



Centro Universitário do Distrito Federal – UDF
Coordenação do Curso de Direito

Luiz Carlos de Sales Biasoli

**DA NECESSIDADE DE TIPIIFICAÇÃO DO CRIME DE
ESTELIONATO PRATICADO NA INTERNET**

Brasília
2009

Luiz Carlos de Sales Biasoli

**DA NECESSIDADE DE TIPIIFICAÇÃO DO CRIME DE
ESTELIONATO PRATICADO NA INTERNET**

Trabalho de conclusão de curso
apresentado à Coordenação de Direito do
Centro Universitário do Distrito Federal -
UDF, como requisito parcial para
obtenção do grau de bacharel em Direito.
Orientador: Prof. Valdinei Cordeiro
Coimbra

**Brasília
2009**

Reprodução parcial permitida desde que citada a fonte.

Biasoli, Luiz Carlos de Sales.

Da necessidade de tipificação do crime de estelionato praticado na Internet / Luiz Carlos de Sales Biasoli. – Brasília, 2009.
52 f.

Trabalho de conclusão de curso apresentado à Coordenação de Direito do Centro Universitário do Distrito Federal - UDF, como requisito parcial para obtenção do grau de bacharel em Direito. Orientador: Prof. Valdinei Cordeiro Coimbra

1. Direito Penal. 2. Estelionato. 3. Internet. – Brasil. I. Título

CDU 343.72:004.738.5

Luiz Carlos de Sales Biasoli

**DA NECESSIDADE DE TIPIIFICAÇÃO DO CRIME DE
ESTELIONATO PRATICADO NA INTERNET**

Trabalho de conclusão de curso
apresentado à Coordenação de Direito do
Centro Universitário do Distrito Federal -
UDF, como requisito parcial para obtenção
do grau de bacharel em Direito.
Orientador: Prof. Valdinei Cordeiro
Coimbra

Brasília, _____ de _____ de 2009.

Banca Examinadora

Valdinei Cordeiro Coimbra
Especialista
Centro Universitário do Distrito Federal

Hudson Bruno Maldonado
Especialista
Centro Universitário do Distrito Federal

José de Ribamar da Silva
Especialista
Centro Universitário do Distrito Federal

Nota: _____

*Dedico a Deus que me capacitou na
realização deste trabalho; à minha esposa e
filha, primícias e herança, incentivadoras
da minha prosperidade.*

AGRADECIMENTO

Agradeço primeiramente a Deus, o autor da vida, por mais esta conquista; ao meu orientador, um educador de excelência, por sua dedicação e compreensão; à minha mãe pelo seu apoio; e aos meus amigos que me encorajam.

“Farei do juízo a régua e da justiça, o prumo.”

Isaias 28: 17

RESUMO

Estudo sobre o crime de estelionato praticado na Internet. Apresenta conceituação do crime de estelionato e aplicabilidade penal ao infrator. Traz um breve histórico do surgimento da Internet, bem como se dá a utilização da Internet pela sociedade. Apresenta um breve comentário sobre alguns crimes que são praticados através da Internet. Discorre sobre o crime de estelionato praticado através da Internet e da aplicabilidade penal ao infrator que atualmente tem sido usada, bem como diferencia alguns crimes do estelionato que são praticados na Internet. Apresenta um breve comentário sobre a criação de Projeto de Lei contra os crimes virtuais, bem como aponta alguns crimes cometidos com o uso da Internet que obtiveram proteção legal. Apresenta a existência de Projeto de Lei contra a prática do crime de estelionato praticado na Internet. Discorre sobre a necessidade de tipificação contra o crime de estelionato praticado na Internet, visando a busca da proteção da sociedade contra o prejuízo patrimonial, através de uma definição legal e mais específica para este tipo de crime, e da necessidade de uma punição mais eficaz e inibidora de sua prática.

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

LISTA DE ABREVIATURAS

ARPAnet	<i>Advanced Research Projects Agency Network</i>
CP	Código Penal
CPI	Comissão Parlamentar de Inquérito
DSL	<i>Digital Subscriber Live</i>
IBM	<i>International Business Machines</i>
LAN	<i>Local Area Network</i>
PLC	Projeto de Lei da Câmara
PLS	Projeto de Lei do Senado
TCP/IP	<i>Transmission Control Protocol / Internet Protocol</i>
WAN	<i>Wide Area Network</i>
WI-FI	<i>Wireless Fidelity</i>
WWW	<i>World Wide Web</i>

SUMÁRIO

INTRODUÇÃO	9
1. O CRIME DE ESTELIONATO	11
1.1 Conceito	11
1.2 Aplicabilidade Penal	12
2. A INTERNET E O CRIME VIRTUAL	16
2.1 Breve histórico do surgimento da Internet	16
2.2 Utilização da Internet	18
2.3 Crimes Praticados na Internet	21
3. O CRIME DE ESTELIONATO NA INTERNET	29
3.1 A prática do crime de estelionato na Internet	29
3.2 Outros crimes semelhantes ao estelionato praticado na Internet	30
3.3 Aplicabilidade Penal	33
4. PROJETO DE LEI CONTRA CRIMES VIRTUAIS	34
4.1 Criação de Projeto de lei contra crimes virtuais	34
4.2 Crimes praticados na Internet atualmente alcançados	35
4.3 Projeto de Lei Contra o Crime de Estelionato praticado na Internet	36
5. DA NECESSIDADE DE TIPIFICAÇÃO DO CRIME DE ESTELIONATO PRATICADO NA INTERNET	38
CONCLUSÃO	41
REFERÊNCIA	43
ANEXO	45

INTRODUÇÃO

O crime de estelionato sempre esteve presente em nossa sociedade, trata-se de um crime contra o patrimônio, no qual o estelionatário obtém para si ou para outrem, vantagem ilícita, induzindo ou mantendo alguém em erro.

Pode-se verificar, ao longo da história da sociedade que tal ato criminoso sempre foi combatido; e, com o advento da criação do Estado, os cidadãos outorgaram a este o poder de punir seus infratores.

No Brasil o crime de estelionato está tipificado no artigo 171 do Decreto-Lei nº 2.484 de 07 de dezembro de 1940, o Código Penal Brasileiro.

No entanto com o passar dos anos a sociedade evoluiu, e com ela entramos na era da Informática, e aprendemos a lidar como os computadores, que se mostraram meios eficazes em ajudar o homem em suas atividades, dando celeridade e facilidade em suas tarefas.

Da evolução da Informática surgiu a Internet, produto este que permitiu que todas as pessoas do mundo pudessem acessar uma única rede mundial, e por meio de suas ferramentas passamos a viver de forma virtual, muitas de nossas relações pessoais, profissionais, educativas e consumistas.

Infelizmente, a Internet se deparou com a possibilidade de ser usada para cometimento de crimes, os denominados crimes virtuais.

Dentre todos os crimes cometidos no meio virtual, este trabalho procura analisar o estelionato que tem sido cometido na Internet.

O estelionatário que comete o crime com o uso da Internet, tem a seu favor a possibilidade de dificultar o Estado em puni-lo, uma vez que problemáticas como o desvendamento de autoria, a competência estatal punitiva, a existência de provas da ocorrência do crime, a necessidade de perícia criminal especializada, a manipulação de Protocolo de Internet, dificultam a ação do Estado na descoberta e punição do criminoso.

Há uma real necessidade do estado brasileiro intervir, com o objetivo de acompanhar esta evolução da sociedade, buscando proteger a nossa sociedade contra o ataque virtual destes criminosos estelionatários.

Na busca de solução, este trabalho propõe os seguintes problemas: Há necessidade para a sociedade brasileira de tipificar o crime de estelionato praticado na Internet, trazendo uma nova definição? E ainda, se fazem necessários meios punitivos mais rigorosos aos infratores que se utilizam da Internet para o cometimento do crime de estelionato?

Neste sentido este trabalho tem por objetivo verificar a necessidade de tipificação do crime de estelionato praticado na Internet, bem como a necessidade de aplicação de penas mais severas a seus infratores. Sendo para tanto apresentado, a conceituação e aplicação penal de estelionato, breve histórico da criação e utilização da Internet, alguns crimes virtuais que são praticados com o uso da Internet, o crime e aplicação penal de estelionato eletrônico, bem como sua comparação com alguns semelhantes crimes praticados na Internet, e ainda, projetos de lei contra os crimes virtuais e especificamente contra o crime de estelionato eletrônico, e por fim a necessidade de tipificação do crime de estelionato praticado na Internet.

A metodologia que foi utilizada neste trabalho, para dar suporte ao seu desenvolvimento, consiste em pesquisa bibliográfica, complementada por pesquisa em artigos de notícias atuais, disponíveis na Internet, bem como por pesquisa de projetos de lei em desenvolvimento, que tem como objetivo o combate aos crimes virtuais e especificamente ao crime de estelionato eletrônico.

1. O CRIME DE ESTELIONATO

O crime de estelionato está previsto no artigo 171 do Decreto-Lei nº 2.484 de 07 de dezembro de 1940 – O Código Penal Brasileiro.

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.

Este primeiro capítulo tem como objetivo apresentar o conceito de Estelionato e a sua aplicabilidade legal a qualquer pessoa que cometa tal infração.

1.1 Conceito

O termo estelionato deriva da palavra “estellio”, “onis”, que significa camaleão, lagarto que muda de cor, por meio do mimetismo, assim adaptando-se à cor do ambiente em que se encontra no objetivo de enganar predadores e facilitar a captura de suas presas. Significa dizer que o praticante do crime de estelionato tem como característica se moldar ao meio em que atua, para enganar a vítima, e obter de forma ilícita ganho sobre ela¹.

No nosso ordenamento jurídico o estelionatário é o agente ativo, entendido como sendo qualquer pessoa que cometa o crime de estelionato de forma dolosa, pela livre e consciente vontade.

Tem o estelionatário o objetivo de obter para si ou para outrem, vantagem ilícita, ou seja, benefício contrário ao permitido na lei. Em prejuízo alheio, e aqui, refere-se ao prejuízo da vítima deste crime, que é o agente passivo desta relação, ou seja, aquele que sofre o dano patrimonial.

Este crime é praticado de forma a induzir ou manter alguém em erro, em engano, podendo ser a própria vítima ou pessoa diversa, sendo que, nesta segunda situação teremos um segundo agente passivo do crime de estelionato, que funciona

¹ ESTELIONATO. In: ENCICLOPÉDIA Saraiva do Direito. São Paulo: Saraiva, 1977, p.127.

como um canal para se chegar à vítima principal, a detentora do bem patrimonial a que se quer usurpar².

O crime de estelionato é cometido mediante artifício, ardil, ou qualquer outro meio fraudulento, meio pelo qual o agente ativo ludibria a vítima, seduzindo-a, criando um cenário enganoso, dificultando a percepção da vítima, o que favorece a ação do criminoso em obter a tão vantagem ilícita almejada da vítima.

Segundo o doutrinador Mirabete, “o artifício existe quando o agente se utilizar de um aparato que modifica, ao menos aparentemente, o aspecto material da coisa, figurando entre esses meios o documento falso ou outra falsificação qualquer, o disfarce, a modificação por aparelhos mecânicos ou elétricos, filmes, efeitos de luz etc.”³.

O entendimento de Ardil é imaterial, sendo usado da intelectualidade da vítima, para que esta seja excitada a uma paixão, emoção, convicção ou ilusão, capaz de favorecer a ação ilícita do criminoso de obter o resultado de subtração do bem patrimonial desta vítima, sem que esta se dê conta que está sendo enganada⁴.

1.2 Aplicabilidade Penal

No crime de estelionato é cominado ao infrator pena de reclusão de um a cinco anos e multa.

