LUIS GUILHERME DE MATOS FEITOZA

CRIMES CIBERNÉTICOS: O ESTELIONATO VIRTUAL.

Monografia apresentada ao curso de Graduação em Direito da Universidade Católica de Brasília, como requisito parcial para obtenção do Título de Bacharel em Direito.

Autor: Luis Guilherme de Matos Feitoza

Orientador: Prof Esp. Hailton da Silva Cunha

Brasília
2012

DEDICATÓRIA

Dedico esta monografia inicialmente a meus pais e irmãos, que estiveram sempre ao meu lado durante toda esta trajetória, me fazendo crer que o sonho pode tornar real quando batalhamos com seriedade por ele. Dedico também a todos que contribuíram de alguma forma para que isto fosse possível, em especial todos os colegas de classe, que foram incentivadores de minha prosperidade.

AGRADECIMENTO

Agradeço primeiramente a Deus por estar ao meu lado todo o tempo e ter me concedido a oportunidade de estar aqui hoje, finalizando mais uma etapa de minha vida. A meus pais, irmãos, amigos e em especial minha namorada, que me incentivou e me apoiou em inúmeros momentos desta jornada. A todos vocês meus sinceros agradecimentos.

EPÍGRAFE

“Determinação coragem e autoconfiança
são fatores decisivos para o sucesso.
Se estamos possuídos por uma inabalável
determinação conseguiremos superá-los.
Independentemente das circunstâncias,
devemos ser sempre humildes, recatados
e despidos de orgulho.”
Dalai Lama.

RESUMO

Referência: FEITOZA, Luis Guilherme de Matos. **Título: Crimes Cibernéticos**: Estelionato Virtual. 2012. 70 p. Direito. UCB. Brasília. 2012.

O estudo do presente trabalho de conclusão de curso baseia-se na investigação do tipo penal do estelionato praticado na internet. Expõe um breve relato histórico sobre o surgimento da rede mundial de computadores no Brasil e no mundo e elucida algumas questões pertinentes. Ilustra como os usuários que navegam na grande rede podem se proteger de possíveis ataques e lesões causadas pelos delinquentes virtuais. Apresenta de forma direta e sucinta todos os assuntos relativos aos cibercrimes e a maneira com que os transgressores agem para fraudar suas vítimas. Versa sobre sua aplicação penal e os incontáveis prejuízos causados à sociedade. Traz a forma como ele é cometido e os meios jurídicos existentes para reprimir e punir esta conduta. Faz menção a outros delitos informáticos recorrentes na internet e aponta o posicionamento dos tribunais a respeito deles. Comenta a importância dos projetos de leis que tramitam no Congresso Nacional e demonstra a carência de leis penais para tipificar e penalizar os indivíduos que incidem nesta técnica criminosa.

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

ABSTRACT

The study of the present course conclusion work based itself in the inquiry of larceny committed on the internet. It exposes a brief historical about the emergence of the world net of computers in Brazil and in the world and explains some relevant questions. It illustrates as the users that sail in the big net are able to protected itself for possible attacks and cheats caused by the virtual delinquents. It presents of succinct and straight form all the relative matters to the cyber crimes and the way with that the transgressors act for defraud its victims. It is about penal application and the countless damages caused to the society. It brings the form as it is made and the existing legal means for repress and punish this conduct. It does mention to others recurring processed cyber crimes in the internet and aims the positioning of the courts as to them. It comments the importance of the projects of laws that are processed in the National Congress and demonstrate the lack of penal laws for typify and penalize the individuals that incident in this technical criminal.

Key words: Internet. Penal Law. Larceny Committed.

LISTA DE SIGLAS

ARPA -- *Advanced Research Projects Agency*

ARPAnet -- *Advanced Research Projects Agency Network*

ART. -- Artigo

BOL -- Brasil *On Line*

CBT – Código Brasileiro de Telecomunicações

CCJ – Comissão de Constituição E Justiça

CCT -- Comissão de Ciência, Tecnologia, Inovação, Comunicação e Informática

CF – Constituição Federal

CONIN – Conselho Nacional de Informática e Automação

CONTEL – Conselho Nacional de Telecomunicações

CPB – Código Penal Brasileiro

EMBRATEL – Empresa Brasileira de Telecomunicações

HTTP -- *Hyper Text Transfer Protocol*

HTTPS -- Hyper Text Transfer Protocol Secure

IBI -- I*ntergovernamental Bureau for Informatics*

LAN – *Local Area Network*

MILNET -- *Military Network*

MINICOM – Ministério das Comunicações

NOMIC - Nova Ordem Mundial da Informação e da Comunicação

OEA – Organização dos Estados Americanos

PL – Projeto de Lei

PLC – Projeto de Lei da Câmara

PLS – Projeto de Lei do Senado

PMDB – Partido do Movimento Democrático Brasileiro

PSDB – Partido da Social Democracia Brasileira

PT – PARTIDO DOS TRABALHADORES

RNP – Rede Nacional de Ensino e Pesquisa

SEI -- Secretaria Especial de Informática

SNT – Sistema Nacional de Telecomunicações

TCP -- *Transmission Control Protocol*

TCP/IP -- *Transmission Control Protocol / Internet Protocol*

UNESCO -- Organização das Nações Unidas para a Educação, Ciência e Cultura.

UOL – Universo *On line*

URL -- Uniform Resource Locator

WAN -- *Wide Area Network*

WWW – *World Wide Web*

SUMÁRIO

INTRODUÇÃO

O direito se faz presente em cada momento da vida dos indivíduos que vivem em um estado regido pela democracia, como é o caso do Brasil. Ele tem sido responsável ao longo do tempo por dar soluções aos conflitos interpessoais e institucionais que advém de uma sociedade moderna, que avança em ritmo acelerado, devido às inúmeras descobertas e melhorias tecnológicas e científicas que visam dar facilidade e agilidade ao dia-dia de nós, cidadãos brasileiros.

Contudo, com o desenvolvimento quase que descontrolado no que tange à área tecnológica, que abrange o ramo da internet de forma genérica, alguns tipos delituosos virtuais difíceis de serem punidos foram surgindo e crescendo na mesma proporção, alastrando-se por todas as direções, tornando-se verdadeiras armadilhas aos desavisados que utilizam a rede mundial de computadores para realizar suas transações bancárias, efetuar compras, ou simplesmente checar sua caixa de e-mails.

Dentre os numerosos crimes virtuais que se afloram diariamente, um deles merece atenção especial, pois sua técnica vem se expandindo com força devastadora, vitimando e lesionando milhares de pessoas anualmente, que é o caso do estelionato cometido por intermédio da internet, objeto principal deste trabalho, onde a identificação de seus autores e sua punição ainda é algo que foge ao controle da legislação atual, haja vista não existir até o momento lei específica tipificando de forma direcionada o delito em tela, deixando os magistrados do direito muitas das vezes com as “mãos atadas” para reprimir e condenar esta conduta.

O crime de estelionato sempre existiu em nossa sociedade, desde as épocas mais remotas, e é introduzido pelo Código Penal no título referente aos crimes contra o patrimônio, onde o estelionatário obtém para si ou para outrem vantagem ilícita, induzindo ou mantendo alguém à erro. No Brasil, este tipo penal encontra-se descrito no caput do artigo 171 do Decreto-Lei nº 2.484 de 07 de dezembro de 1940 (Código Penal Brasileiro), no capítulo VI, que trata do estelionato e outras fraudes.

Entretanto, ao passar dos anos nossa sociedade evoluiu rapidamente, e juntamente com ela, surgiu à era da informática, trazendo uma série de inovações e praticidades para melhorar a vida das pessoas. Infelizmente, alguns sujeitos mal-intencionados viram na internet a possibilidade de praticar o crime tipificado no art. 171, agindo de má fé, expondo milhares de pessoas a este perigo que já se tornou

comum, levando em conta a facilidade com que ele é consumado, garantindo muitas vezes a impunidade por parte de seus praticantes.

Em linhas gerais, pode-se afirmar que o estelionato virtual é caracterizado pelo emprego de meios eletrônicos fraudulentos que de alguma forma induzem o usuário a pensar que a proposta ou o e-mail que lhe foi recebido é de fonte autêntica e idônea, o que, de fato, não ocorre.

O fraudador que insiste em praticar esta modalidade delituosa encontra em seu benefício à dificuldade que o estado possui em puni-lo, ou ao menos puni-lo de forma adequada, uma vez que alguns problemas surgem, como o desvendamento da autoria, a competência territorial para julgar o caso, a existência de provas do crime e a ausência de perícia especializada, impedindo o correto trâmite processual e inibindo também o direito ao contraditório e ampla defesa garantido constitucionalmente ao acusado.

Incontáveis reflexões sobre o direito penal informático têm sido amadurecidas para proporcionar uma “modernização” nos tipos penais que existem nos dias de hoje, pois a legislação hodierna se mostra absolutamente antiquada quanto às fraudes eletrônicas, que são colocadas em prática na maioria das vezes por pessoas com alto grau de inteligência e conhecimento na área de informática, que ao invés de utilizarem a sabedoria à qual são dotadas para beneficiar o próximo, fazem exatamente o inverso, prejudicando em sua maioria pessoas humildes e com baixa instrução escolar.

A deficiência de norma regulamentadora sobre o assunto parece contribuir para que diariamente, centenas de pessoas sejam ludibriadas por estas falsas promessas de “compra perfeita” ou de “*sites* fantásticos”, que fazem inúmeras juras milagrosas para enganar a vítima, e assim obter o lucro ou a vantagem proibida. O Brasil necessita ter um real interesse em coibir este tipo de prática em seu seio, com o intuito de acompanhar a evolução de seu povo e protege-lo de ataques virtuais de criminosos inescrupulosos que ainda persistem em cometer ilícitos deste porte.

Na busca de encontrar algumas soluções, este trabalho aponta alguns problemas basilares que serão analisados, tais quais, sejam eles: Qual a necessidade para a sociedade brasileira em se tipificar o estelionato praticado na internet, definindo-o novamente? Quais as medidas de segurança que devem ser adotadas para evitar este tipo de fraude? Qual o posicionamento dos tribunais

perante o tema?, dentre outros, não menos importantes, que serão debatidos no decorrer do mesmo.

Da mesma forma, esta monografia tem por meta apresentar um breve histórico da evolução da internet e os avanços dos recursos tecnológicos, a segurança da informação e as normas brasileiras de segurança da informação – NBR ISSO/IEC 17799, o estelionato virtual propriamente dito, bem como os projetos de lei contra os crimes virtuais existentes.

A metodologia utilizada para dar suporte ao desenvolvimento do texto consiste basicamente em pesquisa bibliográfica, artigos publicados, projetos de leis em andamento, notícias atuais acerca do tema, bem como textos publicados e devidamente registrados na internet.

CAPÍTULO I

1. O DELITO DE ESTELIONATO

1.1 CONCEITUAÇÃO JURÍDICA

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

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

> "Pesquisas recentes indicam que por volta de 500 anos antes de cristo, já existiam rumores de que alguns egípcios ludibriavam os ricos e nobres comercializando falsos felinos e outros animais embalsamados para serem utilizados nas cerimônias fúnebres, segundo a tradição religiosa daquele povo. Na verdade, as múmias eram fraudulentas, e na maioria das vezes continham em seu interior pequenos pedaços de madeira e outros objetos, que simulavam o peso e o tamanho, e em alguns casos, restos de ossada de outros animais[1]".

No Brasil, o crime de estelionato está descrito no artigo 171 do Decreto-Lei nº 2.484 de 07 de dezembro de 1940 – O Código Penal Brasileiro, abaixo aduzido:

> "Art. 171 - Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento:
> Pena - reclusão, de um a cinco anos, e multa[2]".

Quando praticado de maneira ordinária, ou seja, em sua forma típica, o crime de estelionato sintetiza-se essencialmente na possibilidade em que o autor delituoso encontra para obter proveito de modo ilícito, para si, ou para outrem, utilizando-se de

---

[1] MARQUES, Samuel. Estelionato: Prática comum ao longo da história. **Panorama Empresarial**. Resende. Setembro de 2009. Disponível em: <http://cdlresende.com.br/index.php?menu=17&jornal=5&materia=218> Acessado em: 22 de Agosto de 2012.

[2] BRASIL. **Código Penal Brasileiro**. Organização dos textos, notas remissivas e índices por Juarez de Oliveira. 46. ed. São Paulo: Saraiva, 2000.

meios fraudulentos para tanto. O ordenamento jurídico brasileiro versa que somente a pessoa física pode ser sujeito ativo do crime de estelionato, cometendo-o de forma dolosa, com livre e consciente vontade, embora possa agir de modo diverso para alcançar seus fins. Em contrapartida, o sujeito passivo desta modalidade será a vítima que sofreu o prejuízo patrimonial, devendo ser pessoa certa e determinada, embora muitas vezes exista mais de um indivíduo envolvido na relação.

O crime de estelionato é delimitado pelo binômio, vantagem ilícita/ prejuízo alheio. A vantagem ilícita é esclarecida por um proveito que não encontra amparo legal no ordenamento jurídico, sendo contrário a ele, não obedecendo ao princípio da legalidade. Se por ventura o objeto fosse lícito, o fato poderia ser desclassificado para outra infração penal, como o exercício arbitrário das próprias razões.

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

Desta forma, afirma Luiz Regis Prado:

> "Prevalece o entendimento doutrinário de que a referida vantagem não necessita ser econômica, já que o legislador não restringiu o seu alcance como o fez no tipo que define o crime de extorsão, no qual empregou a expressão indevida vantagem econômica[3]".

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

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

---

[3] PRADO, Luiz Regis. **Curso de Direito Penal Brasileiro**. Parte Especial - arts. 121 a 183. V. 2. Ed. Filiada. 2002. p. 523.

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

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

Segundo o doutrinador Mirabete,

> "O artifício existe quando o agente se utiliza de um aparato que modifica, ao menos aparentemente, o aspecto material da coisa, figurando entre esses meios o documento falso ou outra falsificação qualquer, o disfarce, a modificação por aparelhos mecânicos ou elétricos, filmes, efeitos de luz, etc[4]".

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

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

> "Discute-se, na aferição da idoneidade do meio empregado, se deve ser levada em consideração a prudência ordinária, o discernimento do *homo medius,* ou a pessoa da vítima, concluindo os doutrinadores por esta ultima hipótese. Embora já se tenha decidido que as manobras fraudulentas devem ser suficientes para embair a média argúcia, a prudência normal, aquele mínimo de sagacidade que a pessoa comum usa em seus negócios, é francamente predominante a jurisprudência de que a idoneidade do meio deve ser pesquisada no caso concreto, inclusive, tendo-se em vista as condições pessoais da vítima[5]".

---

[4] MIRABETE, Júlio Fabbrini. **Código penal interpretado**. 4. ed. São Paulo: Atlas, 2003. p.1348.
[5] Idem; **Manual de direito penal**. 20. ed. São Paulo: Atlas, 2003, p. 304.

1.2DA APLICAÇÃO PENAL

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

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

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

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

Nesse sentido, preleciona Nelson Hungria:

> “Há uma analogia substancial entre o induzimento em erro e o doloso silencio em torno do erro preexistente. Praticamente, tanto faz ministrar o veneno como deixar scienter que alguém o ingira por engano (...). A inércia é uma spécies do genus “ação”, é a própria atividade que se refrange sobre si mesma, determinando-se ao non facere. Tanto usa de fraude quem ativamente causa um erro para um fim ilícito, quanto quem passivamente deixa-o persistir e dele se aproveita[6]”.

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

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

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

> "Art. 89. Nos crimes em que a pena mínima cominada for igual ou inferior a um ano, abrangidas ou não por esta Lei, o Ministério Público, ao oferecer a denúncia, poderá propor a suspensão do processo, por dois a quatro anos, desde que o acusado não esteja sendo processado ou não tenha sido condenado por outro crime, presentes os demais requisitos que autorizariam a suspensão condicional da pena.
>
> § 1º Aceita a proposta pelo acusado e seu defensor, na presença do Juiz, este, recebendo a denúncia, poderá suspender o processo, submetendo o acusado a período de prova, sob as seguintes condições:
>
> I - reparação do dano, salvo impossibilidade de fazê-lo;
>
> II - proibição de frequentar determinados lugares;
>
> III - proibição de ausentar-se da comarca onde reside, sem autorização do Juiz;
>
> IV - comparecimento pessoal e obrigatório a juízo, mensalmente, para informar e justificar suas atividades[7]".

