembro de 2016.

BRASIL, **Lei Federal nº 12.737 de 30 de Novembro de 2012**. Disponível em, www.planalto.gov.br, com acesso em 16 de setembro de 2016.

BRASIL, **Lei federal nº 12.965 de 23 de Abril de 2014**. Disponível em, www.planalto.gov.br, com acesso em 16 de setembro de 2016.

BITENCOURT, Cezar Roberto. **Código penal comentado**. 9ª ed. São Paulo: Saraiva, 2015.

CESAR, Fernando. **O surgimento da internet e desenvolvimento até a década de 90**. Disponível em :<http://www.com.ufv.br/cibercultura/o-surgimento-da-internet-e-desenvolvimento-ate-a-decada-de-90/>Acesso em: 01 set. 2016.

FEITOZA, Luis Guilherme de Matos. **Crimes Cibernéticos:** O estelionato virtual. Brasília 2012. Disponível em <http://repositorio.ucb.br/jspui/bitstream/10869/2819/1/Luis%20Guilherme%20de%20Matos%20Feitoza.pdf>Acesso em: 01 set. 2016.

FIORILLO, Celso Antonio Pacheco. **O marco civil da internet e o meio ambiente digital na sociedade da informação**: comentários à Lei nº 12.965/2014. São Paulo: Saraiva, 2015.

FIORILLO, Celso Antonio Pacheco; CONTE, Christiany Pegorari. **Crimes no meio ambiente digital e a sociedade da informação**. 2ª. Ed. São Paulo: Saraiva, 2016.

GRECO, Rogério. **Curso de Direito Penal**. 11 ed. Rio de Janeiro, Iimpetus, 2009.

JESUS, Damásio de. **Direito penal. Parte especial vol. 2** – crimes contra a pessoa a crimes contra o patrimônio público. 35ª ed. São Paulo: Saraiva, 2015.

JESUS, Damásio de; MILAGRE, José Antônio. **Manual de crimes informáticos**. São Paulo: Saraiva, 2016.

JESUS, Damásio de. **Código penal anotado**. 23ª ed. São Paulo: Saraiva, 2016.

JUNIOR, Eudes Quintino de Oliveira. **A nova lei Carolina Dieckmann**. Disponível em: <http://eudesquintino.jusbrasil.com.br/artigos/121823244/a-nova-lei-carolina-dieckmann> Acesso em: 01out.2016.

LIMA, Paulo Marco Ferreira. **Crimes de computador e segurança computacional**. 2ª ed. São Paulo: Atlas, 2011.

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

NUCCI, Guilherme Souza. **Código Penal Comentado**. 15ª ed. São Paulo: Forense, 2015.

PAESANI, Liliana Minardi. **Direito e Internet**: liberdade de informação, privacidade e responsabilidade civil. 6ª ed. São Paulo: Atlas, 2013.

PRADO, Luiz Regis. **Curso de Direito Penal Brasileiro**. Parte Especial - arts. 121 a 183. V. 2. São Paulo: Saraiva, 2002.

SAMPAIO, Mirna Mourão Lôbo. **Invasão de dispositivo informático**: uma analise do novo tipo penal incriminador. Disponível em <http://www.faculdadescearenses.edu.br/biblioteca/TCC/DIR/INVASAO%20DE%20DISPOSITIVO%20INFORMATICO%20UMA%20ANALISE%20DO%20NOVO%20TIPO%20PENAL%20INCRIMINADOR.pdf> Acesso em: 15 set. 2016.

SPAGNOL, Antonio Sergio. **Sociologia jurídica**. São Paulo: Saraiva, 2013.