O acusado de crime de estelionato, desde que não esteja sendo processado ou não tenha sido condenado por outro crime, e ainda, não seja reincidente de crime doloso, como também possua condições satisfatórias quanto à culpabilidade, os antecedentes, a conduta social e a sua personalidade, bem como os motivos e as circunstâncias, previstos pelo artigo 59 do Código Penal, que autorizem a concessão do benefício, poderá beneficiar-se da Suspensão Condicional do Processo prevista no artigo 89, § 1º da Lei 9.099, uma vez que a pena mínima cominada ao crime de estelionato é de um ano.

² MIRABETE, Julio Fabbrini. **Código penal interpretado**. 4. ed. São Paulo: Atlas, 2003, p.1348.

³ Idem. **Manual de direito penal**. 17. ed. Volume 2. São Paulo: Atlas, 2001, p.301.

⁴ CAPEZ, Fernando. **Curso de direito penal**: parte especial: dos crimes contra a pessoa, dos crimes contra o sentimento religioso e contra o respeito aos mortos (arts. 121 a 212), volume 2. São Paulo: Saraiva, 2003, p.471.

Neste caso poderá ser proposto a Suspensão Condicional do Processo pelo Ministério Público no momento em que oferece a denúncia. Cabendo ao acusado aceitar ou não a proposta. E em aceitando, o Juiz suspenderá o processo durante um prazo não inferior a 2 anos e não superior a 4 anos, ficando condicionada o seu cumprimento pelo bom comportamento do acusado, reparando possivelmente o dano causado, não freqüentando determinados lugares proibidos, não se ausentando da comarca onde reside sem prévia autorização do Juiz, comparecendo pessoalmente e justificando suas atividades mensalmente a Juízo, bem como não ser processado por outro crime, casos em que não havendo uma devida justificação aceita pelo juiz implicará na revogação desta suspensão, e conseqüentemente na condenação e no cumprimento da pena⁵.

O réu sendo condenado no crime de estelionato terá a fixação da pena aplicada pelo Juiz, por meio da dosimetria da pena, disciplinado no artigo 68 do Código Penal, tratando-se de um sistema trifásico sendo observado, primeiramente os critérios do artigo 59 deste dispositivo legal, seguido das considerações quanto às circunstâncias atenuantes e agravantes, e por último as causas de diminuição e de aumento da pena⁶.

Na primeira fase deste sistema trifásico de cálculo da pena, temos o cálculo da pena-base, realizada dentre o mínimo e o máximo legal permitido, ou seja, em obediência ao inciso II do artigo 59 do CP. Sendo, no caso do estelionato, o mínimo da pena estabelecida, de 1 ano e o máximo de 5 anos, de acordo com o artigo 171 e assim respeitado o inciso I do artigo 59, como sendo pena aplicável dentre as cominadas pelo ordenamento jurídico⁷.

A análise das oito circunstâncias judiciais disposta pelo artigo 59 do CP, é de suma importância para se chegar a um valor mais justo da pena-base a ser aplicada, para tanto, deve ser analisado, a culpabilidade, ou seja, a importância e participação do crime; os antecedentes, referindo-se a envolvimento do acusado em crimes anteriores; a conduta social, ou seja, o comportamento e vida social do acusado junto à sociedade que o cerca; a personalidade do acusado, observada as circunstâncias do delito e a sua personalidade criminosa; o motivo, quer dizer, o que

⁵ MIRABETE, Julio Fabbrini. **Código penal interpretado**. 4. ed. São Paulo: Atlas, 2003, p. 756.

⁶ SILVA, Jorge Vicente. **Estelionato e outras fraudes**. 1. ed. Curitiba: Juruá, 1995, p. 55.

⁷ MIRABETE, Julio Fabbrini. **Manual de direito penal**. 16 ed. Volume 1. São Paulo: Atlas, 2000, p. 310.

levou o acusado a cometer este delito; as circunstâncias e conseqüências do crime, referindo-se as circunstâncias quanto à forma e o meio com o qual se praticou o crime, e as conseqüências quanto os efeitos produzidos com o crime; o comportamento da vítima, entendendo ser qualquer ação ou omissão praticada pela vítima, de forma que tenha contribuído para que o acusado viesse a praticar o crime contra esta vítima⁸.

Nesta primeira fase, de acordo com a requisição feita pelo inciso III do artigo 59 do CP, se faz necessário ainda a identificação do regime inicial de cumprimento da pena privativa de liberdade, que no caso de estelionato é o de reclusão, trazida pelo próprio artigo 171 do CP.

Por fim, o artigo 59 do CP, em seu inciso VI, trás a possibilidade da substituição da pena privativa de liberdade aplicada, no entanto, se houver dispositivo legal para tanto, o que é positivamente respondido, no caso do crime de estelionato, por meio do parágrafo 1º do artigo 171 do CP, que permite ao réu primário deste crime, caso tenha produzido prejuízo de pequeno valor, a possibilidade do juiz em aplicar o benefício do parágrafo 2º, disposta do artigo 155 do CP, que comina pena ao crime de roubo, e assim possibilitando ao Juiz substituir a pena de reclusão pela de detenção; diminuí-la de um a dois terços; ou aplicar somente a pena de multa.

Na segunda fase da dosimetria da pena, é verificada a situação circunstancial que, conforme o caso, em existindo, aumentará ou diminuirá a pena-base, sendo devidamente disciplinado pelos artigos 61 a 67 do Código Penal Brasileiro.

As circunstâncias que aumentam a pena base são conhecidas como agravantes, dentre elas temos: à reincidência; a ocultação ou qualquer outro meio utilizado para impedir a descoberta do crime; praticado contra ascendente, descendente, irmão ou cônjuge; praticado contra criança, maior de 60 (sessenta) anos, enfermo ou mulher grávida; dentre outros, como ainda no caso do crime ser praticado de concurso de pessoas⁹.

As circunstâncias que diminuem a pena base, são conhecidas como atenuantes, dentre elas temos: ter o acusado na data do crime menos de 21 anos ou

⁸ MIRABETE, Julio Fabbrini. **Manual de direito penal**. 16 ed. Volume 1. São Paulo: Atlas, 2000, p. 292-5.

⁹ Ibidem, p. 295-301.

ter na data da sentença mais de 70 anos; ter o acusado procurado logo após a prática do crime, de livre e espontânea vontade e com eficiência, evitar ou minorar as conseqüências, como ainda ter reparado o dano antes de seu julgamento; ter o acusado cometido o crime sob coação que podia resistir, ou em cumprimento de ordem de autoridade superior, ou sob a influência de violenta emoção, provocada por ato injusto da vítima; ter o acusado confessado espontaneamente a autoria do crime perante a autoridade; dentre outras¹⁰.

Na terceira fase da dosimetria da pena, são verificadas as causas que diminuem ou aumentam a pena, de forma fracionada ou multiplicada, sendo dispostas tanto na parte geral como na parte especial do Código Penal¹¹.

Somente nesta terceira fase é possível que, com a diminuição da pena, esta seja fixada abaixo do mínimo legal previsto para o crime, ou com o aumento da pena, esta seja fixada acima do máximo legal previsto para o crime¹².

Ao réu condenado por crime de estelionato, privativo de liberdade, não sendo condenado a pena de mais de dois anos; não tendo a possibilidade de substituir a pena privativa de liberdade aplicada por restritiva de direito; como também, não sendo reincidente de crime doloso; e, por fim, possuindo circunstâncias judiciais favoráveis; poderá ter a sua pena suspensa condicionalmente por 2 a 4 anos, conforme prevê o artigo 77 do Código Penal Brasileiro, obedecidas as exigências dos parágrafos 1º e 2º do artigo 78 do mesmo dispositivo legal, como a prestação de serviços à comunidade durante o primeiro ano, e demais exigências equivalentes às feitas para a concessão da suspensão condicional do processo, anteriormente exposta¹³.

Para que possamos prosseguir e compreender melhor o crime de estelionato que tem sido praticado com o uso da Internet se faz necessário primeiramente um entendimento básico sobre a Internet, quanto a sua origem e como pode ser utilizada, bem como a ocorrência de alguns crimes por meio de sua utilização. E, é neste sentido, que o próximo capítulo é apresentado.

¹⁰ MIRABETE, Julio Fabbrini. **Manual de direito penal**. 16 ed. Volume 1. São Paulo: Atlas, 2000, p. 306-9.

¹¹ Idem. **Código penal interpretado**. 4. ed. São Paulo: Atlas, 2003, p. 477-8.

¹² Ibidem, p. 478.

¹³ Ibidem, passim.

2. A INTERNET E O CRIME VIRTUAL

Este capítulo tem o objetivo de trazer ao leitor um breve entendimento quanto ao surgimento da Internet e de sua utilização por qualquer pessoa que dela queira fazer uso, sendo ainda feito um breve comentário sobre alguns crimes que são praticados na Internet.

2.1 Breve histórico do surgimento da Internet

A criação da Internet iniciou-se em 1969, diante da grande preocupação norte americana em sofrer ataques nucleares da potencial inimiga Rússia. Sendo necessária que, em caso real de ataque nuclear, fosse necessário que as suas comunicações militares e governamentais não fossem interrompidas¹⁴.

A partir dessa preocupação, o Departamento de Defesa dos Estados Unidos elaborou um Sistema de Telecomunicações, desenvolvido pela Agência de Projetos e Pesquisas Avançadas, a ARPA, criando assim uma rede denominada ARPAnet, que operaria através de inúmeras e pequenas redes locais, denominadas LAN (Local Area Network), que significa rede local responsável em ligar computadores num mesmo edifício, sendo instaladas em locais estratégicos por todo o País, os quais foram interligadas por meios de redes de telecomunicação geográficas, denominadas WAN (Wide Area Network), que significa rede de longo alcance, responsáveis pela conexão de computadores por todo o mundo, e assim, caso houvesse um ataque nuclear contra os Estados Unidos da América, as comunicações militares e governamentais não seriam interrompidas, podendo permanecer interligadas de forma contínua¹⁵.

Em 1970 foi desenvolvido o primeiro protocolo, ou seja, formato de mensagens possuindo regras de envio e recepção entre computadores, ocorrendo de hospedeiro para hospedeiro, que na prática quer dizer, através de um computador de informática capaz de centralizar a hospedagem de página eletrônica

¹⁴ INELLAS, Gabriel César Zaccaria de. **Crimes na Internet**. São Paulo: Editora Juarez de Oliveira, 2004, p.1.

¹⁵ Ibidem, p.1.

denominada Site (sítio), que possibilitaria a troca de mensagens com outro computador que a este estivesse ligado por meio da rede de comunicações previamente instalada¹⁶.

Em 1972 foi desenvolvido o correio eletrônico, mais conhecido como o e-mail, possibilitando assim tanto a troca como o armazenamento de mensagens eletrônicas entre computadores que estivessem ligados ao computador central, este último se responsabilizando pela operação de recepção da mensagem de um endereço virtual, normalmente usado por um usuário em qualquer um dos computadores ligados a ele por meio da rede de comunicações, para envio a outro endereço virtual, usado por outro usuário em qualquer computador que também estivesse ligado a ele por meio desta rede de comunicações¹⁷.

Também neste mesmo ano de 1972, a ARPAnet foi demonstrada em público nos Estados Unidos da América, sendo que esta rede trabalhava com o protocolo denominado *Network Control Protocol*, que logo se tornou obsoleto, dando lugar ao TCP/IP (*Transmission Control Protocol / Internet Protocol*), significando Protocolo de Controle de Transmissão / Protocolo da Internet, proporcionando maior confiabilidade, uma vez que as comunicações seriam feitas por dados enviados pela rede de comunicação, através de pacotes, significando dizer que, os dados seriam divididos em pacotes menores, e assim enviados pela rede, e ao chegar no computador de destino, previamente identificado, seriam novamente reunidos, resultando nos dados previamente enviados, de forma inteligível¹⁸.