[7] BRASIL. BRASIL. **Lei 9.099**, de 26 de Setembro de 1995. Dispõe sobre os Juizados Especiais Cíveis e Criminais. Diário Oficial [da] Republica Federativa do Brasil. Brasília, DF, 27 Set. 1995. Disponível em: <http://www.in.gov.br/mp_leis/leis_texto.asp?Id=LEI%209887>. Acesso em: 22 de Setembro de 2012.

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

O sentido real da concessão de suspensão condicional do processo é evitar que o agente entre em contato de perto com o sistema carcerário, alterando seu convívio social e seu ciclo de amizades, haja vista o sistema penitenciário nacional carecer de assistência sob diversos ângulos, afinal, as estatísticas comprovam que na maioria dos estados, mais de 90% dos criminosos que recebem a liberdade, voltam a delinquir[8].

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

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

> "O réu sendo condenado no crime de estelionato terá a fixação da pena aplicada pelo Juiz, por meio da dosimetria da pena, disciplinado no artigo 68 do Código Penal, tratando-se de um sistema trifásico sendo observado primeiramente os critérios do artigo 59 deste dispositivo legal, seguido das considerações quanto às circunstâncias atenuantes e agravantes, e por último as causas de diminuição e de aumento da pena[9]".

A primeira fase deste sistema de cálculo de pena é a computação da pena-base, que deverá ser realizada de acordo com o mínimo e o máximo legal permitido,

[8] http://fiorisemcensura.com.br/?p=5427.
[9] SILVA, Jorge Vicente. **Estelionato e outras fraudes**. Curitiba: Juruá, 1995, p. 55.

obedecendo ao inciso II do artigo 59 do código penal, que, no caso do estelionato, a pena mínima será de um ano e a máxima de cinco anos, em conformidade com o artigo 171 deste mesmo diploma legal.

Esta fase inicial do sistema de cálculo é crucial para que se ajuste a pena à conduta individual do acusado, fazendo com que a punição seja equitativa ao ato praticado. É nesta fase que o juiz irá identificar qual o regime inicial de cumprimento de pena, que no caso do estelionato, é o de reclusão, podendo ser executada no regime fechado, semi-aberto ou aberto.

Outro ponto relevante para o cálculo é a análise das circunstâncias judiciais que se encontram dispostas no art. 59 do Código Penal, que contribuem para uma pena-base mais justa, livre de vícios que possam prejudicar o acusado.

> "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 levou o acusado a cometer este delito; as circunstâncias e consequências do crime, referindo-se as circunstâncias quanto à forma e o meio com o qual se praticou o crime, e as consequências 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 vítima[10]".

As circunstâncias judiciais consistem na coleta de dados objetivos e subjetivos que fazem parte do fato ilícito, agregando-se a ele sem modificar sua essência. O crime é um acontecimento que não pode ser separado das particularidades que o acompanham, assim, as circunstancias judiciais são dados que se juntam ao delito, não alterando-o substancialmente, embora seus efeitos e consequências sejam relevantes.

As circunstâncias constantes no artigo 59 do Código Penal são respectivamente: (1) culpabilidade, (2) antecedentes, (3) conduta social, (4) personalidade do agente, (5) motivos do crime, (6) circunstâncias do crime, (7) consequências do crime, e, por derradeiro, (8) comportamento da vítima.

Em se tratando de estelionato, o magistrado deverá atentar-se para o fato descrito no parágrafo primeiro do art. 171 do Código Penal, que faz uma ressalva quanto à primariedade do agente e o pequeno valor do prejuízo, dosando

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

adequadamente a pena-base. O parágrafo primeiro do art. 171 determina, *in verbis: "*§ 1º - Se o criminoso é primário, e é de pequeno valor o prejuízo, o juiz pode aplicar a pena conforme disposto no artigo 155, § 2º[11]".

O parágrafo segundo art. 155 do Código Penal diz respeito ao delito de furto, e propicia o benefício acima citado ao criminoso que preencha os requisitos. Na hipótese do estelionato, a redação do dispositivo faz menção ao prejuízo de pequeno valor, e, neste caso, deve-se levar em consideração a condição pessoal da vítima, ao contrário do que ocorre no furto, que leva em conta o valor do objeto subtraído. Sendo assim, se o infrator for primário e o prejuízo for de pequeno valor, que deve girar em torno de um salário mínimo, o juiz poderá alterar a pena de reclusão para a de detenção, diminuindo-a de um a dois terços ou aplicar somente a multa.

Após definir qual será a pena-base, o julgador passará para o segundo estágio do processo de dosimetria da pena, que é a análise das circunstâncias agravantes e atenuantes, que podem vir a beneficiar ou a prejudicar o réu. O código penal ensina que a pena sempre será majorada ou diminuída, embora não defina qualquer valor fixo ou variável para que isto seja feito. Essas circunstâncias são dados acessórios que giram em torno da figura típica do crime, e sua finalidade principal é aumentar ou diminuir a pena que será aplicada ao condenado.

Embora permaneçam ao lado da definição típica, as circunstâncias não interferem em nada na definição jurídica ou legal do delito penal. Os artigos 61 a 67 do Código Penal Brasileiro são norteadores para o operador do direito no momento da aplicação das agravantes e atenuantes que irão incidir sobre o ilícito, devendo o juiz observar obrigatoriamente seu conteúdo para que a sentença final cumpra todos os seus requisitos de validade.

Frise-se que o Código Penal não forneceu em seu texto nenhuma informação no que tange ao *quantum* para fins de atenuação ou agravação da pena, contrariando o que ocorre nas causas de aumento e diminuição de pena, que serão analisados no terceiro momento deste processo trifásico previsto no art. 68 do repressivo diploma. Neste caso, a lei ensina que a dosagem será feita com base em *frações*, que serão apresentadas no próprio preceito secundário do tipo penal. Não

[11] BRASIL. **Código Penal Brasileiro**. Organização dos textos, notas remissivas e índices por Juarez de Oliveira. 46. ed. São Paulo: Saraiva, 2000.

obstante a ausência de delimitação legal para agravar ou atenuar a pena-base, tal apreciação deve ser feita pautada nos princípios da proporcionalidade e razoabilidade previstos na lei penal, garantindo a fluidez da pena ao sentenciado.

Como bem observa Cezar Roberto Bitencourt:

> "O código não estabelece a quantidade de aumento ou de diminuição das agravantes e atenuantes legais genéricas, deixando-as a discricionariedade do juiz. No entanto, sustentamos que a variação destas circunstâncias não deve ir muito além do limite mínimo das majorantes e minorantes, que é fixado em um sexto. Caso contrário, as agravantes e as atenuantes se equipariam àquelas causas modificadoras da pena, que, a nosso juízo, apresentam maior intensidade, situando-se pouco abaixo das qualificadoras (no caso das majorantes)[12]".

As circunstâncias agravantes estão descritas no art. 61 do Código Penal, e são elas: (1) - a reincidência, (2) - ter o agente cometido o crime: a) por motivo fútil ou torpe; b) para facilitar ou assegurar a execução, a ocultação, a impunidade ou vantagem de outro crime; c) à traição, de emboscada, ou mediante dissimulação, ou outro recurso que dificultou ou tornou impossível a defesa do ofendido; d) com emprego de veneno, fogo, explosivo, tortura ou outro meio insidioso ou cruel, ou de que podia resultar perigo comum; e) contra ascendente, descendente, irmão ou cônjuge; f) com abuso de autoridade ou prevalecendo-se de relações domésticas, de coabitação ou de hospitalidade, ou com violência contra a mulher na forma da lei específica; g) com abuso de poder ou violação de dever inerente a cargo, ofício, ministério ou profissão; h) contra criança, maior de 60 (sessenta) anos, enfermo ou mulher grávida; i) quando o ofendido estava sob a imediata proteção da autoridade; j) em ocasião de incêndio, naufrágio, inundação ou qualquer calamidade pública, ou de desgraça particular do ofendido; l) em estado de embriaguez preordenada.

Estas circunstâncias expostas no art. 61 demonstram um grau de reprovação maior da conduta do delinquente, que no caso do estelionato, é severamente repudiado pela sociedade, haja vista a aparente boa-fé por parte do meliante. O saudoso professor Luiz Flávio Gomes ensina que poderá ocorrer concurso de agravantes em um mesmo crime, que será resolvida da seguinte forma:

> "Note-se a possibilidade de incidirem, no mesmo caso, uma ou mais circunstâncias descritas no artigo 61 do Código Penal e que, portanto, agrava a pena e também uma ou mais circunstâncias previstas no artigo 65 do Código Penal (atenuante genérica). A isso se chama concurso de circunstâncias agravantes e atenuantes que, aliás, é prevista no Código

[12] BITENCOURT, Cezar Roberto. **Código Penal Comentado**. São Paulo: Saraiva. 2002. p. 219.

> Penal, cuja solução será: Art. 67 - No concurso de agravantes e atenuantes, a pena deve aproximar-se do limite indicado pelas circunstâncias preponderantes, entendendo-se como tais as que resultam dos motivos determinantes do crime, da personalidade do agente e da reincidência[13]".

De outro modo, as circunstancias atenuantes do delito inseridas no art. 65 do Código Penal Brasileiro, são: (1) - ser o agente menor de vinte e um, na data do fato, ou maior de setenta anos, na data da sentença; (2) - o desconhecimento da lei; (3) - ter o agente: a) cometido o crime por motivo de relevante valor social ou moral; b) procurado, por sua espontânea vontade e com eficiência, logo após o crime, evitar-lhe ou minorar-lhe as consequências, ou ter, antes do julgamento, reparado o dano; c) cometido o crime sob coação a que podia resistir, ou em cumprimento de ordem de autoridade superior, ou sob a influência de violenta emoção, provocada por ato injusto da vítima; d) confessado espontaneamente, perante a autoridade, a autoria do crime; e) cometido o crime sob a influência de multidão em tumulto, se não o provocou.

As circunstâncias atenuantes possuem exatamente a mesma característica das agravantes, contudo, seguem em sentidos opostos, uma vez que aquela orienta na redução da pena, quando presentes os requisitos no caso concreto.

Por fim, o magistrado ao concluir a fixação da pena-base e a análise das circunstâncias agravantes e atenuantes, passará automaticamente para o terceiro e último estágio de aplicação da penalidade, obedecendo sempre ao sistema trifásico de dosimetria. Em se tratando especificadamente do estelionato, é nesta fase que poderá ser concedido o benefício ao réu de substituição de pena privativa de liberdade por alguma restritiva de direito, que será explicitado posteriormente.

As causas de aumento e diminuição de pena estão espalhadas ao longo do código penal em sua parte geral e especial. São de observância obrigatória para que se finalize o processo de aplicação da pena, pois sua carência pode dar ensejo à anulação da sentença. Estas causas possuem a capacidade de aumentar a pena além daquilo que lhe é prevista ou diminui-la aquém do mínimo previsto em lei, a depender do fato concreto. Através desta possibilidade, as causas de aumento e diminuição de pena não ficam restritas ao limite estipulado pela pena do crime cometido, podendo ganhar novas interpretações após a apreciação.

---

[13] GOMES, Luiz Flavio. SOUSA, Áurea Maria Ferraz de. **Agravantes e atenuantes: preponderância das circunstâncias subjetivas. Críticas**. Ago. 2010. Disponível em: <http://www.lfg.com.br>. Acessado em: 13 Set. 2012.

Estas causas não podem ser confundidas com as atenuantes e agravantes, uma vez que estas não possuem explicitação no código e dizem respeito a certas circunstâncias contidas na parte geral, e aquelas são aplicadas com embasamento no resultado final do crime, sendo elencadas ora na parte geral, ora na parte especial.

Neste sentido, o honrável doutrinador Damásio de Jesus esclarece:

> "Na primeira fase o juiz fixa a pena-base em consideração as circunstâncias judiciais, na segunda, faz incidir as agravantes e atenuantes, na terceira, eventuais causas de aumento e diminuição de pena (parte geral ou especial). Ao contrário do que ocorre em face das circunstancias agravantes e atenuantes, incidindo uma causa de aumento ou diminuição, a pena pode ultrapassar o máximo abstrato ou ficar aquém do mínimo abstrato[14]".

As causas de aumento e diminuição inseridas no Código Penal Brasileiro em sua parte geral são chamadas de variáveis, como exemplo o artigo 14 parágrafo único, artigo 16, artigo 21 "*in fine*", entre outros. Já as causas constantes na parte especial são batizadas de "quantidade fixa", com é o caso do artigo 121, § 4º, 122 parágrafo único e do artigo 127, artigo 129, § 7º. As principais causas de aumento de pena da parte geral são: o concurso formal (artigo 70 código penal) e a continuidade delitiva (artigo 71 código penal) e as mais recorrentes para diminuição de pena, são: a tentativa (artigo 14, II código penal), o arrependimento posterior (artigo 16 código penal), o erro inevitável sobre a ilicitude do fato (artigo 21 código penal) e a participação de menor importância (artigo 29 § 1º código penal).

Poderá ocorrer a concorrência de mais de uma causa de aumento ou diminuição de pena no mesmo fato típico, todavia, o conflito aparente deverá ser resolvido em consonância com o parágrafo único do artigo 68 do Código Penal Brasileiro, que o juiz pode limitar-se a um só aumento ou uma só diminuição, utilizando a causa que mais aumente ou mais diminua.

Nesta derradeira fase, o julgador poderá beneficiar o réu que esteja respondendo pelo estelionato com a suspensão condicional da pena, desde que preencha os requisitos, dentre os quais, não ter sido condenado a pena superior a dois anos, não ser reincidente em crime doloso e possuir as circunstancias judiciais favoráveis, poderá ter a pena suspensa por um período de 2 a 4 anos, conforme

---

[14] JESUS, Damásio E. de. **Direito Penal**. 1° Volume - Parte Geral, 20ª ed., São Paulo: Editora Saraiva, 1997. pág. 576.

prevê o artigo 77 do Código Penal, respeitando também as exigências dos parágrafos 1º e 2º do artigo 78 do mesmo dispositivo.

Neste seguimento, se faz mister esclarecer a diferença entre suspensão condicional da pena e suspensão condicional do processo, tarefa bem explicitada por Thiago Lauria, em um texto publicado na internet:

> "Muitas são as semelhanças, grandes também são as diferenças existentes entre essas duas figuras penais". A primeira delas se encontra no próprio diploma legal em que se encontram previstas. O *sursis* está previsto no art. 77 do Código Penal Brasileiro, tendo sido introduzido no ordenamento jurídico nacional a partir da Reforma de 1984. A suspensão condicional do processo, por sua vez, se encontra no art. 89 da Lei n° 9.099/95, que trata dos Juizados Especiais Cíveis e Criminais.
> Na suspensão condicional do processo, o réu aceita o benefício logo após o oferecimento da denúncia. A suspensão é o resultado entre um acordo de vontades entre as partes, homologado pelo juiz. Não há que se falar, portanto, em condenação. O contrário, contudo, ocorre com o *sursis*. Nesse último caso, o processo de desenvolve normalmente, e culmina com a prolação de uma sentença penal condenatória. Ou seja, o réu é condenado por sentença com trânsito em julgado. Apenas a execução da pena permanece suspensa[15]".

Após o exposto, é importante dizer que a ação penal do crime de estelionato é em regra pública e incondicionada, isto quer dizer que a vítima não poderá fazer qualquer tipo de objeção quando da iniciação do processo penal, inexistindo a possibilidade de desistência ou retirada da denúncia, devendo o Ministério Público e demais autoridades se manifestar quanto à elucidação dos fatos. Os artigos 181 e 182 do CPB trazem à tona as hipóteses possíveis a serem aplicadas quando houver isenção de pena (escusas absolutórias), bem como as possibilidades cabíveis para que a ação penal dependa de representação da vítima.

[15] LAURIA, Thiago. Suspensão Condicional da Pena X Suspensão Condicional do Processo. Disponível em: <http://www.jurisway.org.br/v2/dhall.asp?id_dh=143 >. Acessado em: 03 de Setembro de 2012.

CAPÍTULO II

2. A REDE MUNDIAL DE COMPUTADORES E OS CRIMES VIRTUAIS

2.1 BREVE HISTÓRICO DO SURGIMENTO DA INTERNET

Conforme acertadamente asseverou o saudoso Professor Eric Schimidt: “A internet é a primeira coisa que a humanidade criou e não entende, a maior experiência de anarquia que jamais tivemos[16]”. (Ex-executivo da *Sun Microsystems* e atual presidente da Novel).

É fato que a rede mundial de computadores (internet) é o meio de comunicação em massa mais difundido na população nos últimos anos, haja vista sua capacidade infindável e muitas vezes ilimitada de facilitar e modernizar a vida das pessoas que convivem em uma sociedade.

Atualmente, os comentários acerca da internet não se restringem apenas à sua capacidade tecnológica, mas também a quantidade de usuários que utilizam este meio universal de informação.

Criada inicialmente com fins exclusivamente militares, a internet servia como base de apoio para as comunicações feitas entre as forças de ataque norte-americanas em casos de investidas inimigas que pudessem por em risco as informações captadas e emitidas pelos meios convencionais. A internet teve seu nascimento precisamente no mesmo momento em que eclodia a guerra fria, em meados da década de 1960, logo após o termino da Segunda Guerra Mundial, ocasião em que os Estados Unidos da América e a União Soviética disputavam o comando político, econômico e militar em todo o mundo.

Sentindo-se extremamente acuada e impotente no que diz respeito a qualidade e eficiência de transmissão de informação perante os russos, que haviam acabado de lançar à órbita o Sputnik - o primeiro satélite artificial existente à época, da União Soviética, concebida primeiramente com a funcionalidade de estudar a capacidade de lançamento de cargas úteis para o espaço e os efeitos sofridos pela ausência de peso e radiação sobre os organismos vivos; compelindo os EUA a

[16] apud SILVEIRA, Renato de Mello Jorge. **Direito penal supra-individual**: interesses difusos. São Paulo: Revista dos Tribunais, 2003.

fundar uma agência específica para estudar e desenvolver uma tecnologia igual ou superior a dos soviéticos, afastando sua ruína na guerra.

Neste sentido, Fabrízio Rosa ensina que:

> "A fagulha que acabaria por acender a revolução da conectividade ocorreu em 1957, quando a União Soviética pôs em orbita o primeiro satélite espacial, o Sputnik: quatro meses depois, o presidente americano Dwight Eisenhower anunciava a criação de uma agencia federal norte-americana, nos moldes da NASA, conhecida como Advanced Research Projects Agency- ARPA, com a missão de pesquisar e desenvolver alta tecnologia para as forças armadas[17]".

A *Advanced Research Projects Agency* – ARPA foi a agência do governo americano que desempenhava ações destinadas às pesquisas militares de cunho tecnológico que atuavam em defesa do território estadunidense, com a finalidade de prevenir as surpresas tecnológicas de outros países e atuar como mecanismo de pesquisa de alto grau de risco, dedicando-se a apreciação de guerrilha tecnológica.

O governo americano ao desenvolver a ARPA, observou a necessidade de criar uma subdivisão desta agencia para tratar de assuntos exclusivos e sigilosos, que recebeu o nome de ARPAnet, que operava por intermédio de diversas e inúmeras redes locais privadas e de baixo alcance batizadas de LAN (*Local Area Network*), que tinha o objetivo de agrupar as informações contidas no banco de dados das bases militares e do departamento de pesquisa do governo americano e enviá-las as partes interessadas.

O conceituado professor Gabriel Cesar ensina que:

> "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 contínua[18]".

---

[17] ROSA, Fabrízio. **Crimes de Informática.** 2º ed. Campinas: Bookseller, 2005. p. 31.

[18] INELLAS, Gabriel César Zaccaria de. **Crimes na Internet**. 2º ed., atualizada e ampliada. São Paulo: Editora Juarez de Oliveira, 2009. p.1.

Ressalte-se que a ARPAnet foi financiada integralmente pelo governo norte-americano. Utilizando-se de uma *backbone*, link de alta velocidade, usado geralmente como “espinha dorsal” de grandes redes. A internet é formada por inúmeros *backbones* que interligam as redes de universidades, empresas, provedores de acesso, entre outros[19]. O *backbone*, tradução de "espinha dorsal", é uma rede principal por onde passam os dados dos clientes da internet. No Brasil, as empresas BrasilTelecom, Telecom Italia, Telefônica, Embratel, *Global Crossing* e a Rede Nacional de Ensino e Pesquisa (RNP) prestam esse serviço. Essa mesma rede também é responsável pelo envio e recebimento de dados entre grandes cidades e até entre Brasil e outros países, que era cabeado por debaixo do chão, a ARPAnet possuía a capacidade de conectar os militares e os investigadores sem que eles estivessem em um local fixo, podendo ser encontrados em qualquer lugar que houvesse cobertura a referida tecnologia.

Esse avanço tecnologico era capaz de evitar a perda de informações em casos de bombardeio, por exemplo, ficando resguardado o que já estava armazenado no banco de dados.

Por volta de 1970, a internet passou a ser disponibilizada para o uso acadêmico e científico no âmbito das instituições que eram destinadas a este fim, onde ela funcionava como auxiliadora para troca de mensagens e compartilhamento de informações entre os estudantes e professores. Esta disponibilização da internet para o meio academico e cientifico foi o ponta-pé inicial para que este meio de comunicaçao se expandise cada vez mais, evoluindo-se até os dias atuais.

Foi também em 1970 que foi desenvolvido o primeiro padrão de protocolo diverso daquele fornecido pela ARPAnet, que trazia à tona uma nova modalidade e formato de mensagens que possuiam uma série regras para envio e recebimento de informações entre computadores, sendo intermediada por hospedeiros, que conduziam os dados entre as máquinas conectadas à rede. Em informática, *host* ou hospedeiros, é qualquer máquina ou computador conectado a uma rede, podendo oferecer informações, recursos, serviços e aplicações aos usuários ou outros nós na rede, os hosts variam de computadores pessoais a supercomputadores, dentre outros equipamentos, como roteadores. Os hospedeiros nada mais eram do que os

[19] http://pt.wikipedia.org/wiki/Backbone. Acessado em: 15 Set. 2012.

sitios, ou *sites*, que guardavam as informações em páginas da internet e as enviavam/recebiam para seus usuários, formando assim um “cofre” de informações.

O ilustre doutor Gabriel César Zaccaria descreve suscintamente em que consiste o protocolo utilizado pela rede mundial de computadores da seguinte forma:

> “Protocolo é a designação dada aos formatos de mensagens e suas regras, entre dois computadores, para que possa haver troca de mensagens. Vale dizer que o protocolo permite a comunicação entre os dois comunicadores[20]”.

No fim do ano de 1972, um estudioso famoso conhecido por Ray Tomlinson desenvolveu o correio eletrônico, hoje popularmente conhecido como e-mail.

> “Correio eletrônico ou ainda *e-mail* ou *correio-e* é um método que permite compor, enviar e receber mensagens através de sistemas eletrônicos de comunicação. O termo *e-mail* é aplicado tanto aos sistemas que utilizam a Internet e são baseados no protocolo SMTP, como aqueles sistemas conhecidos como *intranets*, que permitem a troca de mensagens dentro de uma empresa ou organização e são, normalmente, baseados em protocolos proprietários[21]”.

O correio eletrônico inovou e revolucionou mais uma vez este imenso universo virtual, pois ele permitia que seus usuários não só trocassem mensagens, mas também que pudessem armazená-las para consulta posterior. Os primeiros países a utilizarem este mecanismo foram a Inglaterra e a Noruega, que interligaram-se na mesma rede, tornando a comunicação por e-mail um fenômeno global.

Um ano após a criação do correio eletrônico, foi criado um protocolo especifico para a transferência de arquivo, visando dar suporte e efetivar ainda mais a correspondência de arquivos e informações na internet. O protocolo recebeu o título de FTP – Protocolo de Transferência de Arquivos, que oferecia um meio de se transferir os arquivos e compartilha-los remotamente. O FTP ainda é utilizado nos dias atuais, principalmente no âmbito acadêmico das universidades e faculdades de todo o mundo.

Segundo Luiz Carlos Santos,

---

[20] INELLAS, Gabriel César Zaccaria de. **Crimes na Internet**. 2º ed., atualizada e ampliada. São Paulo: Editora Juarez de Oliveira, 2009 p. 2.

[21] http://pt.wikipedia.org/wiki/E-mail. Acessado em 15 Set. 2012.

> "O FTP (File Transfer Protocol - Protocolo de transferência de arquivos) oferece um meio de transferência e compartilhamento de arquivos remotos. Entre os seus serviços, o mais comum é o FTP anônimo, pois permite o download de arquivos contidos em diretórios sem a necessidade de autenticação. Entretanto, o acesso anônimo é restrito a diretórios públicos que foram especificados pelo administrador da rede. O protocolo FTP disponibiliza interatividade entre cliente e servidor, de forma que o cliente possa acessar informações adicionais no servidor, não só ao próprio arquivo em questão. Como exemplo de facilidades podemos citar a lista de arquivos, onde o cliente lista os arquivos existentes no diretório, ou opções do tipo Help, onde o cliente tem acesso a lista de comandos. Essa interatividade e proveniente do padrão NVT (Network Virtual Terminal) usado pelo protocolo TELNET. Contudo, o FTP não permite a negociação de opções, utilizando apenas as funções básicas do NVT, ou seja, seu padrão default[22]".

Após a ARPAnet desenvolver grande parte desta tecnologia, e levando em conta que a guerra fria já estava em decadência, os Estados Unidos da América decidiram expor em público o que havia sido desenvolvido pela agência, almejando proteger o futuro e o incremento tecnológico de seu país.

O protocolo utilizado pela ARPAnet encontrava-se obsoleto, foi então que ela se juntou aos cientistas Vinton Cerf e Bob Kahn e propuseram a criação de um novo protocolo, nomeado TCP/IP – Protocolo de Controle de Transmissão/ Internet Protocolo. O TCP/IP usava um sistema baseado em arquitetura de comunicações por camadas, cada uma com uma finalidade distinta, executando tarefas diversas. O TCP era encarregado de partilhar as mensagens em pacotes por um lado e reconstruí-las por outro, garantindo desta forma a segurança da informação contida. O IP era responsável por examinar o melhor caminho para que a mensagem percorresse até o seu destinatário final, enviando os pacotes.

Ao divulgar esta tecnologia a sociedade, a ARPAnet passou a ser utilizada para todos os tipos de comunicação, bem como por todos os tipos de usuários, não havendo mais distinção entre uso militar e uso civil. Com isso, nasceu a necessidade em subdividir suas redes, ficando a ARPAnet exclusiva para uso acadêmica e a MILnet, criada posteriormente, para uso exclusivo das forças militares.

Acerca desta Divisão, Afirma Maria do Socorro Costa do Vale:

> "A ARPANET ficou dividida em duas redes: ARPANET e MILNET que ficaram integrados ao *Defense Data Network*, criado no ano anterior. A MILNET era uma rede de computadores de instituições militares enquanto a

[22] SANTOS, Luiz Carlos dos. Como funciona o protocolo FTP?. **HTML STAFF.** 26 set. 2006. Disponível em: <http://www.htmlstaff.org/ver.php?id=985>. Acessado em: 11 de Outubro de 2012.

> ARPANET servia para dar suporte aos trabalhos de pesquisas avançadas[23]".

2.2INTERNET NO BRASIL

O processo de introdução da internet no Brasil se deu de forma lenta e progressiva; valendo-se de uma série de ações dos governos federais vigentes para dar inicio ao desenvolvimento das telecomunicações no Brasil, tendo em vista a necessidade de um sistema nacional de telecomunicações que buscasse facilitar a difusão de informações em âmbito nacional, alcançando assim também a tão almejada integração nacional.

A indigência de uma rede de telecomunicações de largo alcance foi iniciado pouco antes de o primeiro governo militar tomar o poder, contudo este compreendeu a importância de uma tecnologia que facilitasse a comunicação e contribuísse para a proteção do país. Como bem resume Dias,

> "No início do governo de Jânio Quadros (janeiro a agosto de 1961), foi criado o Conselho Nacional de Telecomunicações (CONTEL) e, em seguida, no governo de João Goulart (setembro de 1961 a março de 1964), foi aprovado e regulamentado o Código Brasileiro de Telecomunicações (CBT), inspirado nos estudos conduzidos pelo Estado Maior das Forças Armadas (EMFA)[24]".

O setor de telecomunicações até esta época era dominado por empresas privadas, e seu desempenho era de baixíssima qualidade, sobretudo beneficiava parte da população deixando regiões pobres ou distantes desprovidas dessa tecnologia. O governo Militar de 1964, com sua agenda politica voltada para a integração nacional, promoveu a implantação do CBT, regulamentado pela Lei de nº 4.117[25], a estruturação do CONTEL, que futuramente em 1967, fora substituído pelo Ministério das Comunicações (Minicom) e a construção da Empresa Brasileira de

---

[23] COSTA DO VALE, Maria do Socorro. COSTA, Denise Coutinho. ALVES JR, Nilton. **Internet**: Histórico, evolução e gestão. p. 30. Disponível em: <http://registro.br/info/dpn.html> Acessado em: 20 Set. 2012.

[24] DIAS, Lia Ribeiro, CORNILS, Patrícia, **Alencastro:** o general das telecomunicações**.** São Paulo, Plano Editorial. 2004.

[25] BRASIL. **Lei nº 4.117**, de 27 de Agosto de 1962. Institui o Código Brasileiro de Telecomunicações. Diário Oficial [da] Republica Federativa do Brasil. Brasília, DF, 28 Ago. 1962. Disponível em: <http://www.in.gov.br/mp_leis/leis_texto.asp?Id=LEI%209887>. Acesso em: 22 de Setembro de 2012.

Telecomunicações (EMBRATEL), constituída em 1965, criada para implantar a rede nacional, que passou a adquirir o controle das concessionárias privadas e assumir os serviços nacionais e internacionais prestados pelas multinacionais.

A constituição do Ministério das Comunicações contribuiu não tão somente para alavancar o status do setor de telecomunicações, como estabeleceu normas operacionais do Sistema Nacional de Telecomunicações (SNT), segundo as quais as telecomunicações ficariam sob o monopólio das empresas estatais, enquanto a radiodifusão ficaria a cargo da iniciativa privada (TELEBRASIL, 2004, p. 14)[26].

Já no inicio da década de setenta, com o aumento do uso de equipamentos eletrônicos no país, o Minicom passou a ter outra preocupação, à da transmissão eletrônica de dados. Diante das limitações dessas redes clássicas, os órgãos responsáveis pela administração dos setores de telecomunicações de vários países começaram a providenciar a instalação de novas redes destinadas à transmissão de dados[27].

Foi criada em 1979, a Secretaria Especial de Informática (SEI), subordinada ao Conselho de Segurança Nacional do governo do Presidente (General) João Figueiredo. Após assumir o setor de informática no Brasil, a SEI também passou a cuidar das diretrizes relacionadas com o fluxo internacional de dados, onde lhe cabia exclusivamente à decisão sobre a autorização do tipo de comunicações de dados e informações seria transferidas do Brasil com o exterior.

Contudo, essa subordinação dificultava o desenvolvimento do país, tendo em vista, que os interesses eram difusos. Por um lado, o Estado buscava filtrar o tipo de informações que poderiam ser trocadas e por outro, as empresas viam essa tecnologia como um facilitador em seus negócios.

No Brasil, os principais discursos de suporte à implantação das redes de comunicação de dados relacionavam-se à competitividade da indústria nacional e às finalidades de ordem estratégico-militar[28].

---

[26] TELEBRASIL ASSOCIAÇÃO BRASILEIRA DE TELECOMUNICAÇÕES, 2004, **Telebrasil:** 30 anos de sucessos e realizações. Rio de Janeiro, Graphbox.

[27] BENAKOUCHE, Tâmara, 1997, "Redes técnicas - redes sociais: a pré-história da Internet no Brasil", **Revista USP**, n. 35, pp. 125-133. Dossiê Informática/Internet.

[28] CARVALHO, MARCELO SÁVIO REVOREDO MENEZES DE. A trajetória da Internet no Brasil: do surgimento das redes de computadores à instituição dos mecanismos de governança [Rio de Janeiro] 2006, XX, 239 p. 29,7 cm (COPPE/UFRJ, M.Sc., Engenharia de Sistemas e Computação, 2006). Dissertação – Universidade Federal do Rio de Janeiro.

Do ponto de vista real, Benakouche, traduz perfeitamente esse sentimento quando diz que,

> "A indústria nacional alcançaria um maior desenvolvimento tecnológico se estivesse em sintonia com o que estava acontecendo nos países centrais, e as questões geopolíticas decorrentes das redes de comunicações eram estratégicas para a autonomia e a segurança nacionais[29]".

Nesse contexto, muitos países sedes de grandes agências de noticiais internacionais defendiam o livre fluxo de informações, o que os países como o Brasil rejeitavam, argumentando que questões de cunho de ordem política, econômica, tecnológica e cultural revela a necessidade de um controle, haja vista o tipo de informações que sai e entra nas fronteiras nacionais.