Em 1983 com a necessidade de uma rede de comunicação acadêmica e uma outra destinada aos objetivos militares, ocorre uma divisão, dando origem a duas redes, a ARPAnet e a MILnet. Em seguida surgiram ainda outras redes, uma para a Fundação Nacional da Ciência, a Csnet, e outra com a Cooperação da instituição IBM, destinada para o uso comercial, a BITnet. Tendo em comum, que todas estas redes permaneciam dependentes da rede principal a ARPAnet, que se tornou em uma espécie de Rede das Redes, passando a denominar-se ARPA-INTERNET, e posteriormente de INTERNET¹⁹.

¹⁶ INELLAS, Gabriel César Zaccaria de. **Crimes na Internet**. São Paulo: Editora Juarez de Oliveira, 2004, p. 1-2.

¹⁷ Ibidem, p. 2.

¹⁸ Ibidem, p. 2.

¹⁹ Ibidem, p. 2.

E ainda, em 1983, em Genebra, foi criada a Rede Mundial de Computadores (*World Wide Web*), comumente conhecida por WWW, na qual se possibilitaria a propagação de documentos por meio de imagens e sons, entre usuários da rede de comunicação por todo o mundo, o que realmente se propagou por todo o planeta²⁰.

2.2 Utilização da Internet

A Internet é um sistema de comunicação formada por redes de computadores, conectando milhares de pessoas em todo o mundo, sendo usado como meio de comunicação e relacionamento entre as pessoas, e ainda, na obtenção de conhecimento, serviços e produtos²¹.

A primeira coisa que se faz necessário a uma pessoa para dispor dos recursos da Internet, é ter um computador de informática previamente configurado para acessar a Internet. Para isso são disponibilizados programas específicos que são instalados no computador, permitindo assim o acesso à rede mundial²².

Outro fator importante é o provedor, ou seja, a ponte de conexão deste computador com a rede mundial. Sendo disponíveis no mercado diversas formas de provedores de conexão, dentre elas, como as principais utilizadas no Brasil, temos a conexão discada, a conexão via rádio, a conexão DSL e a conexão Wi-Fi.

A conexão à Internet pelo modo discado, refere-se à utilização de uma linha telefônica normal ligada à placa eletrônica do computador denominada modem. Este modem tem o papel de transformar os dados digitais de informática em sinais telefônicos, e por meio de uma ligação telefônica normal pode-se transmitir e receber dados para o modem do provedor, o que coloca o usuário em conexão com a rede mundial. No entanto este tipo de conexão tem a desvantagem de ser lento devido a velocidade de troca de dados ser pequena²³.

A conexão à Internet pelo modo via rádio, refere-se à utilização de um sistema de transmissão e recepção em frequência de rádio ligado diretamente ao

²⁰ INELLAS, Gabriel César Zaccaria de. **Crimes na Internet**. São Paulo: Editora Juarez de Oliveira, 2004, p.2.

²¹ LAQUEY, Tracy, 1963 – **O manual da Internet** – tradução insght Serviços de Informática. Rio de Janeiro: Campus, 1994, p. 11-2.

²² Ibidem, p. 184.

²³ Ibidem, p. 185.

computador por meio de uma porta de rede, e assim possibilitando conectar-se ao provedor de Internet igualmente equipado com um transmissor e receptor em frequência de rádio, e assim obter o acesso à rede mundial²⁴.

A conexão à Internet DSL, tem como denominação Digital Subscriber Live significando Linha Digital de Assinante. Neste tipo de conexão há o uso das instalações da linha telefônica, mas não é usado o sistema telefônico em si, ou seja, diferentemente da conexão discada, esta conexão não necessita da realização de uma ligação telefônica para realizar a conexão, usando-se apenas das instalações físicas para transmissão dos dados digitais. Tem como vantagem a grande velocidade, ou seja, rapidez na troca de dados, vez que o modem não necessita de transformações complexas dos dados de informática²⁵.

A conexão à Internet Wi-Fi, tem como denominação Wireless Fidelity, significando Fidelidade sem fio. Neste tipo de conexão é usado um sistema de frequência denominado IEEE 802.11, não havendo necessidade de ligação num sistema físico externo de transmissão e recepção, como ocorre na conexão via rádio, pois tal equipamento pode ser substituído por um pequeno sistema eletrônico instalado ou conectado no próprio computador. Tal conexão tem a vantagem de ter boa velocidade, grande mobilidade, uma vez que a transmissão é realizada sem a necessidade de ligações físicas, operando mediante frequência, sendo empregado principalmente nos computadores portáteis, denominados de notebooks²⁶.

Resolvido a questão de conexão na Internet, poderá o usuário desfrutar dos recursos proporcionados pela rede mundial, tais como a comunicação, a obtenção de conhecimento, de serviços e de produtos.

A comunicação entre pessoas na Internet pode se realizada por meio dos correios eletrônicos, comumente conhecidos por e-mail. Funcionando como um correio virtual, que transmite e recebe correspondências, que são digitadas e armazenadas no próprio computador do usuário, por meios de programas específicos; ou num computador hospedeiro, diferente do computador do usuário, que permanece conectado e disponível a este tipo de serviço de forma contínua,

²⁴ KUROSE, James F.. **Redes de Computadores e a Internet**: uma abordagem top-down. 3. ed. São Paulo: Person Addison Wesley, 2006, p. 20.

²⁵ LAQUEY, Tracy, 1963 – **O manual da Internet** – tradução insight Serviços de Informática. Rio de Janeiro: Campus, 1994, p. 25-6.

²⁶ Ibidem, passim.

onde as mensagens poderão ser criadas, enviadas, recebidas e armazenadas, sendo visualizado pelo usuário por meio de página eletrônica, quando conectado ao hospedeiro²⁷.

Outra forma de comunicação é conhecida por sites de relacionamento, ou seja, páginas eletrônicas, onde diversos usuários da Internet se utilizam para trocar mensagens instantâneas, com possibilidades diversas quanto a troca de dados escritos, de imagens e de sons. Alguns destes sites são comumente chamados de site de bate-papo, destinado a conversas entre os usuários conectados²⁸.

A obtenção de conhecimento pelo usuário é realizada através de páginas eletrônicas criadas especificamente para armazenar e fornecer informações e conhecimentos, sendo buscadas aquelas que sejam de seu interesse. Entre elas, temos as de autoria pessoal, de comunidade, de sociedade e empresarial. Esta busca pode ser realizada, acessando diretamente ao endereço eletrônico destas páginas, ou por meio de utilização de serviços de busca de páginas, que seriam páginas que disponibilizam informações e acessos a diversas páginas, normalmente associadas a ela por meio de pagamento de alguma taxa²⁹.

A obtenção de serviços pela Internet, disponibiliza ao usuário a possibilidade de receber certas prestações de serviços, sendo muitas vezes exigido o preenchimento de determinadas informações ou cadastros, exigidos pelo prestador de serviços. E dessa forma o usuário poderá obter serviços de caráter comercial, governamental, institucional, entre outros. Como por exemplo, serviços de consultas, certidões, permissões, assinaturas, e outras³⁰.

A obtenção de produtos, disponibiliza ao usuário da Internet, principalmente por meio do comércio eletrônico, a possibilidade de aquisição de produtos, como livros, equipamentos eletrônicos, roupas, automóveis, casa, entre outros. Podendo se tratar de apenas um meio de contato entre os interessados, para que se concretize a negociação, ou mesmo, se tratar de sofisticado site que dispõe de

²⁷ LAQUEY, Tracy, 1963 – **O manual da Internet** – tradução insight Serviços de Informática. Rio de Janeiro: Campus, 1994, passim.

²⁸ Ibidem, passim.

²⁹ Ibidem, passim.

³⁰ Ibidem, passim.

inúmeros recursos que possibilitem a própria concretização das negociações³¹.

2.3 Crimes Praticados na Internet

A Internet é um poderoso meio de comunicação, e a cada dia tem aumentado o número de pessoas que a acessam e dela se usufruem, abrindo as fronteiras, permitindo a obtenção de diversos benefícios, como relacionamento comercial, o lazer pessoal, a obtenção de serviços privados e governamentais, dentre outros.

Contudo, a Internet possibilitou também que criminosos fizessem uso deste meio de comunicação para a prática de crimes, como o racismo, o furto, o dano, o estelionato, os crimes contra o sistema financeiro, a pornografia infantil, os crimes contra a honra, a ameaça, a interceptação do fluxo de dados em tráfego por serviço de telecomunicações, os crimes contra a inviolabilidade dos segredos, os crimes contra a ordem tributária, os crimes eleitorais, a violação de correspondência, a incitação ao crime, a apologia de crime ou de criminoso, a violação do direito autoral, o induzimento, instigação ou auxílio ao suicídio, o favorecimento da prostituição, o rufianismo, o tráfico de substâncias estupefacientes, as armas de fogo, a culto e impedimento ou perturbação de ato a ele relativo, os crimes contra o consumidor, os crimes contra a economia popular.

O Crime de racismo está previsto no artigo 20, da Lei 7.716 de 1989, referindo-se a prática, induzimento ou incitação à discriminação ou preconceito racial ou etnológico, podendo ser realizado por alguém através da Internet por meio de divulgação em página eletrônica, correios eletrônicos, bate papos, entre outros³².

O Crime de furto está previsto no artigo 155 do Código Penal, referindo-se a subtração de coisa alheia para si ou para outrem, ocorrendo, por exemplo, na realização de cópias de programas de informática, de cópias de segredos ou dados confidenciais³³.

³¹ LAQUEY, Tracy, 1963 – **O manual da Internet** – tradução insight Serviços de Informática. Rio de Janeiro: Campus, 1994, passim.

³² INELLAS, Gabriel César Zaccaria de. **Crimes na Internet**. São Paulo: Editora Juarez de Oliveira, 2004, p. 36-7.

³³ Ibidem, p. 38-41.

O delito de dano está previsto no artigo 163 do Código Penal, referindo-se a destruição, inutilização ou deterioração de coisa alheia, crime este que vem aumentando a cada dia na Internet, presenciado, por exemplo, por meio de disseminação de vírus por computadores, vírus estes que seriam pequenos programas capazes de provocar prejuízo às informações armazenadas em um computador, sendo normalmente a vítima, qualquer usuário que venha a recebê-lo pela Internet³⁴.

O crime de estelionato tem a sua previsão e disposição referida no capítulo anterior, ocorrendo na Internet, por exemplo, através de criação de páginas falsas, no intuito de obter vantagem ilícita patrimonial da vítima enganada, outra forma, é o envio de correio eletrônico falso, informando ser alguma entidade de que a vítima confie, no intuito de obter desta vítima ganho ilícito sobre o seu patrimônio, entre outros, que serão posteriormente apresentados no terceiro capítulo³⁵.

O crime contra o sistema financeiro encontra-se previsto no artigo 19 da Lei 7.492 de 1986, referindo-se a violação do sigilo de operações ou de serviços prestados por instituição financeira ou integrante do sistema de distribuição de títulos mobiliários de que tenha conhecimento, em razão de ofício, também ocorrido por meio de acesso aos sistemas financeiros disponíveis via Internet³⁶.