Diante do imperativo a uma liberdade de informação e comunicação, o Brasil com outros países e a UNESCO criaram um órgão o *Intergovernamental Bureau for Informatics* (IBI), com o objetivo de conscientizar a sociedade organizada da importância da livre informação e comunicação, sugerindo o inicio de uma movimento denominado NOMIC.

Em seu primeiro congresso, realizado na Espanha, o IBI sugeriu uma Nova Ordem Mundial da Informação e da Comunicação (NOMIC), às vezes também chamada de Nova Ordem Internacional da Informação (NOII) (AGUIAR, 2001. p. 53).

Entre as propostas desse movimento por uma NOMIC estavam dar prioridade ao desenvolvimento da capacidade de auto-suficiência comunicacional; encorajar a produção e distribuição de produtos culturais em nível nacional; estabelecer imprensa comunitária em áreas rurais; estabelecer políticas nacionais para fortalecer a identidade cultural e a criatividade; dar preferência a formas não comerciais de comunicação e informação; contribuir para os direitos humanos via meios de comunicação de massas; experimentar novas formas de envolvimento público na gestão dos meios de comunicação de massas; encorajar todas as formas de cooperação entre profissionais dos meios de comunicação e suas associações para aumentar o conhecimento entre nações e culturas; melhorar a distribuição internacional do espectro de radiofreqüência e, finalmente, estabelecer regulamentação sobre o fluxo de dados transfronteiras[30].

---

[29] BENAKOUCHE, op. cit.

[30] UNESCO, 1987, **Communication and society:** a documentary history of a new world information and communication order seen as an evolving and continuous process, 1975-1986. Paris, UNESCO.

Em um encontro entre países, a posição brasileira foi citada pelo tenente-coronel Joubert de Oliveira Brízida, secretário-executivo da SEI, durante a Primeira Conferência Mundial sobre Fluxo de Dados, realizada em junho de 1980, em Roma (Itália), defendendo o controle governamental sobre os sistemas de informação de cada país e a criação de legislação específica regulamentando os fluxos internacionais de dados[31].

> "A informática não é neutra, isto é, traz em si a cultura de quem a originou. Portanto é fundamental que cada país exerça crítica sobre as informações que lhe atravessam as fronteiras [...]. O país que não se preocupa com o controle das informações estratégicas que utiliza corre o risco de se tornar intoleravelmente dependente, através das telecomunicações, dos interesses de grupos políticos e econômicos fora de suas fronteiras[32]".

Em 1984, a política para o setor de informática deixou de ser de competência exclusiva do poder executivo, trazendo para o debate as entidades acadêmicas que viam nessa tecnologia um importante passo para a capacitação de seus membros.

Precedido de um intenso debate público, o Congresso Nacional aprovou, quase unanimemente, a chamada "Lei de Informática – Lei nº 7.232 de 29 de Outubro de 1984", que referendou os princípios básicos de capacitação tecnológica e reserva de mercado e democratizou o processo decisório através da criação do Conselho Nacional de Informática e Automação (CONIN)[33].

O processo de implantação dessa nova tecnologia no Brasil veio com uma série de desafios, desafios estes que marcou os anos oitenta como "a década das redes", visto que os benefícios advindos seriam muito maiores do que obstáculos postos a prova.

> "O átomo é o passado. O símbolo da ciência para o próximo século é a Rede dinâmica. [...] Enquanto o átomo representa uma clara simplicidade, a Rede canaliza o poder confuso da complexidade. [...] A única organização capaz de crescimento sem preconceitos e aprendizagem sem guias é a rede. Todas as outras topologias são restritivas. Um enxame de redes com acessos múltiplos e, portanto, sempre abertas de todos os lados. Na verdade, a rede é a organização menos estruturada da qual se pode dizer que não tem nenhuma estrutura. [...] De fato, uma pluralidade de

[31] CARVALHO, Marcelo Sávio Revoredo Menezes de. A trajetória da Internet no Brasil: do surgimento das redes de computadores à instituição dos mecanismos de governança [Rio de Janeiro] 2006, XX, 239 p. 29,7 cm (COPPE/UFRJ, M.Sc., Engenharia de Sistemas e Computação, 2006). Dissertação – Universidade Federal do Rio de Janeiro.

[32] DANTAS, Vera, 1988, **Guerrilha Tecnológica:** a verdadeira história da política nacional de informática. Rio de Janeiro, LTC.

[33] TIGRE, Paulo Bastos, 1987, **Indústria Brasileira de Computadores:** perspectivas até os anos 90. Rio de Janeiro, Campus.

> componentes realmente divergentes só pode manter-se coerente em uma rede. Nenhum outro esquema - cadeia, pirâmide, árvore, círculo, eixo - consegue conter uma verdadeira diversidade funcionando como um todo. Devemos esperar ver redes sempre que vemos mudanças irregulares constantes[34]".

A partir desse momento começou a disseminação do uso de computadores nas organizações, empresas, mas, sobretudo em residências, com a finalidade de comunicação interpessoal através de seus computadores pessoais, com a utilização do modem e da rede de telefonia convencional, porém esse serviço ainda era precário, porém os esforços dispostos para sua aprimoração foi dispendioso em novos projetos e pesquisas para que se chegassem ao que hoje utilizamos.

Foi a partir de 1994, com o lançamento da *world wide web* que as empresas que ofereciam seus serviços de rede isolados passaram a atuarem como provedores de acesso a Internet, onde viabilizavam todo o conteúdo da Internet para seus assinantes. Nesse momento surgiram as grandes lojas de comércio eletrônico como *Amazon*, *eBay*, entre outros diretórios de buscas, também dando espaço para organizações públicas e privadas, em todo o mundo, passaram a buscar seu espaço nesse universo da Internet.

A Internet comercial só chegou ao Brasil em 1996, totalmente obsoleto com uma infraestrutura insuficiente para atender às demandas de seus provedores de acesso e, principalmente dos seus usuários, essa cresceu rapidamente, não somente em números de usuários, mas em transações por meio do comércio eletrônico. Em decorrência surgiram diversas lojas virtuais, portais de conteúdo e máquinas de busca, como *Booknet*, Universo *On Line* (UOL), Brasil *On Line* (BOL), Cadê?, entre outros.

2.3 OS CRIMES PRATICADOS NA INTERNET E SUAS CARACTERÍSTICAS

Devido a seu alcance infindável, a internet se posiciona atualmente como um dos maiores meios de comunicação de todo o mundo, adquirindo milhares de novos usuários a cada dia, que buscam usufruir de seus benefícios, seja para

[34] KELLY, Kevin. **Out of Control:** The New Biology of Machines, Social Systems and the Economic World. Basic Book. Reading, MA, Perseus Press. 1995.

relacionamentos negociais, obtenção de bens e serviços, ou simplesmente para o lazer.

Entretanto, com seu avanço crescente e quase que desordenado, inúmeros criminosos reais passaram a utilizar a internet para cometer crimes virtuais, como o estelionato, a calunia, o furto e o racismo, acreditando que seria mais difícil a identificação de autoria dos delitos, bem como a reparação do dano, haja vista o infrator transgredir a lei do sofá de sua casa ou de qualquer lugar que possua um computador com acesso a grande rede.

Neste sentido, posiciona-se Fabrízio Rosa:

> "Com a expansão do uso de computadores e com a difusão da internet, tem-se notado, ultimamente, que o homem está se utilizando dessas facilidades para cometer atos ilícitos, potencializando, cada vez mais, esses abusos cometidos na rede. Como todos os recursos de disponibilidade do ser humano, a informática e a telecomunicação não são utilizadas apenas para agregar valor. O abuso (desvalor), cometido por via, ou com assistência dos meios eletrônicos não tem fronteiras. De um terminal eletrônico instalado num país se poderá manipular dados, cujos resultados fraudulentos poderão ser produzidos noutro terminal, situado em país diverso[35]".

Os crimes praticados na internet assumem posição de destaque dentro do cenário penal brasileiro, embora não haja até o presente momento nenhuma codificação especifica sobre o tema, tornando sua punição dificultosa. Novos criminosos são atraídos diariamente a utilizar este novo *modus operandi* para cometer seus delitos, enganando suas vitimas com maior facilidade.

Infelizmente, os crimes avançam com mais velocidade que as leis existentes, e isto se torna um fator determinante para a impunidade, haja vista os tipos penais descritos no Código Penal Brasileiro de 1940 não terem previsto em capítulo específico algo relativo a crimes cibernéticos, deixando a cargo da doutrina e jurisprudência se manifestar quando ocorrem no caso concreto.

O estado encontra-se absolutamente vulnerável perante os novos criminosos virtuais, muito embora tem-se percebido que algumas medidas estão sendo adotadas para coibir esta prática, como a criação de delegacias especializadas no assunto, o treinamento e aperfeiçoamento dos policiais e outros profissionais que lidam com esta prática cotidianamente e o entendimento dos juízes no âmbito dos tribunais, visando unificar alguns entendimentos sobre o mesmo tema.

---

[35] ROSA, Fabrízio. **Crimes de Informática.** 2º ed. Campinas: Bookseller, 2005.

Nesta linha de raciocínio, nos esclarece o ilustre promotor de justiça Gabriel César Zaccaria:

> "Como promotor de justiça criminal, sei que infelizmente, os criminosos são mais rápidos que os legisladores. Isso acontece em todo o mundo e o Brasil não é exceção. Ainda mais, em se tratando de internet, que passou a ser largamente utilizada em nosso país a pouco tempo e que possui peculiaridades que outros meios de comunicação não tem. A facilidade que a internet oferece para a prática de crimes, deixou os juristas completamente assarapantados. Não possuímos legislação específica a respeito de crimes virtuais em nosso Código Penal de 1940. Evidentemente, no combate aos crimes virtuais, a justiça utiliza o Código Penal, pois a grande maioria das infrações penais cometidas através da internet, pode ser capitulada nas condutas criminosas previstas no Código Penal. Todavia, o ideal seria a existência de lei especial, onde estivessem capituladas as condutas especificas, isto é, as condutas criminosas, praticadas através da internet[36]"

Conforme demonstrado acima, a ausência de legislação especifica sobre o tema abre espaço para que, cada vez mais, novos criminosos migrem para esta modalidade recente, sabendo que a pretensão punitiva do estado encontra-se deficiente no que tange ao meio cibernético, garantindo aos infratores na pior das hipóteses, penas absolutamente incompatíveis com a conduta praticada, fazendo com que os criminosos tenham a certeza de que o crime realmente é o melhor caminho para atingir suas finalidades, valendo-se da forma branda de punir do estado.

No tocante ao sujeito ativo dos crimes de informática, vale dizer que qualquer pessoa pode figurar como autor neste polo, não necessitando obrigatoriamente de ser uma pessoa que tenha pleno domínio do computador e do meio virtual em que navega, bastando apenas o cibercriminoso dispor da vontade final em praticar o delito, embora na maioria das vezes seja executado por pessoas com vasto entendimento na área.

Neste aspecto, Fabrízio Rosa explicita que:

> "É um engano pensar que os "crimes de informática" são cometidos apenas por especialistas, pois, com a evolução dos meios de comunicação, o aumento de equipamentos, o crescimento da tecnologia e, principalmente, da acessibilidade e dos sistemas disponíveis, qualquer pessoa pode ser um criminoso de informática, o que requer apenas conhecimentos rudimentares para tanto; uma pessoa com o mínimo de conhecimento é potencialmente capaz de cometer crimes de informática. É claro que, em sua grande

[36] INELLAS, Gabriel César Zaccaria de. **Crimes na Internet**. 2º ed., atualizada e ampliada. São Paulo: Editora Juarez de Oliveira, 2009. p.100.

> maioria, o delinquente de informática é um operador de computadores e sistemas, mas, como dito, não se pode generalizar[37]".

Após o exposto, pode-se concluir que os crimes de informática possuem como pré-requisito a presença de apenas três fatores fundamentais para que sejam executados: (1)- agente capaz de cometer o ilícito (2)- um computador em pleno funcionamento e, (3)- acesso a rede mundial de computadores. Preenchido estes requisitos, qualquer um pode incidir sobre esta modalidade criminosa.

No que diz respeito ao agente delitivo, um tipo em específico merecesse atenção especial, que é o *hacker*. O *hacker* é aquela pessoa dotada de conhecimentos aprofundados de sistemas operacionais e tipos de linguagens programacionais, ele conhece com perfeição as falhas de segurança existentes nos programas e está sempre em busca de novas outras falhas. O *hacker* invade os sistemas pelo simples prazer de provar para si mesmo que é capaz de fazê-lo, sem alterar nada[38].

Quanto ao sujeito passivo dos crimes virtuais, tem-se a pessoa ou a entidade detentora do bem jurídico protegido pelo legislador e sobre quem irá recair a conduta ilícita do sujeito ativo, podendo ser pessoa física ou jurídica, de gênio público ou privado. Fabrízio Rosa define o sujeito passivo da relação criminosa da seguinte forma: "o sujeito passivo dos crimes de informática pode ser qualquer pessoa, física ou jurídica, de natureza pública ou privada, pouco importando se é capaz ou não de entender o que possa estar acontecendo[39]".

É importante frisar, contudo, que a grande maioria destes crimes praticados em ambiente virtual não chega ao conhecimento de autoridades para que seja apurado corretamente, devido ao medo que as instituições bancárias, por exemplo, sentem de haver desprestígio e perca de credibilidade perante seus clientes, causando má impressão de que a instituição possui sistemas ineficazes de segurança. Muitas vezes o silêncio por parte da vítima acaba por "incentivar" os criminosos a continuar laborando ilicitamente todos os dias, daí a importância em se denunciar e coibir esta prática.

Quanto aos métodos utilizados para a invasão nos computadores e sistemas operacionais, alguns merecem destaque e serão analisados em sequência. O

---

[37] ROSA, Fabrízio. **Crimes de Informática.** 2º ed. Campinas: Bookseller, 2005, p 61.
[38] Ibidem. **Crimes de Informática.** 2º ed. Campinas: Bookseller, 2005, P. 61.
[39] Ibidem. **Crimes de Informática.** 2º ed. Campinas: Bookseller, 2005, P. 63.

primeiro deles é o denominado de “chave mestra”, que se trata basicamente do uso indevido e não autorizado de programas criados para modificar, copiar, utilizar ou inserir o uso de algumas informações arquivadas em bancos de dados informáticos. Esta nomenclatura deriva de um *software* particular chamado superzap, que autoriza a abertura de qualquer espécie de arquivo ou dados de um computador, ainda que o mesmo encontre-se paralisado e protegido por sistemas bloqueadores de ataques, como os antivírus.

O segundo método, e não menos importante, é o *sniffer,* um programa incumbido de captar e interceptar a informação que está trafegando pela rede mundial de computadores (internet). Pode-se citar como exemplo clássico, o caso de um usuário que faça *login* para acessar sua caixa de *e-mails*, digitando seu nome de usuário e senha. Esses dados inseridos anteriormente irão viajar pela rede para fins de confirmação, e é nesta transmissão de dados que o *sniffer* atua, agarrando estas informações e guardando-as para utilizar posteriormente em alguma fraude.

Em terceiro lugar, e talvez o mais utilizado entre os agentes maliciosos, está o cavalo de tróia (*trojan horse*), que é um programa que parece ter uma função útil, que pode ser um jogo, mas guarda em seu escopo recursos ocultos e severamente maliciosos. Fabrízio Rosa descreve o cavalo de tróia da seguinte maneira:

> “O cavalo de troia às vezes dribla mecanismos de segurança ao tapear os usuários e fazê-los autorizar o acesso aos computadores. Com este golpe, permite a entrada no sistema. Um dos objetivos é a sabotagem. Pode objetivar também a alteração de dados, cópia de arquivos com a finalidade de obter ganhos monetários. Esse é o golpe típico para quem quer controle e poder, pois permite, através do cavalo de Tróia, o acesso a diversos sistemas que estarão passíveis de manipulação da forma que mais convier[40]”.

Dando sequência, eis que surge o vírus, que nada mais é do que um fragmento de programa de computador que é capaz de mudar totalmente a estrutura do *software* do sistema operacional, destruindo ou inutilizando dados e outras informações com ou sem o conhecimento do usuário. O vírus recebeu este nome devido a sua forma de propagação, que acaba por lembrar os vírus reais, que acometem os seres humanos, infectando outras pessoas se não for tomada as medidas cabíveis.

---

[40] ROSA, Fabrízio. **Crimes de Informática.** 2º ed. Campinas: Bookseller, 2005, P. 69.

Outro método muito utilizado pelos *hackers* e outros seres que insistem em transgredir os limites impostos é o *spyware*, um programa que tem por intuito monitorar os hábitos recorrentes no computador, como as páginas preferidas da internet e seus padrões de navegação, onde a informação é transmitida para terceiros, muitas vezes sem o consentimento e autorização do usuário. Sua forma mais comum de apresentação é por intermédio de anúncios publicitários, que ao serem clicados, automaticamente se instala na máquina e funciona como um ladrão virtual, furtando as informações relativas ao hábito do usuário.

Dentro do gênero *spyware*, existe outro programa malicioso batizado de *key logger*, que registra todos os toques dados no teclado e em outras atividades do sistema. O *key logger* é responsável, por exemplo, por coletar os números do cartão de crédito, senhas e outros dados e transmiti-los a terceiros.

Por fim, tem-se o cookie, uma espécie de arquivo utilizada por alguns sites que põem no computador do usuário para autorizar a personalização dos conteúdos contidos na web. Em sua grande maioria, os cookies são inofensivos, mais alguns podem ter funções diversas, suprimindo informações que deviam se sigilosas.

Ressalte-se que diferentes tipos de técnicas e golpes de invasão surgem a cada dia, forçando os usuários deste universo virtual a serem mais familiarizados e atentos as transações e informações que são compartilhadas neste meio, tendo em vista minimizar os possíveis danos que possam ser causados.

CAPÍTULO III

3. O CRIME DE ESTELIONATO PRATICADO NA INTERNET

BREVES CONSIDERAÇÕES

A internet e seus mecanismos de pesquisa têm avançado de maneira incisiva desde sua criação, motivo este que acaba por acarretar uma série problemas e danos a seus usuários. A internet é utilizada como um hábil meio de acesso a informações e transferências de dados, e vem se desenvolvendo e realizando profundas modificações nas condutas e comportamento humano.

Neste sentido, a velocidade e agilidade dos avanços tecnológicos bem como a facilidade de acesso aos computadores da rede têm ocasionado diversos tipos de relações sociais e de consumo através da rede mundial de computadores.

Com o nascimento da internet, uma nova forma jamais vista de comunicação entre as pessoas foi se aflorando, sendo também uma importante ferramenta utilizada para compartilhar e pesquisar informações dos mais variados assuntos, dando inicio a uma nova era da sociedade de informação.

Sobre este tema, Léa Elisa elucida que,

> "Hodiernamente, então, temos vivenciado uma intensa revolução tecnológica promovida, principalmente, graças a este comentado "mundo de pontas"[41]. Mister enfatizar que esta rede mundial de computadores tem sua matriz relacionada com fins bélicos, conforme dito anteriormente, propostos pelos Estados Unidos, nos anos 60. No Brasil, entretanto, este mecanismo de troca de bits chegou, com fins comerciais, na década de 90. Desta forma, relações pessoais, comerciais, de consumo e de trabalho, entre outras, passam pela rede mundial de computadores, provocando uma revolução jamais vivida pelo mundo até hoje[42]".

Embora este eficiente meio de comunicação tenha sido criado com o intuito de facilitar e agilizar a vida das pessoas, por muitas vezes é utilizado de forma

---

[41]SEARLS, Doc; WEINBERGER, David. apud MENEZES, André Gonçalves de. AMORIM, Eduardo Antônio Andrade et al. O Estelionato Eletrônico: Uma breve reflexão sobre o Delito Informático. Disponível em: <http://www.brockerhoff.net/bb/viewtopic.php?t=10>. Acessado em: 10. Outubro. 2012.

[42] CALIL, Léa Elisa Silingowschi. **Revolução Digital**. Disponível em: <http://www.mundodosfilosofos.com.br/lea20.htm>. Acessado em: 16. Março. 2012.

ilegítima, acarretando danos para seus usuários. É devida essa intensificação no relacionamento humano pela internet, dando lugar a expansão do comércio eletrônico e o uso indiscriminado e quase mundial dessa tecnologia favorecendo em todos os aspectos novas relações, trazendo assim novas condutas ilícitas.

Está cada vez mais frequente a prática de atividades eletrônicas antijurídicas no meio virtual, onde pessoas mal intencionadas usam de seu conhecimento para obter vantagens ilícitas, dando como exemplo: utilização não autorizada de sistemas informáticos, introdução, alteração ou pagamento de partes inteiras de programas, inserção de funções falsas em software, entre outros.

O Direito como ciência normativa não poderia permanecer inerte a tantas modificações sociais e, neste sentido, as condutas fraudulentas merecem, inclusive, tipificações penais, já que essas ilicitudes lesam bens de suma importância para a sociedade. Assim sendo, muitas reflexões tem sido criada no âmbito do direito penal, com a finalidade de propiciar uma atualização nos tipos penais descritos em nosso ordenamento jurídico penal.

Nesse raciocínio, ressalte-se a dificuldade que o Direito possui em adaptar dentro desse contexto de constante modificação. O Direito em si não consegue acompanhar o frenético avanço proporcionado pelas novas tecnologias, principalmente a internet, um ambiente livre e totalmente sem fronteiras que se desenvolve essa nova modalidade de crimes, por agentes que se aproveitam da possibilidade de anonimato e da ausência de regras.

Segundo Ivette Senise Ferreira,

> "A preocupação com essa questão surge nas ultimas décadas com a popularização dessa nova tecnologia, manifestando-se também através da promulgação de leis relativas à informática e na competência privativa da União para legislar sobre a matéria (CF, art. 22, inciso IV) [43]".

A criminalidade faz parte do homem. Para Émile Durkheim[44], o delito não ocorre somente na maioria das sociedades de uma ou outra espécie, mais sim em todas as sociedades constituídas pelo ser humano. Assim, para o sociólogo francês, o delito não só é um fenômeno social normal, como também cumpre outra função

[43] FERREIRA, Ivette Senise. apud LIMA, Paulo Marco Ferreira. **Crimes de Computador e Segurança Computacional**. Campinas, SP. Ed. Millennium. 2005.

[44] EMILE. Durkheim, Lãs reglas Del método sociológico, Espanha, Morata, 1978, p. 83. (apud) BITENCOURT, Cezar Roberto. **Tratado de Direito Penal** – Parte Geral, 9ª ed., v. I, São Paulo: Saraiva, 2004.

importante: manter aberto o canal de transformações de que a sociedade precisa. De acordo com essa lição, pode-se deduzir que as relações humanas são contaminadas pela violência, portanto, é necessário um conjunto de normas que as regulem, surge, então, o direito penal com natureza de meio de controle social, procurando resolver conflitos e harmonizar a sociedade. Vale indagar a importância dos doutrinadores na evolução da dogmática penal, em virtude dessa nova realidade mundial para que o ciberespaço, não se torne em um universo onde as regras não tenham alcance.

> "Não é exagero afirmar que se aproxima também uma nova revolução jurídica, trazendo, como consequência, a problemática relativa à criação ou readaptação do ordenamento penal para a proteção desses novos bens jurídicos informáticos e de outros de igual ou maior relevância, que venham a ser atingidos criminosamente por meio de computadores e por intermédio da *world wide web*[45]".

O Direito Penal é regido por uma série de princípios, dentre os quais se destaca o Principio da Reserva Legal, constante no artigo primeiro do Código Penal Brasileiro: "Não há crime sem lei anterior que o defina. Não a pena sem prévia cominação legal[46]". Em decorrência desse principio, apenas serão puníveis apenas as condutas que estiverem expressa e precisamente previstas em lei, proibido o uso de analogias para abarcar situações originalmente não previstas ou semelhantes. Ou seja, a lei penal é interpretada de forma restritiva, fazendo com que a definição dos crimes e contravenções sejam claras e precisas, afastando qualquer duvida ou incerteza. No caso do estelionato ocorrido pelo meio virtual, inexiste previsão expressa no Código Penal, portanto, para que a punição seja efetivada temos de nos remeter a outras espécies de diplomas legais, bem como posicionamentos jurisprudenciais sobre o referido tema.

---

[45] LIMA, Paulo Marco Ferreira. Crimes de computador e segurança computacional. p. 3-4. Campinas/SP: Milenium, 2006.

[46] BRASIL. **Código Penal Brasileiro**. Organização dos textos, notas remissivas e índices por Juarez de Oliveira. 46. ed. São Paulo: Saraiva, 2000.

3.1O ESTELIONATO VIRTUAL

A figura do estelionato executado em ambiente virtual ainda é algo recente dentro do estado e dos tribunais brasileiros, no entanto, merece atenção especial, data vênia a popularização e modernização da internet, atingindo e adquirindo milhares de novos usuários a cada dia.

Em linhas gerais, o crime de estelionato é configurado quando alguém obtém, para si ou para outrem, vantagem ilícita em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento. O artigo 171 do Código Penal[47] versa que:

> "Art. 171. Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artificio, ardil, ou qualquer outro meio fraudulento: pena – Reclusão, de 1 (um) a 5 (cinco) anos, e multa".

Ainda que o Código Penal Brasileiro faça menção ao estelionato em seu texto, vale ressaltar que a conduta descrita diz respeito apenas ao delito praticado de forma direta pelo infrator, isto é, obtendo vantagem ilícita em prejuízo alheio em pleno contato com a vítima, não sendo necessário o intermédio do computador e da internet para que reste consumada sua atividade criminosa.

O impasse surge quando da tipificação do estelionato virtual na legislação penal, que se mostra inerte quanto a isso. Note que a própria Constituição Federal traz no inciso 39 do artigo 5º o princípio da legalidade, que também encontra-se redigido no primeiro artigo do CPB, in verbis:

> "Art. 5º. Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
>
> (...)
>
> XXXIX - não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal."

Por este princípio exposto acima, todo e qualquer indivíduo que cometa crime deve ser punido com base neste inciso norteador, portanto, para que o processo

---

[47] BRASIL. **Código Penal Brasileiro**. Organização dos textos, notas remissivas e índices por Juarez de Oliveira. 46. ed. São Paulo: Saraiva, 2000.

penal tenha seu curso normal e previsto, o fato deve se adequar perfeitamente na legalidade estrita da lei, não podendo ser reprovável sem que cumpra os requisitos de validade. A natureza jurídica deste dispositivo legal acaba por limitar a pretensão punitiva estatal, e por inexistir a tipificação expressa do estelionato virtual em diploma legal, em alguns casos seus adeptos são absolvidos devido a esta “brecha” deixada pelo Código antiquado aos dias atuais, datado no ano de 1940.

Neste sentido, corrobora Cézar Roberto Bitencourt:

> "O principio da legalidade ou da reserva legal constitui efetiva limitação ao poder punitivo estatal. Feuerbach, no inicio do século XIX, consagrou o principio da reserva legal por meio da fórmula latina nullum crimen, nulla poena sine lege. O principio da reserva legal é um imperativo que não admite desvios nem exceções e representa uma conquista da consciência jurídica que obedece a exigências de justiça; somente os regimes totalitários o têm negado[48]”.

Diante do explicitado, conclui-se que para a prática do estelionato virtual e de qualquer outro crime é necessário a presença de três requisitos essenciais de validade que compõem o fato típico, sem os quais seria impossível a imputação de penalidade ao agente.

O primeiro requisito diz respeito à tipificação expressa do crime em lei, ou seja, sua denominação legal e precisa do ato volitivo contributivo do infrator para o resultado finalístico. Se não houver tal tipificação, a materialidade para o delito simplesmente irá desaparecer, o tornando atípico e consequentemente não punível pela legislação jurídica penal brasileira.

A próxima condição fundamental que se encaixa ao delito é a conduta do autor, que pode se dar de forma comissiva ou omissiva, dolosa ou culposa. A conduta comissiva se aduz em uma ação positiva desencadeada pelo transgressor, ocorrendo quando a ação for expressamente proibida por lei, como por exemplo, matar alguém, contrariando o que diz o artigo 121 do CPB.

Já na hipótese de ato omissivo, o indivíduo age negativamente, deixando de praticar algo que lhe era devido por obrigação ou que poderia fazer para amenizar a consequência derradeira, como a inércia de pedido de socorro em ocorrências de acidente automobilístico com vítimas, caracterizando a omissão de socorro.

Observe que o estelionato virtual ou real não admite a modalidade culposa, valendo-se do preceito que o estelionatário sempre irá proceder com a vontade de

[48] BRASIL. **Código Penal Brasileiro**. Organização dos textos, notas remissivas e índices por Juarez de Oliveira. 46. ed. São Paulo: Saraiva, 2000.

induzir ou manter a vítima em erro, criando situações que se furtam com a realidade dos acontecimentos, não advindo à situação negligência, imprudência ou imperícia. Portanto, toda fraude classificada como estelionato será sempre dolosa, onde o autor age com *animus* livre e consciente de praticar a conduta inserida na norma penal incriminadora.

O saudoso doutrinador Rogério Greco divide os crimes omissivos em duas partes: omissivos próprios e omissivos impróprios, lecionando-os da seguinte maneira:

> "Há dois tipos de crimes omissivos, os omissivos próprios e os omissivos impróprios. Os omissivos próprio são aqueles que se satisfazem apenas com a inação do agente, não sendo necessário nenhum resultado naturalístico, como é o caso do artigo 135 do CP, que determinar: "Deixar de prestar assistência, quando possível fazê-lo sem risco pessoal". Ora, não há necessidade da ocorrência de qualquer resultado, como lesão ou morte, para que o agente seja punido, basta que ele se comporte de forma inerte, sem prestar assistência. Já a omissão do artigo 13, § 2, do CP, descreve uma outra forma de crime omissivo, chamado pela doutrina de impróprio, em razão especialmente porque cabe ao omitente o dever de agir, ou seja, o omitente tem o dever de impedir o resultado. Segundo Rogério Grecco, nos omissivos impróprios há necessidade da produção de um resultado naturalístico que modifique visivelmente o mundo exterior, sendo perceptível pelos sentidos[49]".

Por fim, exige-se o resultado que foi ocasionado com a atividade ilícita, que se traduz no dano causado à vítima. Segundo a corrente majoritária, o resultado é o efeito que se dá de forma natural configurando a conduta típica, produzindo o resultado no mundo exterior, diretamente interligado pelo nexo de causalidade.

O professor Rogério Greco explana em que consiste o nexo causal:

> "O nexo causal, ou relação de causalidade, é aquele elo necessário que une a conduta praticada pelo agente ao resultado por ela produzido. Se não houver esse vinculo que liga o resultado à conduta que levada a efeito pelo agente, não se pode falar em relação de causalidade e, assim, tal resultado não poderá ser atribuído ao agente, haja vista não ter sido ele seu causador[50]"

A prática do estelionato em ambiente virtual é concretizada na maioria das vezes por pessoas detentoras de notável conhecimento sobre internet e tecnologia de informação, que embora possam agir de outra maneira, preferem se arriscar no mundo virtual do crime para iludir e prejudicar pessoas reais, obtendo algum tipo de vantagem com esta técnica. Destaque-se que a única diferença existente entre o

[49] GRECO, Rogério. **Curso de Direito Penal**. 11 ed. Rio de Janeiro, Iimpetus, 2009. p. 294.
[50] Ibidem. **Curso de Direito Penal**. 11 ed. Rio de Janeiro, Iimpetus, 2009. p. 294.

estelionato virtual e o estelionato real está no *modus operandi* empregado, onde, este é realizado pela internet, enquanto aquele no mundo físico.

Nesta superfície cibernética, alguns criminosos receberam nomenclaturas próprias e peculiares aos crimes informáticos, e seria evidentemente impossível a compreensão efetiva do assunto sem que houvesse a devida explicação individualizada de cada um deles, feita nos parágrafos posteriores.

Como já dito anteriormente, o *hacker* é aquela pessoa dotada de conhecimentos aprofundados de sistemas operacionais e diversos tipos de linguagens programacionais, conhece com culminância as falhas de segurança existentes nos programas e está sempre em busca de novas outras falhas. A grande maioria das pessoas costuma associar as atitudes do hacker com as invasões e golpes perpetrados por estelionatários virtuais, o que é um erro, considerando-se que ele apenas busca descobrir as lacunas contidas em programas e sistemas para mostrar a si mesmo que é perito em sua área.

Em contrapartida, os usuários com conhecimento avançado neste campo da informática e que cometem crimes e outras ações maldosas, são chamados de *crackers*, que na simplória definição de Fabrízio Rosa, abaixo aduzida, ensina que:

> "*Cracker* é o mesmo que *hacker*. A diferença entre um e outro está em utilizar o seu conhecimento para o mal. Destruir e roubar são suas palavras de ordem. Assim, o *cracker* usa os seus conhecimentos para ganhar algo, rouba informações sigilosas para fins próprios e destrói sistemas para exibir[51]".