O crime de pornografia infantil, a princípio, somente tinha sua previsão no artigo 234 do código penal, referindo-se a prática de fazer, importar, exportar, adquirir ou ter sob sua guarda, para fim de comércio, de distribuição ou de exposição pública, escrito, desenho, pintura, estampa ou qualquer objeto obsceno, estando intimamente ligado à busca de sentimentos eróticos através do uso da criança ou adolescente, denominado de pedofilia, tendo como ferramenta o próprio uso da informática para possibilitar esta disseminação, ocorrendo por meio de páginas eróticas e incentivadoras da pedofilia, como também por envio de imagens e ilustrações eróticas de crianças e adolescentes através de correios eletrônicos, e outro. Sendo fortalecido quanto a sua prática na Internet que recebeu maior proteção por meio da alteração dos artigos 240 e 241, e da inserção dos artigos 241-A a 241-E da Lei 8.069 de 1990, que disciplina o Estatuto da Criança e do

³⁴ INELLAS, Gabriel César Zaccaria de. **Crimes na Internet**. São Paulo: Editora Juarez de Oliveira, 2004, p. 41-43.

³⁵ Ibidem, p. 43-5.

³⁶ Ibidem, p. 45.

Adolescente, referindo-se dentre outros, ao oferecimento, troca, disponibilização, transmissão, distribuição, publicação ou divulgação por qualquer meio, inclusive de informática ou telemático, fotográfico, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfico envolvendo criança ou adolescente³⁷.

O crime contra a honra tem previsão nos artigos 138, 139 e 140 do Código Penal, referindo-se respectivamente a Calúnia, a Difamação e a Injúria. Ocorrendo na Calúnia a imputação falsa a outrem de fato definido como crime, na Difamação a imputação ofensiva à reputação de outrem, e na Injúria a ofensa à dignidade ou decoro de outrem. Sendo que tal prática criminosa tem sido bastante exercida por meio da Internet, como por exemplo, em se utilizando correios eletrônicos, bate papos, paginas eletrônicas pessoais, entre outros meios disponibilizados pela Internet, para alcançar este objetivo³⁸.

O crime de ameaça está previsto no artigo 147 do Código Penal, referindo-se a ameaça a alguém, por meio de palavra, escrita ou gesto, ou qualquer outro meio simbólico, de causar-lhe mal injusto e grave, no qual tem sido utilizado do meio de comunicação de Internet através principalmente do correio eletrônico para a prática deste crime³⁹.

O crime de interceptação do fluxo de dados em tráfego por serviço de telecomunicações tem previsão no artigo 10 da Lei 9.296 de 1996, referindo-se a realização de interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da justiça, sem autorização judicial ou com objetivos não autorizados em lei, entre os quais a realização de interceptação feita pela Internet, aplicando-se tal interceptação ao fluxo de comunicações em sistema de informática⁴⁰.

O crime contra a inviolabilidade dos segredos tem sua previsão no artigo 153 do código penal, referindo-se a divulgação, sem justa causa, de conteúdo particular ou de caráter sigiloso, de que é destinatário ou detentor, cuja divulgação possa produzir dano a outrem. Do qual o criminoso, tem se utilizado da Internet para a

³⁷ INELLAS, Gabriel César Zaccaria de. **Crimes na Internet**. São Paulo: Editora Juarez de Oliveira, 2004, p. 45-8.

³⁸ Ibidem, p. 48-51.

³⁹ Ibidem, p. 51-2.

⁴⁰ Ibidem, p. 52-3.

prática reprovável desta divulgação⁴¹.

O crime contra a ordem tributária está disciplinado no inciso V do artigo 2º, da Lei 8.137 de 1990, referindo-se a utilização ou divulgação de programa de processamento de dados que permita ao sujeito passivo da obrigação tributária possuir informação contábil diversa daquela que é, por lei, fornecida à Fazenda Pública. Sendo este crime muito praticado através de meios de comunicações da Internet na utilização ou a divulgação destes dados⁴².

Os crimes eleitorais têm sua previsão nos incisos I, II e III do artigo 72, da Lei 9.504 de 1997, referindo-se o inciso I a obtenção de acesso de sistema de tratamento automático de dados usado pelo serviço eleitoral; o inciso II ao desenvolvimento ou introdução de comando, instrução, ou programação de computador capaz de destruir, apagar, eliminar, alterar, gravar ou transmitir dado, instrução ou programa ou provocar qualquer outro resultado diverso do esperado em sistema de tratamento automático de dados usados pelo serviço eleitoral; e o inciso III quanto a causar, propositadamente, dano físico ao equipamento usado na votação pelo serviço eleitoral, sendo estes crimes cometidos apenas por meio da Internet. No entanto há crimes eleitorais que podem ser praticados através da Internet, como o crime de induzimento de alguém, que tenha infração em qualquer dos dispositivos do Código Eleitoral, a se inscrever como eleitor, o que está previsto no artigo 290 do referido código, Lei 4.737 de 1965⁴³.

O crime de violação de correspondência está previsto no artigo 151 do código penal, referindo-se a violação indevida de conteúdo de correspondência fechada de outrem, no entanto o artigo 56 da Lei 4.117 de 1962 se torna mais adequado à violação de mensagem na Internet, como o correio eletrônico, referindo-se a prática de crime à violação de telecomunicação que, transgredindo lei ou regulamento, exhiba autógrafo ou qualquer documento do arquivo, divulgue ou comunique, informe ou capte, transmita a outrem ou utilize o conteúdo, resumo, significado, interpretação indicação ou efeito de qualquer comunicação dirigida a terceiro, o que é complementada com o parágrafo 1º do respectivo artigo, que nos trás ainda como crime, a pratica da violação de telecomunicações por quem ilegalmente vier a

⁴¹ INELLAS, Gabriel César Zaccaria de. **Crimes na Internet**. São Paulo: Editora Juarez de Oliveira, 2004, p. 53-5.

⁴² Ibidem, p. 55.

⁴³ Ibidem, p. 55-6.

receber, divulgar ou utilizar, de forma interceptada. Isto se deve a limitação proposta pelo código penal, quando se trata de crime de violação de correspondência fechada, o que por meio da Lei 4.117, possibilita a correção desta limitação, sendo ampliado este entendimento, e em consequência disto, a possibilidade de punição quando o crime for praticado com o uso da Internet⁴⁴.

A Incitação ao crime tem sua previsão no artigo 286 do código penal, que possui a compreensão de igualdade quanto ao induzimento e a instigação, sendo praticado na Internet como, por exemplo, através de correios eletrônicos, páginas eletrônicas, bate-papos, e outros, incitando a crimes como, o racismo, intolerância religiosa, e outros⁴⁵.

A apologia de crime ou de criminoso está previsto no artigo 287 do código penal, sendo praticado na Internet por meio da disseminação de informações e imagens apologética, ou seja, o elogio, enaltecimento a conduta ou prática de ato criminoso⁴⁶.

A violação de direito autoral tem sua previsão no artigo 12 da Lei 9.609 de 1998, referindo-se a violação de direitos de autor de programa de computador, por sua vez complementado por seu parágrafo primeiro quando da prática resultante da reprodução por qualquer meio de programa de computador para fins comerciais, sem autorização expressa do autor ou de quem o represente, ou complementado pelo parágrafo segundo deste mesmo artigo, quando o infrator vende, expõe, introduz no país, adquire, oculta ou tem em depósito, para fins de comércio, original ou cópia de programa de computador, produzido com violação de direito autoral. Tendo com ferramenta o uso da Internet como meio de comercialização, fornecimento e obtenção ilegal destes programas, violando o direito autoral de seu autor ou de quem o represente⁴⁷.

O crime de induzir, instigar ou auxiliar alguém ao suicídio é previsto no artigo 122 do código penal, referindo-se a pessoa que comete o ato ilícito de convencer, provocar ou ajudar a outrem para que cometa o suicídio. Sendo a sua prática também ocorrida através da Internet por meio de uso de mensagens por meio de

⁴⁴ INELLAS, Gabriel César Zaccaria de. **Crimes na Internet**. São Paulo: Editora Juarez de Oliveira, 2004, p. 56-7.

⁴⁵ Ibidem, p. 58.

⁴⁶ Ibidem, p. 58-9.

⁴⁷ Ibidem, p. 59-60.

correio eletrônico, bate papo, entre outros, com o objetivo de que determinada pessoa, quer por fragilidade emocional, quer por incapacidade de compreensão do ato, quer por estímulo de crença ou ideologia, venha a cometer o suicídio⁴⁸.

O crime de favorecimento da prostituição está previsto no artigo 228 do Código Penal, referindo-se ao ato de induzir ou atrair alguém à prostituição, facilitá-la ou impedir que dela a pessoa inserida abandone. Sendo buscado através da Internet, pela página eletrônica, envio de mensagens por correio, e outros, objetivando a atração, facilitação ou a permanência de alguém na prática da prostituição⁴⁹.

O crime de rufianismo tem sua previsão no artigo 230 do Código Penal, referindo-se ao fato do criminoso tirar proveito da prostituição alheia, participando diretamente de seus lucros ou fazendo-se sustentar, no todo ou em parte, por quem a exerça. Tal crime tem sido praticado por meio da Internet, onde o criminoso cria páginas eletrônicas, que visam expor imagens e textos atrativos, que não somente favorecem a prostituição alheia, mas que de forma habitual, tira proveito, por meio de lucro ou se fazendo sustentar-se por meio disso⁵⁰.

O crime de tráfico de substâncias entorpecentes tem sua tipificação no artigo 33 da Lei 11.343 de 2006, dispondo sobre o crime de importação, exportação, remeter, como também a preparação, produção, fabricação, aquisição, venda, exposição à venda, oferecimento, depósito, transporte, guarda, prescrição, administração, entrega, fornecimento de drogas, mesmo que de forma gratuita, sem autorização ou discordância a determinação legal. Sendo utilizado o meio de comunicação através da Internet, para que as negociações e etapas operacionais da produção ao fornecimento da droga sejam facilitadas e agilizadas. Para isso são utilizados principalmente de ferramentas de comunicação como o correio eletrônico⁵¹.

O crime de armas de fogo tem sua previsão no artigo 17 da Lei 10.826 de 2003, referente ao Estatuto do Desarmamento, dispondo sobre o crime quanto à aquisição, aluguel, recebimento, transporte, condução, ocultação, depósito,

⁴⁸ INELLAS, Gabriel César Zaccaria de. **Crimes na Internet**. São Paulo: Editora Juarez de Oliveira, 2004, p. 60-1.

⁴⁹ Ibidem, p. 61-2.

⁵⁰ Ibidem, p. 62-3.

⁵¹ Ibidem, p.63-4.

desmontagem, montagem, remontagem, adulteração, venda, exposição para venda, ou de qualquer outra forma, em proveito próprio ou alheio, no exercício de atividade comercial ou industrial, de arma de fogo, acessório ou munição, sem autorização ou em desacordo com determinação legal ou regulamentar. Em que o criminoso tem se utilizado da Internet como meio de negociar ou facilitar a prática de quaisquer destes atos criminosos referentes a armas de fogo⁵².

O crime a culto e impedimento ou perturbação de ato a ele relativo está previsto no artigo 208 do Código Penal, referindo-se ao escarnecimento de alguém publicamente, por motivo de crença ou função religiosa; ao ato de impedir ou perturbar cerimônia ou prática de culto religioso; e ao ato de vilipendiar, ou seja, desprezar, publicamente ato ou objeto de culto religioso. Tem encontrado espaço na sua prática através da Internet, como o ato de escarnecer de alguém por motivo de crença ou função religiosa, utilizando correio eletrônico ou página eletrônica para cometer tal crime⁵³.