Conforme demonstrado, o *cracker* utiliza o vasto conhecimento que possui para praticar crimes ou danificar sistemas, e no caso do estelionato, ele é o protagonista principal, haja vista a grande maioria dos crimes serem praticados por estes usuários maliciosos. No entanto, muitos usuários comuns também cometem crimes, haja vista a facilidade que a internet proporciona para isto.

Indo adiante, surge a pessoa do *preaker*, que ao contrário dos outros dois usuários maliciosos supracitados, não emprega o computador e a internet como ferramentas para atingir seu ataque desonesto, mas sim, os telefones. O *preaker* é conhecedor argucioso em redes de telefonia, seja ela móvel ou fixa. Sua cartada principal se revela na instalação de escutas telefônicas ilegais com fins de obter informações que são, ou deveriam ser, sigilosas.

---

[51] ROSA, Fabrízio. **Crimes de Informática.** 2º ed. Campinas: Bookseller, 2005, P. 61.

O mestre em direito penal Fabrízio Rosa classifica o *preaker* da seguinte forma:

> "O *preaker* é especializado em telefonia, atua na obtenção de escutas telefônicas gratuitas e instalação de escutas, facilitando o ataque a sistemas a partir de acesso exterior, tornando-se invisíveis ao rastreamento ou colocando a responsabilidade em terceiros[52]".

Pode-se asseverar com segurança que o *preaker* realiza chamadas sem o devido pagamento, é capaz de transferir faturas telefônicas para outros endereços e altera ou modifica telefones públicos para obter a possibilidade de fazer chamadas ilimitadas.

Perseverando na matéria, tem-se o personagem pouco conhecido do *loser*, que em vias gerais é um operador de internet novo e sem muita experiência técnica, entretanto, é atraído intimamente pelo mundo virtual e quer adquirir cada vez mais novos conhecimentos. É correto dizer que o *loser* é um *hacker* em potencial, pois seu maior desejo é um dia se tornar um, e para tanto, não mede esforços em estudar e perguntar para outras pessoas como proceder nas mais diversas situações.

O perito judicial na área de informática Pedro Augusto Zaniolo[53] classifica o *loser* da seguinte maneira*:*

> "L*oser* é a união *loser (*perdedor) *e user (*usuário) e denota aquele que não quer aprender nada útil, objetivando apenas saber o mínimo necessário para operar o computador e terminar suas tarefas o mais rápido possível."

O *wannabe* é o usuário de computador comum, entretanto aprendeu a manusear diversos programas produzidos e disponibilizados por hackers na internet e os usa para facilitar suas tarefas privadas. O *wannabe,* embora não desenvolva nenhum tipo de sistema ou programa, também é considerado um agente malicioso, afinal, acaba por incentivar e estimular a ação dos *hackers.*

Finalizando a demonstração de alguns tipos de usuários mal-intencionados na internet, tem-se o *guru,* que é aquele usufruinte *expert* em informática e navegação na rede mundial de computadores. É a pessoa que possui conhecimentos superiores em tecnologia, sendo chamado muitas vezes de "mestre" ou "pai" dos *hackers*.

---

[52] ROSA, Fabrízio. **Crimes de Informática.** 2º ed. Campinas: Bookseller, 2005, p. 61.
[53] ZANIOLO, Pedro Augusto. **Crimes Modernos:** O Impacto da Tecnologia no Direito. Curitiba: Juruá, 2007.

Nos casos em que ocorre o estelionato virtual, a conduta finalística do agente se volta na mesma que se encontra descrita no caput do artigo 171, entretanto o criminoso irá valer-se do meio informático para induzir ou manter a vítima em erro, obtendo com isto a vantagem ilícita almejada.

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

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

A ausência de legislação específica sobre o tema acaba por induzir os criminosos a cometer esta nova modalidade de infração, pois eles acreditam que não haverá punição devido à falta de lei sobre a matéria imputada. Muitos são os problemas que rondam o estelionato virtual, dentre os quais destacam-se: a dificuldade de identificação dos autores, a delimitação do local do crime e a competência do juízo.

A grande problemática de se identificar os autores dos fatos é que a rede mundial de computadores interliga em seu seio pessoas do mundo inteiro, e em alguns casos é praticamente impossível se determinar o local em que o ato ilícito foi gerado, sabendo-se que o mesmo criminoso pode-se valer de inúmeros computadores e locais diferentes de acesso para exaurir o fato. Devido ao computador e a internet serem objetos móveis, muitas vezes um único crime cometido por apenas um autor “viaja” por diversos lugares, impossibilitando o trabalho investigatório de identificação de autoria.

Seguindo este pensamento, Sandra Carla Castro Marques Martins leciona que,

> "Destarte, o mundo cibernético tem sido alvo da atuação crescente de criminosos, que encontram na *internet* um meio fácil de cometer crimes, muitas vezes, aproveitando-se do anonimato, o que é vedado pela Constituição Federal, e da falsa impressão de que são impunes, ou pela falta de legislação específica, ou pela dificuldade na investigação criminal em encontrar os autores. É importante ressaltar que os usuários facilitam muito a prática destes ilícitos, tornando-se presas fáceis, pois ao acessar informações bancárias utilizando dados sigilosos, bem como a exposição da imagem, sem os devidos cuidados, acabam por favorecer a criminalidade cibernética[54]".

Outro ponto árduo e dificultoso para a perfeita resolução do crime é a delimitação exata do local onde o mesmo foi cometido. A identificação do local exato do crime é de suma importância para se delimitar a competência jurisdicional e a origem da ocorrência criminosa, que será de grande valia no processo acusatório.

Segundo o Código Penal Brasileiro, em seu artigo 6º, o lugar do crime é aquele local onde ocorreu a ação ou a omissão por artefato do agente, ainda que em parte, bem como onde se produziu ou deveria ser produzido o resultado. Este preceito é de uso obrigatório quando da ocorrência de crimes reais, contudo, no caso de crimes eletrônicos ou virtuais, isto se distorce um pouco. A teoria adotada pelo CPB a respeito da aplicação da lei penal no espaço recebe o nome de teoria mista ou da ubiquidade.

Segundo Rogério Greco,

> "Com a adoção da teoria da ubiquidade resolvem-se os problemas já há muito tempo apontados pela doutrina, como aqueles relacionados a crimes a distancia. Na situação clássica, suponhamos que alguém, reside na Argentina, enviasse uma carta-bomba tendo como destinatário uma vítima que reside no Brasil. A carta-bomba chega a seu destino e, ao abri-la, a vitima detona o seu mecanismo de funcionamento, fazendo-a explodir, causando-lhe a morte. Se adotada no Brasil a teoria da atividade e na Argentina a teoria do resultado, o agente, autor do homicídio ficaria impune. A adoção da teoria da ubiquidade resolve problemas de direito penal internacional. Ela não se destina à definição de competência interna, mas, sim, a determinação da competência da justiça brasileira[55]".

---

[54] MARTINS, Sandra Carla Castro Marques. **Estelionato Eletrônico:** a (des) necessidade de uma tipificação legal. Disponível em: <http://www.ambitojuridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=10133&revista_caderno=3> Acessado em: 30 de Out. de 2012.

[55] GRECO, Rogério. **Curso de Direito Penal**. 11 ed. Rio de Janeiro, Iimpetus, 2009. p. 294.

Esta teoria, embora seja um tanto quanto antiga, ainda se mostra eficiente quanto aos crimes virtuais, em especial destaque ao crime de abordado neste trabalho, entretanto, sem leis específicas ao tema, a teoria cai em desuso, afinal, o processo penal se forma com a junção de várias leis e garantias constitucionais, e a teoria da ubiquidade é apenas uma das fases do procedimento de apuração e punição.

Após definir o lugar em que foi iniciado ou findado o delito virtual, surge outra dúvida pertinente ao assunto: qual o juízo competente para analisar e julgar a ação? sabendo-se que a internet é um meio de comunicação sem fronteiras, e sem proprietários, que alcança milhares de pessoas por todo o mundo, é quase que impossível para qualquer país ou território executar as leis para punir e regular o ciberespaço.

No Brasil não é diferente, todo e qualquer crime virtual que é cometido reveste-se de uma dificuldade imensa de apuração, pois a lei não impõe limites efetivos a este meio, deixando parte da população vulnerável a estes ataques.

O Código Penal Brasileiro, no título I do artigo 5º preceitua que:

> "Art. 5º aplica-se a lei brasileira, sem prejuízo de convenções, tratados e regras de direito internacional, ao crime cometido no território nacional.
>
> §1º para os efeitos penais, consideram-se como extensão do território nacional as embarcações e aeronaves brasileiras, de natureza pública ou a serviço do governo brasileiro onde quer que se encontrem, bem como as aeronaves e embarcações brasileiras, mercantes ou de propriedade privada, que se achem, respectivamente, no espaço aéreo correspondente ou em alto mar.
>
> §2º é também aplicável a lei brasileira aos crimes praticados a bordo de aeronaves ou embarcações estrangeiras de propriedade privada, achando-se aquelas em pouso no território nacional ou em voo no espaço aéreo correspondente, e estas em porto ou mar territorial do Brasil".

E sabido que a lei tem vigência de acordo com os limites territoriais de soberania estatal, é o que diz o princípio da territorialidade. No entanto, em ocasiões de crimes virtuais, a delimitação de competência é algo um pouco mais delicado de se tratar. Com isso, surge o problema da delimitação de espaço e de abrangência de atuação e eficácia da lei penal, afinal, a lei penal só pode e deve ser aplicada no estado que a instituiu, sendo desprezível a origem da nacionalidade do sujeito ativo do crime ou do possuidor do bem jurídico prejudicado.

O que acontece, é que, em vias gerais, os crimes que são praticados na internet tem sua fase de *iter criminis,* expressão em latim que significa caminho do delito, que em direito penal é utilizado para delinear as etapas de evolução de um delito, ou seja, de sua ideia até sua consumação, esse processo pode ser desenvolvido em locais diferentes, podendo se estender por vários estados e até mesmo, países. Eis que surge o problema da competência, uma vez que é necessário saber em qual local se deu o delito.

Em primeiro lugar, é primordial que se saiba se os lugares em que o crime foi cometido é no país de origem ou em país diverso. As infrações penais adolescidas em diferentes lugares dentro do mesmo território recebem o nome de delitos plurilocais, já os que são executados em países diferentes, são nomeados de crime a distância. Inúmeros autores acreditam que esta questão pode ser facilmente resolvida pelo artigo 70, caput do Código de Processo Penal: "A competência será, de regra, determinada pelo local em que se consumar a infração[56]".

Embora isso não seja tão simples, o ilustre promotor de justiça do estado de São Paulo, Gabriel Cesar Zaccaria de Inellas esclarece,

> "Não é algo simplório delimitar a competência pelo art. 70 do Código de Processo Penal. Se ocorrerem, em países diversos, os atos executórios e os resultados, temos os denominados crimes a distância. Todavia, sendo o crime um todo indivisível, tanto nos casos dos crimes a distância, quanto nos casos dos crimes plurilocais, basta que uma de suas características tenha se realizado em território nacional para solucionarmos a questão da competência; pouco importa que a infração penal seja de igual modo, punida no outro país; produzindo efeitos no Brasil, aplicar-se-á a lei penal brasileira. com relação aos delitos a distância, a competência da autoridade judiciária brasileira encontra-se fixada pelo disposto nos parágrafos 1º, 2º e 3º do artigo 70 do Código de Processo Penal[57]".

Apesar disto, em se tratando de crimes cometidos pela internet, a verdade é que alguns magistrados e operadores do direito acabam utilizando analogias para adequar a lei ao caso concreto, fato que deveria ser proibido, considerando que o direito penal não admite o uso de analogias, mas enquanto não sobrevier lei destinada a este assunto, atualmente esta é a melhor alternativa a ser tomada.

Saliente-se que a solução para os problemas que abrangem o estelionato virtual e outros crimes cibernéticos estão longe de serem solucionados. A simples

---

[56] BRASIL. **Código Penal Brasileiro**. Organização dos textos, notas remissivas e índices por Juarez de Oliveira. 46. ed. São Paulo: Saraiva, 2000.

[57] INELLAS, Gabriel César Zaccaria de. **Crimes na Internet**. 2º ed., atualizada e ampliada. São Paulo: Editora Juarez de Oliveira, 2009. p.122.

tipificação do tipo penal não será suficiente para coibir esta prática que vem devastando a sociedade, é preciso que o estado atue de forma preventiva no combate a estes crimes e informe a sociedade sobre como coibi-los e evita-los. O tópico seguinte se dedica a apontar outras modalidades comuns de crimes de internet, exibindo a correlação com o estelionato virtual.

3.2 OUTROS CRIMES RELACIONADOS

Infelizmente, devido à internet ser um meio vasto de comunicação com milhares de usuários, inúmeros crimes vem sendo cometido por seu intermédio, não restringindo-se tão somente ao estelionato virtual, tema deste trabalho, mas estendendo-se a outros tipos penais, os quais serão destaque nos próximos parágrafos.

O primeiro a ser relacionado neste rol é o crime de racismo, que cada vez mais é exercido com o auxílio da internet e do computador. O racismo encontra-se inserido na lei nº 7.716/89 e tem como punição a reclusão de dois a cinco anos e multa. O racismo é um dos delitos mais repudiados e condenáveis pela legislação penal e pela coletividade, considerando que fazer qualquer tipo de distinção devido à cor do indivíduo é algo inaceitável, de forma que a própria Constituição Federal afirmar que todos são iguais perante a lei, e que qualquer forma de discriminação será punida severamente.

Numerosos grupos racistas encontraram na internet uma forma de expor seus pensamentos condenáveis em páginas da web, acreditando que assim poderiam ficar livres de possíveis sanções por parte das autoridades. O fato é que a propagação do racismo via internet ou *e-mail* acaba sendo mais prejudicial que a conduta exercida pessoalmente, pois atinge um numero maior de pessoas, daí a importância em se averiguar mais rigorosamente estas ocorrências.

Gabriel Cesar Zaccaria de Inellas compartilha a seguinte informação:

> “Recentemente, a Policia Federal e o Ministério Público Federal, apreenderam, mediante o competente mandado de busca e apreensão, na capital do estado de São Paulo, fato material de cunho nazista, que estava veiculado através da internet. O material pertencia ao grupo imperial *Klans of Brazil,* ramificação brasileira, da organização nazista norte-americana *Ku Klux Kan.* O usuário foi indiciado pela prática de crime de racismo e o site

> do grupo www.kkkk.net/brazil foi tirado do ar. O conteúdo do site incitava o "castigo para os judeus", denominando-os de "filhos do demônio[58]".

Outro crime recorrente na rede mundial de computadores é o crime de furto eletrônico. O furto no CPB é predito no artigo 155,caput, e visa proteger o bem alheio móvel, seja ele qual for. Nos casos de furtos virtuais, a ação se dá por intermédio de fraudes que burlam os sistemas de segurança das empresas privadas ou de agencias bancárias. Através destas fraudes, o criminoso consegue adquirir informações e capturar programas ou dados que não são disponíveis gratuitamente para o público, caracterizando a subtração do bem alheio.

No âmbito dos tribunais e da doutrina brasileira já, é pacificado o entendimento de que é absolutamente possível o crime de furto praticado pela internet, que embora ainda não possua tipificação penal própria, já está sendo punido há algum tempo.

O crime de dano também vem se alastrando diariamente no ciberespaço, principalmente em resultado aos milhares de vírus de computador que existem. O dano é caracterizado pelo prejuízo ou ofensa a um bem jurídico tutelado, seja ele patrimonial ou extrapatrimonial, que foi causado por uma ação comissiva ou omissiva do agente.

Sem sombra de duvidas, o vírus é o principal gerador de danos aos usuários que navegam na rede mundial de computadores, sabendo-se que muitos deles podem inutilizar por completo o *desktop* (computador de mesa) ou o *notebook* do cidadão desavisado que o instala em seu equipamento sem tomar o devido conhecimento.

Nesta esfera de raciocínio, a professora Maria Helena Junqueira Reis explica:

> "Os principais, e mais danosos tipos de vírus existentes são os vírus alterador, como o próprio nome indica, altera os dados contidos em bancos de dados, arquivos, documentos e planilhas. Atua de forma aleatória. É altamente destrutivo. O vírus catastrófico, diferentemente do anterior, é ativado repentinamente e causa danos, completos e imediatos. Esse vírus apaga arquivos de sistema e destrói ou inutiliza todas as informações contidas no disco rígido. O vírus genético é começo, meio e fim dos programas; em algum momento, em resposta a um sinal esperado, ativa-se e destrói ou modifica os arquivos[59]".

---

[58] INELLAS, Gabriel César Zaccaria de. **Crimes na Internet**. 2º ed., atualizada e ampliada. São Paulo: Editora Juarez de Oliveira, 2009. p.53.