Os crimes contra o consumidor têm sua previsão dentre os artigos do Título II – Das Infrações Penais da Lei 8.078 de 1990, referente ao Código de Defesa do Consumidor. Sendo dentre eles, os artigos 67 e 68, referentes a crimes contra o consumidor que também são praticados através da Internet, entre tanto, o artigo 67 refere-se ao ato de fazer ou promover publicidade que sabe ou deveria saber ser enganosa ou abusiva, tendo o artigo o objetivo de buscar uma punição de maneira geral. Já o artigo 68, refere-se ao ato de fazer ou promover publicidade que sabe ou deveria saber ser capaz de induzir o consumidor a se comportar de forma prejudicial ou perigosa a sua saúde ou segurança, assim o artigo traz um alcance de maior gravidade e conseqüentemente uma necessidade punitiva mais eficaz. E Para tais crimes contra o consumidor, o criminoso na forma virtual utiliza página eletrônica ou envio de mensagens por correio eletrônico a pessoas ou grupos, sem prévia determinação pessoal, expondo imagens e textos, do qual se promove uma publicidade enganosa ou abusiva⁵⁴.

Os crimes contra a economia popular estão previstos nos artigos 2º a 4º da Lei 1.521 de 1951, referindo-se a recusa de prestação serviços essenciais à

⁵² INELLAS, Gabriel César Zaccaria de. **Crimes na Internet**. São Paulo: Editora Juarez de Oliveira, 2004, p. 64.

⁵³ Ibidem, p. 64.

⁵⁴ Ibidem, p. 65-71.

subsistência, a sonegação ou recusa de venda de mercadoria, favorecimento de compradores em detrimento de outros, venda de produtos alimentícios em desconformidade com determinações oficiais, adulteração de produtos, bem como sua exposição à venda, informando diferentemente do que fora rotulado, procedimento mediante especulações ou processos fraudulentos no objetivo de conseguir ganhos ilícitos em detrimento do povo ou indeterminado número de pessoas, fraude dos pesos ou medidas padronizadas legalmente, ou delas se utilizar conscientemente, dentre outras. Crimes este que tem sido praticado também por meio do uso da Internet, o que facilita a propagação e o aumento maior e mais abrangente de vítimas, visto a própria natureza da rede de comunicações entre as pessoas que dela fazem uso⁵⁵.

Neste momento tendo absorvido um pouco a respeito do histórico do surgimento da Internet, bem como podemos dela fazer uso, nos auxiliando na vida pessoal, profissional e educativa, e ainda tendo observado um pouco sobre alguns crimes que são cometidos com o auxílio da Internet, podemos adentrar ao próximo capítulo que nos apresentará de forma um pouco mais detalhada como é procedida a prática do crime de estelionato por meio do uso da Internet, sendo também apresentado alguns crimes semelhantes ao do estelionato que também são praticados na Internet, com o objetivo de distingui-los, e por fim, qual tem sido a medida penal aplicada para reprimir este crime.

⁵⁵ FURLANETO NETO, Mário; GUIMARÃES José Augusto Chaves. Crimes na Internet: elementos para uma reflexão sobre a ética informacional. **R. CEJ**, Brasília, n. 20, p. 67-73, jan./mar. 2003. Disponível em: <<http://www.cjf.jus.br/revista/numero20/artigo9.pdf>>. Acesso em: 28 abr. 2009.

3. O CRIME DE ESTELIONATO NA INTERNET

Este capítulo tem o objetivo de apresentar ao leitor a prática do crime de estelionato que vem sendo praticado na Internet, bem como apresentar alguns crimes virtuais que se assemelham ao crime de estelionato eletrônico, no intuito de diferenciá-lo, e ainda o de trazer, qual a medida penal que tem sido aplicada aos infratores deste tipo de crime.

3.1 A prática do crime de estelionato na Internet

O crime de estelionato praticado na Internet também é conhecido por estelionato eletrônico, consistindo no crime previsto no artigo 171 do CP, cujo conceito foi apresentado no Primeiro Capítulo, sendo, para tanto, usado pelo agente ativo o meio de comunicação eletrônico, a Internet, para que se possa atingir o objetivo final, que é o de obter para si ou para outrem vantagem patrimonial ilícita, induzindo ou mantendo a vítima em erro⁵⁶.

A prática deste tipo de crime, ou seja, o estelionato cometido através da Internet, pode ser realizado tanto por pessoa que tenha grande conhecimento de informática e de sistema de rede utilizado na Internet, como por pessoa que tenha pouco conhecimento, sendo apenas um simples usuário da Internet.

Quanto ao usuário de conhecimento avançado, que busca criar mecanismos sofisticados capazes de enganar facilmente suas vítimas, é conhecido por usuário Cracker, tratando-se de uma pessoa física, portadora de avançado conhecimento de programação de computador, que busca prejudicar com dolo suas vítimas, ou seja, conscientemente por vontade própria, penetrando em redes locais, ligadas à rede mundial, previamente seguradas por seus proprietários, e assim invadindo e praticando ações sem a devida e correta autorização, de forma ilegal, objetivando entre outros crimes possíveis pela Internet, já abordados no capítulo anterior, o

⁵⁶ INELLAS, Gabriel César Zaccaria de. **Crimes na Internet**. São Paulo: Editora Juarez de Oliveira, 2004, p. 43-4.

cometimento do crime de estelionato⁵⁷.

Como exemplo de estelionato praticado na Internet por um usuário Cracker, temos, a obtenção de dinheiro da vítima, por meio de transferência bancária para uma conta de posse do Cracker, ou de outrem. Isto ocorre mediante a criação de sites similares aos utilizados por bancos, sendo armazenados na Internet, e concomitantemente o Cracker desenvolve mensagens atrativas como fosse de autoria do banco da vítima, que é encaminhada à vítima por meio do correio eletrônico, e ao ser acessada, automaticamente será direcionada ao site similar de seu banco, ou seja, aquele criado pelo Cracker, possibilitando que, ao ser feito pela vítima qualquer transferência bancária, na verdade o dinheiro será transferido para uma outra conta que o Cracker previamente tenha registrado⁵⁸.

Como exemplo de estelionato praticado na Internet por simples usuário, temos os pertinentes às correntes da sorte, ou seja, o estelionatário por meio de mensagem eletrônica enviada por e-mail, convida uma determinada vítima a depositar uma certa quantia de dinheiro em sua conta bancária, e posteriormente indicar alguns amigos, para participarem de uma corrente de sorte, que lhes renderá muito dinheiro⁵⁹.

3.2 Outros crimes semelhantes ao estelionato praticado na Internet

Um grande problema na identificação do crime de estelionato, que vem sendo praticado na Internet, é em se esbarrar na semelhança de outros crimes, como por exemplo, o furto qualificado, devido a grande semelhança no procedimento preparatório.

A fraude eletrônica, refere-se ao furto qualificado, conforme entendimento do Superior Tribunal de Justiça, sendo identificado como a ocorrência de subtração para si ou outrem, de bem móvel, mediante uso de fraude, o que não se pode confundir com o crime de estelionato eletrônico, no qual a vítima é induzida a entregar o produto patrimonial ao criminoso, de livre e espontânea vontade,

⁵⁷ PLANTULLO, Vicente Lentini. **Estelionato eletrônico**. 1ª ed. (ano 2003), 6ª tir. Curitiba: Juruá, 2008, p. 77-8.

⁵⁸ Ibidem, p. 102.

⁵⁹ Ibidem, p. 98.

mediante erro⁶⁰.

Podemos melhor visualizar esta diferença entre a fraude eletrônica e o estelionato eletrônico, em cujo modo preparatório se assemelham, tomando o exemplo de crime de estelionato praticado por Cracker exposto no subitem 3.1.

Observando o exemplo citado temos que a forma em que foi empregado o cometimento do crime foi a atração da vítima através da mensagem por ela recebida pelo correio eletrônico, que aparentemente se apresenta como tendo sido enviada pela própria instituição bancária da vítima, e que, ao ser acessado direciona automaticamente ao site criado pelo Cracker, semelhante ao site do banco da vítima.

Até aqui ambos os crimes, de furto qualificado e estelionato, nesta fase preparatória, se assemelham, no entanto, na fraude eletrônica, ou seja, no furto qualificado, o interesse final almejado é a obtenção dos dados da conta da vítima, bem como a sua senha de acesso, para que num momento posterior o Cracker, de posse destas informações possa realizar transferências bancárias de dinheiro, da conta da vítima para uma outra conta bancária, de sua propriedade ou de outrem. Assim observamos a ocorrência do furto, pela subtração do bem da vítima, ou seja, do dinheiro da vítima, realizada pelo Cracker, por meio de transferência de valores da conta da vítima para a outra conta bancária, e ainda, observamos a forma qualificada deste crime, que ocorreu mediante fraude, devido a todo este sistema montado pelo Cracker, que possibilitou enganar a vítima, e obter os dados e senhas de sua conta bancária, para que o crime de furto fosse posteriormente consumado.

Agora no caso do estelionato eletrônico, no qual a fase preparatória se assemelha ao do furto qualificado, temos um sistema operando pelo falso site criado pelo Cracker, que se mantém continuamente interligado com o verdadeiro site do banco da vítima, e quando for realizada qualquer transferência bancária de dinheiro pela vítima, na verdade a conta bancária que será creditada será aquela previamente registrada pelo Cracker.

Outro crime que possui semelhança com o crime de estelionato, que tem sido praticado na Internet, refere-se aos crimes contra o consumidor, no entanto no crime

⁶⁰ BRASIL. Superior Tribunal de Justiça. Penal e Processo Penal. Conflito de Competência. Processo CC nº 67343 – GO. Terceira Seção. Relatora: Ministra Laurita Vaz, DF, 28 de março de 2007. Disponível em: < [http://www.stj.gov.br/SCON/jurisprudencia/toc.jsp?livre= \(\('CC'.clap.+ou+'CC'.clas.\)+e+@num='67343'\)+ou+\('CC'+adj+'67343'.suce.\)> .](http://www.stj.gov.br/SCON/jurisprudencia/toc.jsp?livre= (('CC'.clap.+ou+'CC'.clas.)+e+@num='67343')+ou+('CC'+adj+'67343'.suce.)> .) Acessado em 13 abr. 2009.

de estelionato a vítima é pessoa determinada, ao passo que no crime contra o consumidor, as vítimas são pessoas de uma relação de consumo⁶¹.

Para um melhor entendimento, sobre as semelhanças entre o crime de estelionato e o crime contra o consumidor, com o uso da Internet, tomemos a seguir o exemplo.

Um Cracker envia um e-mail a uma certa vítima, informando se tratar de uma determinada loja, convidando-a a participar de uma certa promoção, posteriormente reenvia outro correio eletrônico informando a esta vítima que ganhara o prêmio, e que para recebê-lo deveria efetuar um depósito bancário de certa quantia na conta informada, referindo se tratar de despesas de correspondência para o envio do prêmio, e desta forma enganando a vítima a efetuar o depósito. Aqui, estaríamos diante de um crime de estelionato praticado na Internet.

Agora, se um comerciante de uma determinada loja envia mensagens por correio eletrônico a consumidores, informando-os de uma certa promoção com sorteio de um brinde, sendo necessário fornecer alguns dados pessoais para fins de pequeno cadastro, tendo o comerciante o real interesse de utilizar os dados obtidos dos consumidores para repassá-los a outros fornecedores de produtos ou vendas, sem a prévia autorização destes consumidores, estaremos diante de um crime contra o consumidor.

Outro crime que pode apresentar semelhança ao crime de estelionato, tendo sido praticado na Internet, é o crime contra a economia popular, sendo que no estelionato como exposto anteriormente, é cometido contra determinada pessoa, já no crime contra a economia popular o crime é direcionado ao povo ou a um número indeterminado de pessoas, sendo que possui uma dimensão de resultado maior do que o crime contra o consumidor, de forma a trazer prejuízo à economia popular⁶².

Exemplificando o exposto acima, observemos primeiramente a seguir um caso de crime de estelionato praticado por meio da Internet.