[59] REIS, Maria Helena Junqueira. **Computer crimes a criminalidade na era dos computadores.** Belo Horizonte: Del Rey editora,1997. P. 34/35.

A pornografia infantil, infelizmente também se espalha com força pela internet. Muitos indivíduos repudiáveis sentem prazer em divulgar estas fotos ou vídeos contendo cenas de nudez ou sexo explícito com crianças e adolescentes indefesas, que são enganadas e atraídas por estes delinquentes diariamente pelas ruas de nosso país.

A pornografia infantil é reprimida pelo Código Penal em seu artigo 234, que recebeu reforço com a alteração dos artigos 240 e 241 e no Estatuto da Criança e do Adolescente, lei nº 8.069/90. Embora os respeitosos diplomas legais façam previsão deste crime, a falta de legislação aplicada ao tema específico abre uma porta para que os criminosos continuem propagando este conteúdo proibido, satisfazendo seus desejos obscuros.

Gabriel Cesar Zaccaria de Inellas faz a seguinte consideração acerca da pornografia infantil vinculada a internet:

> "O delito prescinde da ocorrência de dano efetivo: basta que o escrito, desenho ou estampa, ofendam o pudor público. O elemento subjetivo do tipo é o dolo, tanto no *caput,* quanto no paragrafo único, consistente na finalidade de comercializar, distribuir ou expor ao público o objeto material do crime. No caso, o momento consumativo ocorre com a realização de qualquer das condutas. Portanto, não será necessário, para a configuração do momento consumativo, que alguém tenha acesso ao escrito ou objeto obsceno, nem que o pudor público seja efetivamente atingido, bastando a mera possibilidade de que tal aconteça, posto que a doutrina o considera crime de perigo. Consideram ainda, os doutrinadores, que, se o crime for cometido através da imprensa, a infração penal não será aquela do art. 234 do código penal, mas, sim, o crime capitulado no artigo 17 da lei de imprensa[60]".

Finalizando a apresentação de crimes correlatos ao estelionato virtual em seu *modus operandi,* têm-se os delitos que vão contra o consumidor, antevistos no título II do Código de Defesa do Consumidor – lei nº 8.078/90, que trata das infrações penais advindas das relações de consumo.

Com a chegada do comércio virtual, ou *e-commerce,* muitas pessoas deixaram de realizar suas compras pelo modo tradicional, dirigindo-se às lojas ou shoppings para adquirir o que necessitam, optando por fazê-las no conforto de seu lar ou de seu ambiente de trabalho com o auxilio do computador. Assim como as

[60] INELLAS, Gabriel César Zaccaria de. **Crimes na Internet**. 2º ed., atualizada e ampliada. São Paulo: Editora Juarez de Oliveira, 2009. p.53. p.68/69.

aquisições feitas de maneira normal podem acarretar uma serie de danos ao consumidor, na internet não poderia ser diferente, existindo de igual forma alguns impasses quanto às relações de consumo.

Um dos principais problemas relativos a compras na internet é a dificuldade de troca de mercadoria em caso de defeito de fabricação ou por qualquer outro motivo, pois em vias gerais, a empresa emitente se localiza em estado ou país diverso do emissor, fazendo com que haja um impasse em saber quem arcará com os custos do envio. Isso se dá devido a não haver legislação reguladora do tema, deixando a cargo das partes a resolução do conflito.

Outro ponto enfraquecedor das relações de consumo virtual é a insegurança que existe no tocante ao pagamento do bem adquirido. Em maioria indiscutível, o pagamento é efetuado com o cartão de crédito do consumidor, que insere os dados contidos em seu escopo no site da loja, lançando-os ao oceano virtual, e muitas vezes se torna vítima de fraudes e clonagens.

Seguindo este raciocínio, o nobre promotor de justiça Paulo M. Ferreira Lima explana:

> "As transações *on line* representam hoje apenas 1% no porcentual de faturamento da empresa, isto porque permanece, entre os consumidores e os lojistas, o justificável temor de fraudes com o número do cartão de crédito. Com tudo isto, apesar de o nível do comércio eletrônico no mercado brasileiro estar aquém daquele verificado nos EUA e na comunidade europeia, a adoção do comércio eletrônico no Brasil é a mais avançada de todos os países da América do sul, principalmente quanto ao sistema bancário eletrônico.
> Um em cada 20 consumidores tem sido vítima de fraudes com cartões de crédito nos últimos 12 meses, de acordo com um estudo do Gartner. Segundo o instituto, em 2001, as perdas em fraudes *on line* foram 19 vezes maiores que as registradas *off line*[61]".

Após o expositivo, chega-se a conclusão de que assim como o estelionato virtual, as fraudes no comércio eletrônico se expandem em igual velocidade, ocasionando danos morais e materiais aos que preferem fazer suas transações pela rede mundial de computadores.

[61] LIMA, Paulo Marco Ferreira. **Crimes de Computador e Segurança Computacional**. Campinas, SP. Ed. Millennium. 2005.p. 75.

3.3FORMAS DE PREVENÇÃO DOS CRIMES VIRTUAIS

A internet trouxe à sociedade moderna uma imensa facilidade e ao mesmo tempo dependência de seus usuários, seja na escola, trabalho, na rua ou em qualquer lugar onde possa ser visto seu uso indiscriminado.

Nesse sentido, o comércio eletrônico criado para facilitar a vida destes usuários traz uma série ameaças, algumas já abordadas ao longo do trabalho; elucidada esta questão, surge a necessidade de oferecer mecanismos de proteção e prevenção aos abusos praticados na rede. Proteção baseia-se no ato ou efeito de se proteger de algum dano ou crime que possa vir a ocorrer; prevenção consiste em evitar que o crime ocorra, realizando ações tendentes a interpor obstáculos no caminho da delinquência, visto que inexiste forma de garantir 100% à ocorrência destes delitos[62].

Como bem explana Silva[63], podem ser visualizadas três categorias gerais no ambiente de proteção do computador, que não se finda nesses campos, devendo ser também observadas a segurança física e o meio de comunicação eletrônica.

> *a) Software, dados e informações.*
>
> Exigências de proteção para software, dados e informações estão baseadas na necessidade de preservar a confidência, integridade e disponibilidade. A confidência pode ser requerida, porque o sistema contém dados pessoais, informações de uma organização ou até dados relacionados a segurança nacional. A integridade de dados é exigência de todo sistema de computador. Usuários do sistema exigem garantias de que mudanças sem autorização, deliberada ou acidentalmente, não aconteçam. A preocupação da disponibilidade é importante a curto e em longo prazo.
>
> *b) Serviços de processamento de dados.*
>
> Serviço de processamento pode ser o recurso mais importante para requerer proteção em casos onde a segurança nacional, a segurança ou sustento de cidadãos individuais ou serviços essenciais, são dependentes dos sistemas de computador, p.ex., controle de tráfego aéreo, informações policiais, sistemas de monitoramento médico, fundos eletrônicos de transferência, etc.
>
> *c) Equipamento de processamento de dados eletrônicos e instalação.*

[62] VALLOCHI, Savio Talamoni. Tipificação dos Crimes de Informática, métodos de combate e prevenção. São Paulo. 2004. 80p.
[63] SILVA, Jorge Vicente. **Estelionato e outras fraudes**. 1. ed. Curitiba: Juruá, 1995, p. 55.

> Esta categoria envolve a propriedade tangível. O próprio computador e materiais, as instalações físicas, bibliotecas de mídia, áreas de preparação de dados e áreas terminais, como também os serviços ambientais.

Para fins de preservação de dados e de seu sistema os usuários da grande rede devem se proteger e prevenir com o uso de todos os recursos necessários e à disposição contra essas ameaças. Pronunciando sobre o tema em comento, irei dissertar sobre alguns mecanismos de prevenção e proteção de seus equipamentos físicos e da integridade de seus usuários.

Em primeiro lugar, a primeira forma de proteção seria o uso de senhas, onde o usuário faz uso de informações pessoais para autenticar o acesso a sistema de informação de ambientes de uso pessoal, como exemplo, caixas de banco, transações eletrônicas, e-mails, entre outros. Segundo Zaniolo, alguns cuidados especiais devem ser levados em conta na formulação de senhas como: "Não estar contido em nenhuma espécie de dicionários, idiomas estrangeiros ou temas correlatos, não utilizar informações pessoais como data de aniversário, apelido ou sobrenome, usar variações de caracteres e de pontuação[64]".

Outro dispositivo de proteção do seu computador são os *softwares Antimalware*, que são ferramentas que procuram detectar e, então anular ou remover esses arquivos maliciosos de seu computador, entre eles estão os antivírus, *antispyware, antirootkit* e *antitrojan.* É importante frisar a necessidade de se ter um *software antimalware* (*malware* são programas concebidos com a intenção de causar algum tipo de dano no sistema) sempre atualizado, a fim de que atue com mais exatidão no seu sistema. E é com base nessas afirmações que o perito judicial Zaniolo[65] descreve alguns dos principais atributos do *software* antivírus:

> a) Identificar e eliminar a maior quantidade possível de vírus e *malware*;
> b) Analisar os arquivos que estão sendo obtidos pela internet;
> c) Procurar ameaças em arquivos anexados à mensagens de e-mail;
> d) Verificar continuamente os discos (rígidos, flexíveis, CD's, DVD's, dispositivos de armazenamento USB etc) de forma transparente ao usuário.

É necessário que o programa antivírus que estejam usando seja de procedência confiável, para que os bancos de dados estejam sempre atualizados, e antes de iniciar qualquer ação em seu computador faça uma varredura no sistema

[64] ZANIOLO, Pedro Augusto. **Crimes Modernos:** O Impacto da Tecnologia no Direito. Curitiba: Juruá, 2007. p. 366.
[65] Ibidem. p. 366.

para que assim possa verificar a presença de alguma ameaça que possa estar em seu equipamento eletrônico.

Também conhecidos como “parede de fogo”, o *Firewall* é um elemento de suma importância no combate aos perigos digitais, Schneier[66] conceitua-o como sendo “um mecanismo que protege a rede interna de uma organização contra *hackers* maliciosos, criminosos vorazes e malfeitores que espreitam ao longo da internet, e os mantém do lado de fora”; isolando as ameaças dos computadores. Com relação a esse tema ainda existe o *firewall* pessoal, que é um tipo específico do descrito acima, que já vem integrado ou não, podendo ser pago ou gratuito.

Quando bem configurado, o *firewall* pessoal pode ser capaz de:

> - Registrar as tentativas de acesso aos serviços habilitados no seu computador;
> - Bloquear o envio para terceiros de informações coletadas por invasores e códigos maliciosos;
> - Bloquear as tentativas de invasão e de exploração de vulnerabilidade do seu computador e possibilitar a identificação das origens destas tentativas;
> - Analisar continuamente o conteúdo das conexões, filtrando diversos tipos de códigos maliciosos e barrando a comunicação entre um invasor e um código malicioso já instalado;
> - Evitar que um código malicioso já instalado seja capaz de propagar, impedindo que vulnerabilidades em outros computadores sejam explorados[67].

Nessa espécie de antivírus se faz necessário à verificação da procedência do produto, e se é confiável, verificar a ativação correto do programa e, sobretudo procurar registrar o maior número de informações, proporcionando máxima alerta das notificações de tentativas de invasão.

Também tem os filtros *antispam,* que são integrados aos e-mails e programas correlatos, permitindo a separação de e-mails que não sejam desejados (*spams*), podendo assim, os usuários classifica-los conforme desejar. Outro recurso que pode o usuário fazer uso é os *Honeypots* e os *Honetnets*, sendo que estes são recursos computacionais de segurança destinado à serem sondados, atacados ou comprometidos, cujo valor esta na capacidade de reunir a maior quantidade de

---

[66] Apud ZANIOLO, Pedro Augusto. **Crimes Modernos:** O Impacto da Tecnologia no Direito. Curitiba: Juruá, 2007. p. 366.

[67] CERT.BR – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. **Cartilha de segurança na Internet**: Mecanismos de segurança, 03 Jun. 2012. Disponível em: < http://cartilha.cert.br/mecanismos/>. Acesso em: 10 Out. 2012, sem paginação.

informações importantes sobre tendências, comportando assim, o aperfeiçoamento na segurança das redes.

Por derradeiro, e por si o mais importante para o estudo aqui feito é o teste de reputação de *site*, que permite determinar a confiabilidade dos sites em que estejam acessando. No entanto essa aferição pode ser feita de diferentes maneiras, por meio de esquemas de cores, onde o programa indica a reputação do *site*, em verde escuro (excelente), verde claro (boa), amarelo (insatisfatório), vermelho (má) e vermelho escuro (péssima) [68]. Outra maneira de verificar é valendo-se de informações que estejam na página de acesso, é certificar que sua url (*Uniform Resource Locator)* que em tradução livre que dizer Localizador-Padrão de Recursos, que nada mais é que um localizador de recurso disponível em uma rede, podendo ela ser de internet ou intranet, esse recurso pode ser uma impressora, um arquivo.

Dessa forma, ao fazer uma busca na rede, é preciso atentar ao que aparece na janela do browser, e ver se esse endereço começa com http**S**:// (*Hyper Text Transfer Protocol Secure*) o que significa que o *site* é seguro, garantindo que os dados que sejam transferidos venham criptografados, verificando a autenticidade entre o servidor e do cliente, garantindo que a mensagem não seja vista por terceiros.

Com o avanço tecnológico, muitos *sites* imitam até url, sendo assim é necessária a observação de outros meios de identificação de seguridade do *site*, como o cadeado, que representa o certificado de segurança da pagina, pode ser visto na maioria das vezes na parte superior da página ao lado da janela de endereço ou na parte inferior da página perto da barra de ferramentas do sistema operacional.

Quando estiver fazendo alguma transação eletrônica (compra, transação bancária, etc), clique duas vezes sobre o cadeado para conferir se o certificado de segurança da página está atualizado, deve aparecer uma janela contendo o número do registro e a sua validade.

Por fim, outro mecanismo de identificação é o diretório da página, que deve ser verificado sempre, principalmente se faz uso de *sites* internacionais, ou qualquer outro, ou que venha realizar alguma transação eletrônica. É importante atentar aos

---

[68] CERT.BR – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. **Cartilha de segurança na Internet**: Mecanismos de segurança, 03 Jun. 2012. Disponível em: < http://cartilha.cert.br/mecanismos/>. Acesso em: 10 Out. 2012, sem paginação.

links de redirecionamento, não abrir *sites* desconhecidos, não fazer downloads de *sites* que não sejam seguros.

O diretório de página permite a confirmação por parte do usuário do endereço do *site*, podendo ser realizado da seguinte forma, posicionando o *mouse* (o que é) sobre algum link da página, e assim aparecerá no canto esquerdo da tela, próximo à barra de ferramenta do sistema operacional o direcionamento do site que aparece na janela de endereço.

Tais mecanismos não são totalmente eficientes, considerando que eles serviram apenas como medida preventiva para amenizar os ataques cibernéticos.

CAPITULO IV

4. PROJETOS DE LEIS SOBRE O TEMA

4.1 PROJETO DE LEI CONCERNENTE AO ESTELIONATO VIRTUAL

Já foi dito anteriormente que o crime de estelionato virtual merece atenção especial por parte dos legisladores devido ao alto grau de dano que vêm ocasionando a sociedade, portanto, não há mais tempo para se protelar os projetos que se encontram em tramitação no Congresso Nacional e que pendem de aprovação por parte dos deputados e senadores das respectivas casas.

Diariamente, novos usuários se tornam presas fáceis destes criminosos que se aproveitam da inexistência de lei para fraudar suas vítimas, oferecendo os mais variados bens e serviços e não cumprindo com sua obrigação, gerando prejuízos irreparáveis. O crime de estelionato cometido por intermédio da internet está inserido em alguns projetos de lei que se prontificam em tipificar esta e outras condutas e puni-las de maneira mais intransigente.

O projeto de lei, bem como seu substitutivo ao PLS/2000, PLC 89/2003 e PLC 173/2000, faz o pedido formal para que a lei seja alterada, abrindo espaço para a inserção de um inciso específico ao parágrafo segundo do artigo 171 do Código Penal, trazendo uma nova definição do que é o estelionato virtual e como ele deve ser punido, aumentando sua pena.

Segundo estes projetos, a redação passaria a figurar da seguinte forma:

.

> “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.” (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[69]".

Embora a ideia do projeto exposto acima seja considerada boa, o mesmo encontra-se até o presente momento parado no Senado Federal e parece não haver qualquer tipo de esforço para sua aprovação ou rejeição, levando-se em conta que ele foi apresentado em meados do ano 2000.