⁶¹ INELLAS, Gabriel César Zaccaria de. **Crimes na Internet**. São Paulo: Editora Juarez de Oliveira, 2004, p. 65–7.

⁶² FURLANETO NETO, Mário; GUIMARÃES José Augusto Chaves. Crimes na Internet: elementos para uma reflexão sobre a ética informacional. **R. CEJ**, Brasília, n. 20, p. 67-73, jan./mar. 2003. Disponível em: <<http://www.cjf.jus.br/revista/numero20/artigo9.pdf>>. Acesso em: 28 abr. 2009.

Certo criminoso envia um e-mail a uma determinada vítima, informando ser uma organização de proteção ao meio ambiente, convidando-a a participar, e disponibilizando a ela determinada conta bancária para que se possa contribuir. Aqui, estamos diante de um caso de estelionato.

Agora tomando o mesmo exemplo, para o caso de crime contra a economia popular, temos: um certo criminoso envia mensagens de correio eletrônico sem determinação de pessoa, buscando encaminhar para o maior número de pessoas e esperando com que as vítimas iludidas possam estar encaminhando a mesma mensagem a seus amigos, parentes e outros, por tal causa nobre. Aqui estamos diante de um crime contra a economia popular, que além da indeterminação da pessoa, pode atingir uma grande projeção prejudicial econômica social.

3.3 Aplicabilidade Penal

O crime de estelionato que tem sido praticado na Internet ainda não possui uma tipificação própria quanto a esta nova relação de crime virtual, sendo usualmente utilizado por analogia de interpretação o próprio artigo 171 do Código Penal Brasileiro, conforme apresentado no primeiro capítulo, e havendo qualificação deste crime tão somente quando cometido em detrimento de entidade de direito público ou de instituto de economia popular, assistência social ou beneficência.

Agora que pudemos melhor compreender o crime de estelionato praticado na Internet, e ainda ter uma visão mais clara na distinção de alguns crimes virtuais que apresentam semelhanças ao estelionato eletrônico, observando por fim qual tem sido a medida penal aplicada para reprimir este crime, podemos então adentrar ao próximo capítulo que nos fala dos projetos de lei que visam por meio de aprovação produzir ferramentas legais para combater o crime virtual, bem como quais os crimes virtuais que já foram alcançados por projetos de lei, e por fim como está a questão de projeto de lei contra o crime de estelionato praticado na Internet.

4. PROJETO DE LEI CONTRA CRIMES VIRTUAIS

Este capítulo tem o objetivo de apresentar ao leitor um breve comentário a cerca da criação de Projeto de Lei contra os crimes virtuais, e ainda apontar alguns crimes que são cometidos na Internet e que obtiveram proteção legal de forma mais adequada à realidade atual, e por fim apresentar um breve comentário sobre a existência de Projeto de Lei contra o crime de estelionato praticado na Internet.

4.1 Criação de Projeto de lei contra crimes virtuais

Os crimes praticados na Internet precisam ser definidos, e melhor disciplinados, para que haja um combate mais eficaz, e conseqüentemente uma melhor proteção à sociedade.

Neste sentido parlamentares tem criado projetos de lei que visam contribuir no combate a ações criminosas realizadas por meio da rede de comunicação virtual, ou seja, da Internet, no território brasileiro.

Tanto se vislumbra esta problemática, cobrada pela sociedade, e buscada pelos parlamentares, de se sanar a falta de punibilidade eficaz contra tais ações criminosas, praticadas com o uso da Internet, que tem causado enormes prejuízos individuais e coletivos, que recentemente o Senado Federal tem aprovado projetos que visam a proteção do indivíduo e da coletividade contra crimes desta natureza, crendo realmente na necessidade de tipificação que não somente defina corretamente o crime, mas que traga meios coercitivos eficazes no seu combate⁶³.

⁶³ BRASIL. Substitutivo ao Projeto de Lei do Senado nº 0076 de 2000, ao Projeto de Lei do Senado nº 0137 de 2000 e ao Projeto de Lei da Câmara nº 89 de 2003. Dispõe sobre a tipificação de condutas realizadas mediante uso de sistema eletrônico, digital ou similares, de rede de computadores, ou que sejam praticadas contra dispositivos de comunicação ou sistemas informatizados e similares. Disponível em: <http://www.senado.gov.br/comunica/agencia/pags/01.html>. Acesso em: 29 abr. 2009.

4.2 Crimes praticados na Internet atualmente alcançados

O Projeto de Lei do nº 3773 de 2008, da CPI da Pedofilia no Senado possibilitou que fosse criada o diploma alterador, a Lei 11.829 em novembro de 2008, permitindo a alteração dos artigos 240 e 241, bem como a inclusão dos artigos 241-A a 241-E a Lei 8.069 de 1990, do Estatuto da Criança e do Adolescente⁶⁴.

Essa aprovação possibilitou uma maior proteção a crianças e adolescentes, no momento em que cria medidas punitivas mais eficazes contra ações criminosas de produção, participação, venda, exposição, oferecimento, troca, disponibilidade, transmissão, distribuição, publicação, divulgação, armazenamento, asseguarção de acesso, aquisição ou simule qualquer tipo de material visual de cena de sexo explícito ou pornográfica, envolvendo crianças ou adolescentes, bem como o aliciamento, assédio, instigação, constrangimento, com finalidade de prática de ato libidinoso com criança, que vinha sendo utilizado dentre outros meios possíveis a rede de comunicação entre computadores, ou seja, a Internet.

Muitos outros crimes estão propostos por meio de Projeto de Lei, como o caso do Projeto de Lei proposto pelo Senador Eduardo Azeredo, como substitutivo dos Projetos - PLS nº 76 de 2000, PLS nº 137 de 2000 e PLC nº 89 de 2003, que teve aprovação no Senado Federal, e aguarda a decisão da Câmara dos Deputados. Visando o combate de forma mais eficaz aos crimes praticados na Internet, dentre eles, o acesso indevido a meio eletrônico; a manipulação indevida de informação eletrônica; o dano eletrônico; o atentado contra a segurança de serviço de utilidade pública; a interrupção ou perturbação de serviço telegráfico e telefônico; a falsificação de cartão de crédito; a falsificação de telefone celular; a divulgação de informações pessoais ou de empresas; dentre outros⁶⁵.

⁶⁴ PINTO, Carlos Alberto Ferreira. Pedofilia: Uma abordagem essencialmente jurídica. **Recanto das Letras**. São Paulo, 26 Jan. 2009. Disponível em: <<http://recantodasletras.uol.com.br/textosjuridicos/1405178>>. Acesso em: 26 abril 2009.

⁶⁵ APROVADO projeto que pune crimes praticados com a utilização da internet. **O GLOBO**. Brasil, 10 jul. 2008. Disponível em: <http://oglobo.globo.com/pais/mat/2008/07/10/aprovado_projeto_que_pune_crimes_praticados_com_utilizacao_da_internet-547186659.asp>. Acesso em: 24 abr. 2009.

4.3 Projeto de Lei Contra o Crime de Estelionato praticado na Internet

O crime de estelionato praticado na Internet, ou seja, o estelionato eletrônico, tem sido observado pela sociedade, e exigido de forma crescente a necessidade em se criar meios mais eficazes no seu combate, uma vez que o desenvolvimento da Internet, vem possibilitando a cada dia um maior número de usuários conectados, atraídos pelos benefícios oferecidos pela Internet, como obtenção de serviços mais eficazes, obtenção de produtos dos mais diversos, possibilidade de comunicação mais rápida e agradável entre entes queridos, facilidade na obtenção de clientes e no desenvolvimento de negócios, dentre outros.

Neste sentido o crime de estelionato praticado na Internet também é objeto de mudança por meio de projeto de lei, como do substitutivo ao PLS 76/2000, PLC 173/2000 e PLC 89/2003, que traz o pedido justificado de mudança de lei pela necessidade de maior proteção da sociedade contra crimes como o estelionato eletrônico, pelo qual se pede pela inserção de inciso ao parágrafo 2º do artigo 171 do Código Penal, buscando trazer uma definição, bem como se pede pela inserção de parágrafo ao mesmo artigo, no intuito de aumentar a pena ao estelionatário que praticar o crime eletronicamente utilizando nome falso ou identidade de terceiros⁶⁶.

“Art. 171
 § 2º Nas mesmas penas incorre quem:

 Estelionato Eletrônico
 VII – difunde, por qualquer meio, código malicioso com intuito de facilitar ou permitir acesso indevido à rede de computadores, dispositivo de comunicação ou sistema informatizado:
 § 3º Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime do inciso VII do § 2º deste artigo, a pena é aumentada de sexta parte.”

Neste momento, tendo sido observado um breve comentário sobre a criação de projeto de lei contra crimes virtuais, e quais os crimes desta natureza foram objetos de projetos de lei que obtiveram alcance por meio de aprovação do poder legislativo, bem como observado nesta questão de projeto de lei o que tem sido

⁶⁶ BRASIL. Substitutivo ao Projeto de Lei do Senado nº 0076 de 2000, ao Projeto de Lei do Senado nº 0137 de 2000 e ao Projeto de Lei da Câmara nº 89 de 2003. Dispõe sobre a tipificação de condutas realizadas mediante uso de sistema eletrônico, digital ou similares, de rede de computadores, ou que sejam praticadas contra dispositivos de comunicação ou sistemas informatizados e similares. Disponível em: <http://www.senado.gov.br/comunica/agencia/pags/01.html>. Acesso em: 29 abr. 2009.

formulado no objetivo de combater o estelionato praticado na Internet, podemos então adentrar ao próximo e último capítulo que discorre justamente sobre a necessidade de tipificação do crime de estelionato praticado na Internet.

5. DA NECESSIDADE DE TIPIFICAÇÃO DO CRIME DE ESTELIONATO PRATICADO NA INTERNET

O crime de estelionato praticado na Internet tem a necessidade de ser tipificado, buscando assim uma proteção mais eficaz da sociedade, por um meio mais coercitivo, com punições mais severas a sua prática, tendo em vista as problemáticas envolvidas quanto da utilização da Internet para o cometimento deste tipo de crime.

Uma problemática que envolve o estelionato praticado na Internet diz respeito o da autoria, ou seja, a identificação do autor desta infração penal. Estando este criminoso muito mais protegido por trás de uma rede virtual do que o próprio estelionatário comum, ou seja, aquele que se expõe. E assim, favorecendo que não seja identificado pela vítima, nem pelas autoridades, podendo estar atuando de qualquer lugar. E, ainda, pela própria natureza deste crime, que é o de enganar, o estelionatário provavelmente virá a se passar por uma pessoa inexistente, ou de identidade de terceiros, informando local diverso do seu paradeiro⁶⁷.

Outra problemática quanto ao estelionato praticado na Internet é a questão da competência, ou seja, sendo a Internet uma rede mundial, e não havendo tipificação penal que defina o crime de estelionato eletrônico, quais são os requisitos para que o cometimento do crime de estelionato tenha respaldo da competência brasileira, quando por exemplo utilizado meios virtuais no exterior e consumado o crime no Brasil, ou quando os meios virtuais do estelionato são produzidos no Brasil e o resultado é consumado no exterior, entre outras inúmeras possibilidades⁶⁸.

Além disso, a prática do crime de estelionato pela Internet, surge a questão da produção de provas para caracterização do delito, ou seja, por se tratar de um crime cometido com o uso de ferramentas virtuais, se torna muito mais fácil ao criminoso se desfazer das provas, ou seja, dos sites, correios eletrônicos, mensagens, dentre outras, favorecendo ainda mais a ocultação do crime, e a falta

⁶⁷ INELLAS, Gabriel César Zaccaria de. **Crimes na Internet**. São Paulo: Editora Juarez de Oliveira, 2004, p. 73–7.