4.2PROJETOS DE LEI CONTRA OUTROS CRIMES VIRTUAIS

No Congresso Nacional tramitam incontáveis projetos de lei referentes aos delitos informáticos, no entanto, até o presente momento, nenhum foi sancionado ou aprovado definitivamente para que passe a ser revestido de uma norma *erga omnes.* Sabe-se que a OEA – Organização dos Estados Americanos tem pressionado fortemente o Brasil e outros países a elaborarem o quanto antes leis que regulem e tipifiquem os crimes cibernéticos.

Recentemente, A CCT - Comissão de Ciência, Tecnologia, Inovação, Comunicação e Informática aprovou o PLC 35/2012 da Câmara dos Deputados que codifica os delitos da internet, criando novos tipos penais. O autor deste projeto é o Deputado Paulo Teixeira (PT-SP). Este projeto veio à baila logo após uma atriz famosa de uma respeitada emissora de televisão brasileira ter suas imagens em cenas de nudez divulgadas e publicadas na internet.

O fato gerou uma polêmica muito grande em toda população, ocasião em que se começou a discutir a ausência de limites na grande rede, fazendo com que pessoas ficassem vulneráveis a determinadas condutas.

Neste sentido, a página eletrônica do Senado Federal publicou a seguinte notícia:

> "A Comissão de Ciência, Tecnologia, Inovação, Comunicação e Informática (CCT) aprovou projeto de lei da Câmara dos Deputados (PLC 35/2012) que tipifica crimes cibernéticos. A decisão veio depois de acordo para que a proposta fosse incluída extra pauta. Foi também aprovado requerimento de urgência para que o texto seja examinado em Plenário ainda nesta quarta-feira, com leitura, nessa instância, de parecer da Comissão de Constituição e Justiça (CCJ).
> A proposta estabelece que a devassa de dispositivo informático alheio, conectado ou não à rede de computadores, ou ainda adulteração ou

[69] Disponivel em: http://www.senado.gov.br/comunica/ agencia/pags/01.html. Acesso em: 31 de Out. de 2012.

> destruição de dados ou informações sem autorização do titular poderá levar à prisão de três meses a um ano mais multa. O projeto, de autoria do deputado Paulo Teixeira (PT-SP), foi aprovado pela Câmara dos Deputados em maio, logo depois do vazamento de fotos íntimas da atriz Carolina Dieckmann.
> O senador Aloysio Nunes (PSDB-SP) foi contra a inclusão da matéria na pauta do dia. Ele ponderou que nesse momento atua no Senado uma comissão especial de senadores com a função de reformar o Código Penal, um texto que contém capítulo especial sobre os crimes cibernéticos, decorrente do trabalho de comissão de juristas. Aloysio observou ainda que, por normas regimentais, qualquer matéria que trate de temas penais deve ser transferida para o exame desta comissão. O objetivo é assegurar que crimes e penas sejam adequadamente balanceadas em termos de conjunto.
> Outros senadores ponderaram que há urgência em definir uma legislação para os crimes pela internet. Salientaram que a comissão que está reformando o Código poderá sugerir aperfeiçoamentos à legislação que for aprovada agora. O projeto foi relatado pelo presidente da CCT, senador Eduardo Braga (PMDB-AM). Como houve emendas ao texto, à matéria deverá retornar á Câmara para exame das modificações[70]".

A aprovação do projeto referenciado acima demonstra que o governo está começando a encarar com mais seriedade e responsabilidade o assunto relativo aos crimes virtuais. O caminho a percorrer ainda é longo, mas uma lei deste porte poderá sanar muitas duvidas que cercam estes delitos, e com certeza irá reduzir as taxas de incidência desta prática criminosa.

Na data de 5 de novembro de 2003, o plenário da Câmara dos Deputados aprovou também um importante projeto de lei que irá contribuir e muito para frear esta violência virtual que se propaga diariamente. O projeto tem como proposta a tipificação de alguns crimes de informática, dentre os quais, o de estelionato. O precursor desta ideia é o deputado Luiz Piauhylino (PSDB-PE), e o PL recebeu o nº 84/1999.

Em 13 de novembro de 2003 o PL aprovado na Câmara chegou ao Senado para que fosse votado em sessão plenária, contudo, a referida votação só ocorreu três anos mais tarde, em 20 de junho de 2006, pela comissão de educação do SF. O parecer foi apresentado por Eduardo Azeredo e substituía o texto que incorporava ao PL 76/00, substituindo alguns pontos.

Em seu vasto parecer, Azeredo baseou-se na necessidade urgente em se regulamentar uma norma que versasse sobre os crimes virtuais, afirmando que o avanço dos recursos tecnológicos era capaz de gerar vazios na lei e motivavam a proliferação de fraudes e danos aos usuários. O senador citou também uma interligação com as organizações terroristas internacionais e com o tráfico de seres

[70] http://www12.senado.gov.br/noticias/materias/2012/08/29/vai-a-plenario-em-regime-de-urgencia-criminalizacao-de-delitos-na-internet. Acessado em 31/10/2012.

humanos e drogas. Devido a sua atuação constante no caso, Azeredo foi nomeado relator, e em 22 de setembro do mesmo ano mostrou-se favorável à aprovação do projeto.

Este projeto nada tem haver com o PLC 35/2012, sendo revestido de um projeto independente, pois ele acrescenta diversos crimes correlatos a uma nova seção do Código Penal, ampliando e modificando seus artigos.

Fabrízio Rosa faz a seguinte ponderação sobre o PL:

> "O PL nº 84/99 foi aprovado na forma do substitutivo da comissão de segurança pública. O relatório aprovado, do deputado Nélson Pellegrino (PT-BA), acrescenta nova seção do Código Penal para tipificar diversos crimes relacionados aos sistemas informatizados, como a difusão de vírus eletrônico, de pornografia infantil na internet e o acesso indevido a meio eletrônico ou sistema informatizado, entre outros. Também está prevista no texto a tipificação do crime de falsificação de telefone célula ou de meio de acesso a sistema eletrônico, como cartão inteligente, transmissor ou receptor de radiofrequência. Para os efeitos penais, serão considerados meios eletrônicos elementos como computador, processador de dados, disquete e CD-ROM. A rede de computadores, base de dados e o programa de computador são classificados como sistema informatizado[71]".

Muito embora o projeto tenha sido aprovado por maioria, existiram muitos vetos em seu texto, senão, vejamos: o projeto inicial era composto por 22 artigos. Após ser votado e discutido, decidiu-se por vetar 17, restando apenas 6 de sua proposta original, data vênia algumas condutas extrapolarem os limites da proporcionalidade e razoabilidade exigidas constitucionalmente, como por exemplo, a punição de quem compartilhasse músicas sem a devida autorização do autor.

Existem outros projetos de lei concernentes aos delitos informáticos, no entanto, a grande maioria foi arquivado ou não interessa ao assunto, sendo demonstrado tão-somente os mais relevantes.

[71] ROSA, Fabrízio. **Crimes de Informática.** 2º ed. Campinas: Bookseller, 2005. p. 90.

5. CONCLUSÃO

Diante do avanço dos recursos tecnológicos e científicos disponíveis atualmente, a sociedade de modo geral evoluiu mais rápido que o esperado. A internet trouxe uma série de benefícios a toda população, apresentando novidades jamais antes vistas. Com isto, alguns criminosos viram neste mundo virtual a possibilidade de cometer crimes, desvirtuando o fim para o qual ela foi criada.

Sabe-se que a sociedade se encontra em constante evolução, e junto com ela devem caminhar as leis que regem o estado, sendo alteradas e modificadas sempre que necessário para que o país continue se desenvolvendo de forma justa e igualitária, preservando o bem-estar de seus habitantes.

O estelionato virtual, tema deste trabalho, é apenas um destes crimes cibernéticos que vem se expandindo com força devastadora a cada dia, onde milhares de pessoas desavisadas acabam sendo vitimadas por estes indivíduos sem escrúpulo algum, que insistem em transgredir a lei para conseguir seus objetivos.

É fato que a internet, assim como a criminalidade, se alastra com velocidade superior as leis existentes, daí a importância em se alterar a legislação penal o quanto antes, para que se adeque aos novos tipos penais que surgem a cada dia.

É de conhecimento de todos que atuam e laboram na área do Direito, que o Código Penal Brasileiro de 1940 está parcialmente ultrapassado e necessita urgentemente de uma reforma, afinal muitas condutas que eram reprováveis à época de sua criação já não são mais tão relevantes, bem como outros comportamentos atuais que carecem ser inseridos dentro do ordenamento jurídico.

As dificuldades enfrentadas pelas autoridades em se investigar e punir os crimes informáticos refletem diretamente no aumento significativo desta prática delituosa, pois os criminosos enxergam na ausência de legislação uma “autorização” para empreenderem no crime, fazendo dele seu meio de sustento. Inúmeros debates sobre o tema têm sido propostos para regulamentar à situação, no entanto, o que se percebe, é que medidas coercitivas efetivas para coibir os *cibercrimes* ainda não saíram do papel, o que torna ainda mais difícil a ocasião.

Os projetos de lei sobre o assunto precisam ser aprovados o quanto antes, pois só assim o estado poderá demonstrar sua força perante os transgressores que usam a internet para satisfazer suas ilicitudes. Neste sentido, ressalte-se para a prioridade em se alterar o tipo penal do estelionato descrito no artigo 171 do CPB, a

fim de amenizar os prejuízos sofridos diariamente por pessoas inocentes que apostam suas fichas em situações ilusórias narradas por estes fraudadores.

Ademais, o presente trabalho visou contribuir e ajudar os pesquisadores e estudiosos do direito para que o conhecimento a respeito da matéria avance cada vez mais, servindo como apoio para a realização de novos estudos acerca do tema e também como fonte de informação a entusiastas que acreditam que a legislação penal brasileira necessita urgentemente de modificações no que tange ao direito informático.

6. REFERÊNCIAS BIBLIOGRÁFICAS

BENAKOUCHE, Tâmara, 1997, “Redes técnicas - redes sociais: a pré-história da Internet no Brasil”, **Revista USP**, n. 35, pp. 125-133. Dossiê Informática/Internet.

BITENCOURT, Cezar Roberto. **Código Penal Comentado**. São Paulo: Saraiva. 2002.

BRASIL. **Código Penal Brasileiro**. Organização dos textos, notas remissivas e índices por Juarez de Oliveira. 46. ed. São Paulo: Saraiva, 2000.

BRASIL. **Lei 9.099**, de 26 de Setembro de 1995. Dispõe sobre os Juizados Especiais Cíveis e Criminais. Diário Oficial [da] Republica Federativa do Brasil. Brasília, DF, 27 Set. 1995. Disponível em: <http://www.in.gov.br/mp_leis/leis_texto.asp?Id=LEI%209887>.

BRASIL. **Lei nº 4.117**, de 27 de Agosto de 1962. Institui o Código Brasileiro de Telecomunicações. Diário Oficial [da] Republica Federativa do Brasil. Brasília, DF, 28 Ago. 1962. Disponível em: <http://www.in.gov.br/mp_leis/leis_texto.asp?Id=LEI%209887>.

BRASIL. **Lei nº 7.232**, de 29 de Outubro de 1984. Dispõe sobre a Política Nacional de Telecomunicações. Diário Oficial [da] Republica Federativa do Brasil. Brasília, DF, 30 Out. 1984. Disponível em: <http://www.in.gov.br/mp_leis/leis_texto.asp?Id=LEI%209887>.

CALIL, Léa Elisa Silingowschi. **Revolução Digital**. Disponível em: <http://www.mundodosfilosofos.com.br/lea20.htm>.

CARVALHO, Marcelo Sávio Revoredo Menezes de. **A trajetória da Internet no Brasil**: do surgimento das redes de computadores à instituição dos mecanismos de governança. Rio de Janeiro, 2006, XX, 239 p. 29,7 cm (COPPE/UFRJ, M.Sc., Engenharia de Sistemas e Computação, 2006). Dissertação – Universidade Federal do Rio de Janeiro.

CERT.BR – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. **Cartilha de segurança na Internet**: Mecanismos de segurança, 03 Jun. 2012. Disponível em: < http://cartilha.cert.br/mecanismos/>. sem paginação.

COSTA DO VALE, Maria do Socorro. COSTA, Denise Coutinho. ALVES JR, Nilton. **Internet**: Histórico, evolução e gestão. p. 30. Disponível em: <http://registro.br/info/dpn.html>

DANTAS, Vera. **Guerrilha Tecnológica:** a verdadeira história da política nacional de informática. Rio de Janeiro, LTC. 1988.

DIAS, Lia Ribeiro, CORNILS, Patrícia, **Alencastro:** o general das telecomunicações**.** São Paulo, Plano Editorial. 2004.

GOMES, Luiz Flávio. SOUSA, Áurea Maria Ferraz de. ***Agravantes e atenuantes****: preponderância das circunstâncias subjetivas. Críticas. Ago. 2010.* Disponível em:< http://www.lfg.com.br>.

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

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

INELLAS, Gabriel César Zaccaria de. **Crimes na Internet**. 2º ed., atualizada e ampliada. São Paulo: Editora Juarez de Oliveira, 2009.

JESUS, Damásio E. de. **Direito Penal**. 1° Volume - Parte Geral, 20ª ed., São Paulo: Editora Saraiva, 1997.

KELLY, Kevin. **Out of Control:** The New Biology of Machines, Social Systems and the Economic World. Basic Book. Reading, MA, Perseus Press. 1995.

LAURIA, Thiago. **Suspensão Condicional da Pena X Suspensão Condicional do Processo**. Disponível em: <http://www.jurisway.org.br/v2/dhall.asp?id_dh=143 >.

LIMA, Paulo Marco Ferreira. **Crimes de Computador e Segurança Computacional**. Campinas, SP. Ed. Millennium. 2005.

MARQUES, Samuel. Estelionato: Prática comum ao longo da história. **Panorama Empresarial**. Resende. Setembro de 2009. Disponível em: <http://cdlresende.com.br/index.php?menu=17&jornal=5&materia=218>

MARTINS, Sandra Carla Castro Marques. **Estelionato Eletrônico:** a (des) necessidade de uma tipificação legal. Disponível em: <http://www.ambitojuridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=10133&revista_caderno=3>.

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

_____. **Manual de direito penal.** 20. Ed. São Paulo: Atlas, 2003.

MENEZES, André Gonçalves de. AMORIM, Eduardo Antônio Andrade. NAPOLI, Lorena Ornelas. MUTIM, Marcel Santos. **O Estelionato Eletrônico**: Uma breve reflexão sobre o Delito Informático. 22 p. Salvador.

PRADO, Luiz Regis. **Curso de Direito Penal Brasileiro**. Parte Especial - arts. 121 a 183. V. 2. Ed. Filiada. 2002. p. 523.

REIS, Maria Helena Junqueira. **Computer crimes a criminalidade na era dos computadores.** Belo Horizonte: Del Rey editora,1997.

ROSA, Fabrízio. **Crimes de Informática.** 2º ed. Campinas: Bookseller, 2005.

SANTOS, Luiz Carlos dos. Como funciona o protocolo FTP?. **HTML STAFF.** 26 set. 2006. Disponível em: <http://www.htmlstaff.org/ver.php?id=985>.

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

SILVA, Remy Gama. **Crimes da Informática**. Ed. CopyMarket.com, 2000. 30 f. Dissertação (Especialização em Direito Penal). Disponível em: < http://www.cesarkallas.net/arquivos/livros/direito/00715%20-%20Crimes%20da%20Inform%E1tica.pdf>

SILVEIRA, Renato de Mello Jorge. **Direito penal supra-individual**: interesses difusos. São Paulo: Revista dos Tribunais, 2003.

TELEBRASIL ASSOCIAÇÃO BRASILEIRA DE TELECOMUNICAÇÕES, 2004 **Telebrasil:** 30 anos de sucessos e realizações. Rio de Janeiro, Graphbox.

TIGRE, Paulo Bastos. **Indústria Brasileira de Computadores:** perspectivas até os anos 90. Rio de Janeiro, Campus. 1987.

UNESCO, 1987, **Communication and society:** a documentary history of a new world information and communication order seen as an evolving and continuous process, 1975-1986. Paris, UNESCO.

VALLOCHI, Savio Talamoni. **Tipificação dos Crimes de Informática, métodos de combate e prevenção**. São Paulo. 2004. 80 f. Dissertação (Pós Graduação) – Faculdade Senac de Ciências Exatas e Tecnologia.

ZANIOLO, Pedro Augusto. **Crimes Modernos:** O Impacto da Tecnologia no Direito. Curitiba: Juruá, 2007.