⁶⁸ *Ibidem*, p. 79–84.

da comprovação de que aquele crime na versão da vítima realmente ocorrera⁶⁹.

Neste diapasão, muitas vezes o crime de estelionato pela Internet exigirá a realização de perícia criminal, pois, não adianta tão somente existir as provas do cometimento do crime, se fazendo necessário uma perícia especializada criminal de informática, com objetivo de confirmar a ocorrência do crime. O que onera mais ainda os cofres públicos, pois, muitas vezes o tempo para se fazer uma perícia é longa, e com os inúmeros casos de crimes de estelionato praticados na Internet, cria-se uma necessidade maior na contratação de mais peritos especializados para executar tais serviços⁷⁰.

Outra problemática com relação ao estelionato praticado na Internet envolve o Protocolo da Internet, também denominado TCP/IP (*Transmission Control Protocol / Internet Protocol*), significando Protocolo de Controle de Transmissão / Protocolo da Internet. Se tratando de um conjunto de número, pelo qual cada computador se tornaria identificável na rede da Internet, no entanto o criminoso experiente, como o Cracker, pode se utilizar de meios de camuflagens de seus TCP/IP para enganar. Entre os meios de camuflagens temos, o IP Sproofing e o IP Proxies⁷¹.

O IP Sproofing consiste numa técnica de camuflagem do Protocolo de Internet do computador que o criminoso está acessando, sendo utilizado o TCP/IP de outro computador, como por exemplo, de uma instituição bancária, por quem se quer fazer passar⁷².

O IP Proxy consiste numa técnica de camuflagem do Protocolo de Internet do computador que o criminoso está acessando, por meio de um programa que mascara o TCP/IP de uma rede interna ou externa, usando o servidor Proxy, ou seja, o computador que centraliza o tráfego de todos os computadores a ele ligados, inclusive o do criminoso, é identificado na rede por meio de seu TCP/IP como o computador que acessou a rede, ao invés do computador do criminoso⁷³.

Diante das questões apontadas, que envolvem o crime de estelionato praticado na Internet, com relação a autoria, a competência, a existência de provas,

⁶⁹ INELLAS, Gabriel César Zaccaria de. **Crimes na Internet**. São Paulo: Editora Juarez de Oliveira, 2004, p. 91.

⁷⁰ Ibidem, p. 97.

⁷¹ Ibidem, p. 99-100.

⁷² Ibidem, p. 100.

⁷³ Ibidem, p. 100.

a necessidade de perícia criminal especializada, a manipulação do Protocolo de Internet, temos como resultado uma necessidade social em se combater este crime de forma mais eficaz, utilizando-se de meios punitivos mais severos, com isso, deixando de aplicar a simples tipificação de estelionato disposto pelo artigo 171 do Código Penal Brasileiro, para a utilização de uma nova e eficaz tipificação ao combate do crime de estelionato eletrônico.

CONCLUSÃO

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

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

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

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

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

E, nesse sentido que se faz necessário, a atuação do Estado brasileiro, de levar maior seriedade e celeridade às propostas e aprovações de projetos de lei contra o crime de estelionato eletrônico, suprimindo esta necessidade de tipificação do crime de estelionato praticado na Internet, visando disciplinar de maneira mais clara e precisa sua conduta criminoso, bem como trazer meios punitivos mais eficazes no seu combate.

E assim, este trabalho alcança seu objetivo, trazendo um breve estudo que

demonstre ser necessária a tipificação do crime de estelionato eletrônico, com inserção de penas mais severas aos infratores.

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

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

REFERÊNCIA

- APROVADO projeto que pune crimes praticados com a utilização da internet. **O GLOBO**. Brasil, 10 jul. 2008. Disponível em: <http://oglobo.globo.com/pais/mat/2008/07/10/aprovado_projeto_que_pune_crimes_praticados_com_utilizacao_da_internet-547186659.asp>. Acesso em: 24 abr. 2009.
- BRASIL. Lei nº 11.829 de 25 de novembro de 2008. Diário **Oficial [da] República federativa do Brasil**, Poder Executivo, Brasília, DF, 26 dez. 2008. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2008/Lei/L11829.htm> Acesso em: 27 abr. 2009.
- BRASIL. Substitutivo ao Projeto de Lei do Senado nº 0076 de 2000, ao Projeto de Lei do Senado nº 0137 de 2000 e ao Projeto de Lei da Câmara nº 89 de 2003. Dispõe sobre a tipificação de condutas realizadas mediante uso de sistema eletrônico, digital ou similares, de rede de computadores, ou que sejam praticadas contra dispositivos de comunicação ou sistemas informatizados e similares. Disponível em: <http://www.senado.gov.br/comunica/agencia/pags/01.html>. Acesso em: 29 abr. 2009.
- BRASIL. Superior Tribunal de Justiça. Penal e Processo Penal. Conflito de Competência. Processo CC nº 67343 – GO. Terceira Seção. Relatora: Ministra Laurita Vaz, DF, 28 de março de 2007. Disponível em: <[http://www.stj.gov.br/SCON/jurisprudencia/toc.jsp?livre=\('%CC'.clap.+ou+'CC'.clas.\)+e+@num='67343'\)+ou+\('%CC'+adj+'67343'.suce.\)](http://www.stj.gov.br/SCON/jurisprudencia/toc.jsp?livre=('%CC'.clap.+ou+'CC'.clas.)+e+@num='67343')+ou+('%CC'+adj+'67343'.suce.)>)>. Acessado em 13 abr. 2009.
- CAPEZ, Fernando. **Curso de direito penal**: parte especial: dos crimes contra a pessoa, dos crimes contra o sentimento religioso e contra o respeito aos mortos (arts. 121 a 212), volume 2. São Paulo: Saraiva, 2003.
- ESTELIONATO. In: ENCICLOPÉDIA Saraiva do Direito. São Paulo: Saraiva, 1977, p.127.
- FURLANETO NETO, Mário; GUIMARÃES José Augusto Chaves. Crimes na Internet: elementos para uma reflexão sobre a ética informacional. **R. CEJ**, Brasília, n. 20, p. 67-73, jan./mar. 2003. Disponível em: <<http://www.cjf.jus.br/revista/numero20/artigo9.pdf>>. Acesso em: 28 abr. 2009.
- INELLAS, Gabriel César Zaccaria de. **Crimes na Internet**. São Paulo: Editora Juarez de Oliveira, 2004.
- KUROSE, James F.. **Redes de Computadores e a Internet: uma abordagem top-down**. 3. ed. São Paulo: Person Addison Wesley, 2006.
- LAQUEY, Tracy, 1963 – **O manual da Internet** – tradução insight Serviços de Informática. Rio de Janeiro: Campus, 1994.
- MIRABETE, Julio Fabbrini. **Código penal interpretado**. 4. ed. São Paulo: Atlas, 2003.

MIRABETE, Julio Fabbrini. **Manual de direito penal**. 16 ed. Volume 1. São Paulo: Atlas, 2000.

MIRABETE, Julio Fabbrini. **Manual de direito penal**. 17. ed. Volume 2. São Paulo: Atlas, 2001.

PAULINO, José Alves. **Crimes de Informática**. Brasília: Projecto Editorial, 2001.

PINTO, Carlos Alberto Ferreira. Pedofilia: Uma abordagem essencialmente jurídica. **Recanto das Letras**. São Paulo, 26 Jan. 2009. Disponível em: <<http://recantodasletras.uol.com.br/textosjuridicos/1405178>>. Acesso em: 26 abr. 2009.

PLANTULLO, Vicente Lentini. **Estelionato eletrônico**. 1ª ed. (ano 2003), 6ª tir. Curitiba: Juruá, 2008.

RIBEIRO, José Antônio Pereira. **Fraude e estelionato**. 1ª ed. São Paulo: Sugestões Literárias S/A, 1973.

SILVA, Jorge Vicente. **Estelionato e outras fraudes**. 1. ed. Curitiba: Juruá, 1995.

ANEXO – SUBSTITUTIVO AO PROJETO DE LEI DO SENADO Nº 76 DE 2000, AO PROJETO DE LEI DO SENADO Nº 176 DE 2000 E AO PROJETO DE LEI DA CÂMARA Nº 89 DE 2003

“SUBSTITUTIVO

(ao PLS 76/2000, PLS 137/2000 e PLC 89/2003)

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), a Lei nº 7.716, de 5 de janeiro de 1989, e a Lei nº 8.069, de 13 de julho de 1990, e a Lei nº 10.446, de 8 de maio de 2002, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, de rede de computadores, ou que sejam praticadas contra dispositivos de comunicação ou sistemas informatizados e similares, e dá outras providências.”

O CONGRESSO NACIONAL decreta:

Art.1º Esta Lei 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), a Lei nº 7.716, de 5 de janeiro de 1989, e a Lei nº 8.069, de 13 de julho de 1990, e a Lei nº 10.446, de 8 de maio de 2002, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, de rede de computadores, ou que sejam praticadas contra dispositivos de comunicação ou sistemas informatizados e similares, e dá outras providências.

Art. 2º O Título VIII da Parte Especial do Código Penal fica acrescido do Capítulo IV, assim redigido:

“Capítulo IV

**DOS CRIMES CONTRA A SEGURANÇA
DOS SISTEMAS INFORMATIZADOS**

Acesso não autorizado a rede de computadores, dispositivo de comunicação ou sistema informatizado

Art. 285-A. Acessar, mediante violação de segurança, rede de computadores, dispositivo de comunicação ou sistema informatizado, protegidos por expressa restrição de acesso:

Pena - reclusão, de 1 (um) a 3 (três) anos, e multa.

Parágrafo único. Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime, a pena é aumentada de sexta parte.

Obtenção, transferência ou fornecimento não autorizado de dado ou informação

Art. 285-B. Obter ou transferir, sem autorização ou em desconformidade com autorização do legítimo titular da rede de computadores, dispositivo de comunicação ou sistema informatizado, protegidos por expressa restrição de acesso, dado ou

informação neles disponível:

Pena – reclusão, de 1 (um) a 3 (três) anos, e multa.

Parágrafo único. Se o dado ou informação obtida desautorizadamente é fornecida a terceiros, a pena é aumentada de um terço.

Ação Penal

Art. 285-C. Nos crimes definidos neste Capítulo somente se procede mediante representação, salvo se o crime é cometido contra a União, Estado, Município, empresa concessionária de serviços públicos, agências, fundações, autarquias, empresas públicas ou sociedade de economia mista e subsidiárias.”

Art. 3º O Título I da Parte Especial do Código Penal fica acrescido do seguinte artigo, assim redigido:

“Divulgação ou utilização indevida de informações e dados pessoais
154-A. Divulgar, utilizar, comercializar ou disponibilizar dados e informações pessoais contidas em sistema informatizado com finalidade distinta da que motivou seu registro, salvo nos casos previstos em lei ou mediante expressa anuência da pessoa a que se referem, ou de seu representante legal.
Pena – detenção, de 1 (um) a 2 (dois) anos, e multa.
Parágrafo único. Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime, a pena é aumentada da sexta parte.”

Art. 4º O caput do art. 163 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal) passa a vigorar com a seguinte redação:

“Dano

Art. 163. Destruir, inutilizar ou deteriorar coisa alheia ou dado eletrônico alheio:
.....”(NR)

Art. 5º O Capítulo IV do Título II da Parte Especial do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal) fica acrescido do art. 163-A, assim redigido:

“Inserção ou difusão de código malicioso
Art. 163-A. Inserir ou difundir código malicioso em dispositivo de comunicação, rede de computadores, ou sistema informatizado.
Pena – reclusão, de 1 (um) a 3 (três) anos, e multa.

Inserção ou difusão de código malicioso seguido de dano

§ 1º Se do crime resulta destruição, inutilização, deterioração, alteração, dificuldade do funcionamento, ou funcionamento desautorizado pelo legítimo titular, de dispositivo de comunicação, de rede de computadores, ou de sistema informatizado:
Pena – reclusão, de 2(dois) a 4 (quatro) anos, e multa.

§ 2º Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime, a pena é aumentada de sexta parte.”

Art. 6º O art. 171 do Código Penal passa a vigorar acrescido dos seguintes dispositivos:

“Art. 171

§ 2º Nas mesmas penas incorre quem:

.....

Estelionato Eletrônico

VII – difunde, por qualquer meio, código malicioso com intuito de facilitar ou permitir acesso indevido à rede de computadores, dispositivo de comunicação ou sistema informatizado:

§ 3º Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime do inciso VII do § 2º deste artigo, a pena é aumentada de sexta parte.”

Art. 7º Os arts. 265 e 266 do Código Penal passam a vigorar com as seguintes redações:

“Atentado contra a segurança de serviço de utilidade pública

Art. 265. Atentar contra a segurança ou o funcionamento de serviço de água, luz, força, calor, informação ou telecomunicação, ou qualquer outro de utilidade pública:

..... “(NR)

“Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático, dispositivo de comunicação, rede de computadores ou sistema informatizado

Art. 266. Interromper ou perturbar serviço telegráfico, radiotelegráfico, telefônico, telemático, informático, de dispositivo de comunicação, de rede de computadores, de sistema informatizado ou de telecomunicação, assim como impedir ou dificultar-lhe o restabelecimento:

..... “(NR)

Art. 8º O caput do art. 297 do Código Penal passa a vigorar com a seguinte redação:

“Falsificação de dado eletrônico ou documento público

Art. 297. Falsificar, no todo ou em parte, dado eletrônico ou documento público, ou alterar documento publico verdadeiro:

.....”(NR)

Art. 9º O caput do art. 298 do Código Penal passa a vigorar com a seguinte redação:

“Falsificação de dado eletrônico ou documento particular

Art. 298. Falsificar, no todo ou em parte, dado eletrônico ou documento particular ou alterar documento particular verdadeiro:

.....”(NR)

Art. 10º O art. 251 do Capítulo IV do Título V da Parte Especial do Livro I do Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar), passa a vigorar acrescido do inciso VI ao seu § 1º, e do § 4º, com a seguinte redação:

“Art. 251.

§ 1º - Nas mesmas penas incorre quem:

.....

Estelionato Eletrônico

VI - Difunde, por qualquer meio, código malicioso com o intuito de facilitar ou permitir o acesso indevido a rede de computadores, dispositivo de comunicação ou a sistema informatizado, em prejuízo da administração militar

.....

§ 4º - Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime, a pena é aumentada da sexta parte.”

Art. 11º O caput do art. 259 e o caput do art. 262 do Capítulo VII do Título V da Parte Especial do Livro I do Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar), passam a vigorar com a seguinte redação:

“Dano Simples

Art. 259. Destruir, inutilizar, deteriorar ou fazer desaparecer coisa alheia ou dado eletrônico alheio, desde que este esteja sob administração militar:”(NR)

.....

.....

“Dano em material ou aparelhamento de guerra ou dado eletrônico

Art. 262. Praticar dano em material ou aparelhamento de guerra ou dado eletrônico de utilidade militar, ainda que em construção ou fabricação, ou em efeitos recolhidos a depósito, pertencentes ou não às forças armadas:”(NR)

Art. 12º O Capítulo VII do Título V da Parte Especial do Livro I do Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar), fica acrescido do art. 262-A, assim redigido:

“Inserção ou difusão de código malicioso

Art. 262-A. Inserir ou difundir código malicioso em dispositivo de comunicação, rede de computadores, ou sistema informatizado, desde que o fato atente contra a administração militar:

Pena – reclusão, de 1 (um) a 3 (três) anos, e multa.

Inserção ou difusão código malicioso seguido de dano

§ 1º Se do crime resulta destruição, inutilização, deterioração, alteração, dificuldade do funcionamento, ou funcionamento não autorizado pelo titular, de dispositivo de comunicação, de rede de computadores, ou de sistema informatizado:

Pena – reclusão, de 2 (dois) a 4 (quatro) anos, e multa.

§ 2º Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime, a pena é aumentada da sexta parte.”

Art. 13º O Título VII da Parte Especial do Livro I do Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar), fica acrescido do Capítulo VII-A, assim redigido:

“Capítulo VII-A

DOS CRIMES CONTRA A SEGURANÇA DOS SISTEMAS INFORMATIZADOS

Acesso não autorizado a rede de computadores, dispositivo de comunicação ou sistema informatizado

Art. 339-A. Acessar, mediante violação de segurança, rede de computadores, dispositivo de comunicação ou sistema informatizado, protegidos por expressa restrição de acesso, desde que o fato atente contra a administração militar:

Pena - reclusão, de 1 (um) a 3 (três) anos, e multa.

Parágrafo único. Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime, a pena é aumentada de sexta parte.

Obtenção, transferência ou fornecimento não autorizado de dado ou informação

Art. 339-B. Obter ou transferir, sem autorização ou em desconformidade com autorização do legítimo titular da rede de computadores, dispositivo de comunicação ou sistema informatizado, protegidos por expressa restrição de acesso, dado ou informação neles disponível, desde que o fato atente contra a administração militar:

Pena – reclusão, de 1 (um) a 3 (três) anos, e multa.

Parágrafo único. Se o dado ou informação obtida desautorizadamente é fornecida a terceiros, a pena é aumentada de um terço.

“Divulgação ou utilização indevida de informações e dados pessoais

Art. 339-C Divulgar, utilizar, comercializar ou disponibilizar dados e informações pessoais contidas em sistema informatizado sob administração militar com finalidade distinta da que motivou seu registro, salvo nos casos previstos em lei ou mediante expressa anuência da pessoa a que se referem, ou de seu representante legal.

Pena – detenção, de um a dois anos, e multa.

Parágrafo único - Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática de crime, a pena é aumentada da sexta parte.”

Art. 14º O caput do art. 311 do Capítulo V do Título VII do Livro I da Parte Especial do Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar), passa a vigorar com a seguinte redação:

“Falsificação de documento

Art. 311. Falsificar, no todo ou em parte, documento público ou particular, ou dado eletrônico ou alterar documento verdadeiro, desde que o fato atente contra a administração ou o serviço militar:”(NR)

Art. 15º Os incisos II e III do art. 356 do Capítulo I do Título I do Livro II da Parte Especial do Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar), passa a vigorar com a seguinte redação:

“CAPÍTULO I

DA TRAIÇÃO

Favor ao inimigo

Art. 356.:

II - entregando ao inimigo ou expondo a perigo dessa consequência navio, aeronave, fôrça ou posição, engenho de guerra motomecanizado, provisões, dado eletrônico ou qualquer outro elemento de ação militar;

III - perdendo, destruindo, inutilizando, deteriorando ou expondo a perigo de perda, destruição, inutilização ou deterioração, navio, aeronave, engenho de guerra motomecanizado, provisões, dado eletrônico ou qualquer outro elemento de ação militar.”(NR)

Art. 16º Para os efeitos penais considera-se, dentre outros:

I – dispositivo de comunicação: qualquer meio capaz de processar, armazenar, capturar ou transmitir dados utilizando-se de tecnologias magnéticas, óticas ou qualquer outra tecnologia;

II – sistema informatizado: qualquer sistema capaz de processar, capturar, armazenar ou transmitir dados eletrônica ou digitalmente ou de forma equivalente;

III – rede de computadores: o conjunto de computadores, dispositivos de comunicação e sistemas informatizados, que obedecem a um conjunto de regras, parâmetros, códigos, formatos e outras informações agrupadas em protocolos, em nível topológico local, regional, nacional ou mundial através dos quais é possível trocar dados e informações;

IV – código malicioso: o conjunto de instruções e tabelas de informações ou qualquer outro sistema desenvolvido para executar ações danosas ou obter dados ou informações de forma indevida;

V – dados informáticos: qualquer representação de fatos, de informações ou de conceitos sob forma suscetível de processamento numa rede de computadores ou dispositivo de comunicação ou sistema informatizado;

VI – dados de tráfego: todos os dados informáticos relacionados com sua comunicação efetuada por meio de uma rede de computadores, sistema informatizado ou dispositivo de comunicação, gerados por eles como elemento de uma cadeia de comunicação, indicando origem da comunicação, o destino, o trajeto, a hora, a data, o tamanho, a duração ou o tipo do serviço subjacente.

Art. 17º Para efeitos penais consideram-se também como bens protegidos o dado, o dispositivo de comunicação, a rede de computadores, o sistema informatizado.

Art. 18º Os órgãos da 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.

Art. 19º O inciso II do § 3º do art. 20 da Lei nº 7.716, de 5 de janeiro de 1989, passa a vigorar com a seguinte redação:

“Art. 20

§ 3º

II – a cessação das respectivas transmissões radiofônicas, televisivas, eletrônicas, ou da publicação por qualquer meio.

..... “(NR)

Art. 20º O caput do art. 241 da Lei nº 8.069, de 13 de julho de 1990, passa a vigorar com a seguinte redação:

“Art. 241. Apresentar, produzir, vender, receptar, fornecer, divulgar, publicar ou armazenar consigo, por qualquer meio de comunicação, inclusive rede mundial de computadores ou Internet, fotografias, imagens com pornografia ou cenas de sexo explícito envolvendo criança ou adolescente:

..... “(NR)

Art. 21º O art. 1º da Lei nº 10.446, de 8 de maio de 2002 passa a vigorar com a seguinte redação:

“Art. 1º

V – os delitos praticados contra ou mediante rede de computadores, dispositivo de comunicação ou sistema informatizado.

.....”(NR)

Art. 22º O responsável pelo provimento de acesso a rede de computadores mundial, comercial ou do setor público é obrigado a:

I – manter em ambiente controlado e de segurança, pelo prazo de três anos, com o objetivo de provimento de investigação pública formalizada, os dados de endereçamento eletrônico da origem, hora, data e a referência GMT da conexão efetuada por meio de rede de computadores e fornecê-los exclusivamente à autoridade investigatória mediante prévia requisição judicial;

II – preservar imediatamente, após requisição judicial, outras informações requisitadas em curso de investigação, respondendo civil e penalmente pela sua absoluta confidencialidade e inviolabilidade;

III – informar, de maneira sigilosa, à autoridade competente, denúncia que tenha recebido e que contenha indícios da prática de crime sujeito a acionamento penal público incondicionado, cuja perpetração haja ocorrido no âmbito da rede de computadores sob sua responsabilidade.

§ 1º Os dados de que cuida o inciso I deste artigo, as condições de segurança de sua guarda, a auditoria à qual serão submetidos e a autoridade competente responsável pela auditoria, serão definidos nos termos de regulamento.

§ 2º O responsável citado no caput deste artigo, independentemente do ressarcimento por perdas e danos ao lesado, estará sujeito ao pagamento de multa variável de R\$ 2.000,00 (dois mil reais) a R\$ 100.000,00 (cem mil reais) a cada requisição, aplicada em dobro em caso de reincidência, que será imposta pela autoridade judicial desatendida, considerando-se a natureza, a gravidade e o prejuízo resultante da infração, assegurada a oportunidade de ampla defesa e contraditório.

§ 3º Os recursos financeiros resultantes do recolhimento das multas estabelecidas neste artigo serão destinados ao Fundo Nacional de Segurança Pública, de que trata a Lei nº 10.201, de 14 de fevereiro de 2001.

Art. 23º Esta Lei entrará em vigor cento e vinte dias após a data de sua publicação.”