UNIVERSIDADE ESTADUAL DA PARAÍBA
CENTRO DE CIÊNCIAS JURÍDICAS
CURSO DE DIREITO

GEORGE DE OLIVEIRA SOUSA

OS CRIMES CIBERNÉTICOS E SUAS FORMAS DE COMBATE

Campina Grande
2012

GEORGE DE OLIVEIRA SOUSA

OS CRIMES CIBERNÉTICOS E SUAS FORMAS DE COMBATE

Trabalho acadêmico orientado apresentado à Universidade Estadual da Paraíba em cumprimento às exigências para obtenção do grau de Bacharel em Direito.

Orientador: Prof. Dr. Félix Araújo Neto

CAMPINA GRANDE
2012

S725c Sousa, George de Oliveira.
Os crimes cibernéticos e suas formas de combate [manuscrito] / George de Oliveira Sousa.– 2012.
49 f.

Digitado.
Trabalho de Conclusão de Curso (Graduação em Direito) – Universidade Estadual da Paraíba, Centro de Ciências Jurídicas, 2012.
"Orientação: Prof. Dr. Felix Araujo Neto, Departamento de Direito Público".

1. Crimes cibernéticos. 2. Convenção sobre o cibercrime. 3. Projeto de lei 84/1999. I. Título.

21. ed. CDD 345

GEORGE DE OLIVEIRA SOUSA

OS CRIMES CIBERNÉTICOS E SUAS FORMAS DE COMBATE

Aprovado em: 20 / 06 / 2012

BANCA EXAMINADORA

Prof. Doutor Félix Araújo Neto
Centro de Ciências Jurídicas da UEPB
Orientador

Prof. Mestre Herry Charriery da Costa Santos
Centro de Ciências Jurídicas da UEPB
Examinador

Prof. Especialista Jaime Clementino de Araujo
Centro de Ciências Jurídicas da UEPB
Examinador

DEDICATÓRIA

Tempo houve em que deles muito precisei, e me foram eles fartos e atenciosos. Aos amigos dedico.

AGRADECIMENTOS

A Deus primeiramente, pela vida tão graciosa que me deu, pela determinação que não me deixou faltar.

Ao meu orientador, Professor Felix Araújo Neto, sempre solícito nas valiosas orientações, professor querido de todos os alunos, e que comporta em si grande saber.

Aos meus familiares que enxergaram em mim uma pessoa digna de merecer o saber e que sempre me incentivaram.

Aos meus pais e irmãos.

As pessoas que passaram em minha vida, e ainda que indiretamente contribuíram para o meu esforço.

Por ultimo, agradeço aos amigos de todas as horas, que sempre estiveram comigo, que não me deixaram desistir, que me incentivaram, que viram em minha vitória a sua vitória, saibam que jamais esquecerei o vosso apoio.

RESUMO

O presente estudo teve como finalidade analisar a atual dificuldade existente no que se refere ao combate aos crimes cibernéticos, sobretudo pela ausência de legislação penal específica que tipifique algumas das condutas lesivas praticadas por meio da *internet*. Define o que são crimes cibernéticos próprios e impróprios, atentando para a possibilidade de aplicação do Código Penal em alguns casos ante a ausência de legislação própria, bem como aborda uma série de condutas difíceis de serem combatidas, por não serem ainda tipificadas. Aborda a possibilidade de aplicação da Lei de Interceptações Telefônicas na investigação dos crimes perpetrados através da rede mundial de computadores, trazendo o entendimento jurisprudencial acerca do tema. Traz à tona a Convenção sobre o Cibercrime, demostrando a grande importância desse documento internacional no combate aos crimes cometidos mediante o uso de equipamentos informáticos. Apresenta o Projeto de Lei 84/1999, tentativa nacional de dificultar o cometimento de crimes cibernéticos propondo a tipificação de condutas que hoje são cometidas na área de informática, demostrando ser um projeto que caso seja aprovado passará a suprir a dificuldade legal no combate aos crimes cibernéticos.

Palavras-chave: Crimes Cibernéticos, Convenção sobre o Cibercrime, Projeto de Lei 84/1999.

ABSTRACT

This study aimed to analyze the current problems existing as regards the combat against cyber crime, overcoat by the absence of specific penal legislation exemplify that some of the harmful behavior practiced over the internet. Define what are a proper and improper cyber crimes, nothing the possibility of application of the Penal Code in some cases in the absence of specific legislation, in addiction a series of ducts to treat because they are not typed yet. Broaches the possibility of applying the Law of Telephone intercepts in investigating the crimes perpetrated through the World Wide Web, bringing the understanding of jurisprudence on the subject. Brings up the Convention on Cyber crime, demonstrating the great importance of this international document on combating crimes committed over the use of computer. Introduces the Bill 84/1999, the national effort to hinder the commission today in computer science, demonstrating that a project be approved if it is passed to supply for the law difficulty in combating crimes cyber.

Keywords: Cyber Crime, Convention on Cyber Crime, Bill 84/1999

SUMÁRIO

INTRODUÇÃO

Atualmente a sociedade passa por grandes mudanças com o advento dos recursos tecnológicos de comunicação e informação. Hodiernamente, os benefícios que advêm da avançada tecnologia da informação são muitos, sendo o principal, a agilidade com que se tem acesso as mais diversas dinâmicas das relações sociais, beneficiando a atuação nos campos políticos, econômico, social, bem como no âmbito das relações privadas. Infelizmente tamanho benefício, vem também acompanhado de uma parte negativa, que é a enorme quantidade de crimes cometidos através de meios eletrônicos, crimes esses muitas vezes, difíceis de serem combatidos.

A tecnologia atual permite que um crime eletrônico possa ser efetuado em um país, sendo que o mesmo pode ter sido planejado em local muito distante, ate mesmo outro país, o que obviamente traz sérios prejuízos a apuração desse tipo de delito, mormente pelas diferenças legislativas, entre os países, o que pode muitas vezes evoluir para uma questão que envolva os ramos do direito internacional, aquele em que se deu o crime, e aquele onde ele foi planejado ou teve a execução iniciada. A tecnologia atual de comunicação é extremamente eficiente, podendo inclusive salvar vidas, melhorando diagnósticos, permitindo rápida comunicação entre pontos remotos do globo, dentre outros tantos benefícios, no entanto a mesma tecnologia que salva é usada para o cometimento de novas modalidades de crimes.

Atualmente, as infrações penais, são cometidas das mais diversas formas, dentre as quais estão aquelas cometidas mediante recursos oferecidos pelos computadores ligados a internet. Os criminosos passaram a atualmente utilizar-se da tecnologia de comunicação existente para o cometimento de crimes, com o auxilio desses meios, quando, por exemplo, se comunicam pela internet para o cometimento de um homicídio, extorsão, ou qualquer outra modalidade criminal, e principalmente, passaram a cometer crimes nos próprios meios eletrônicos, quando, exemplificando, se utilizam da internet para desviar indevidamente dinheiro de contas bancarias, disseminar *vírus*, colher dados pessoais.

Ao Estado é imprescindível cumprir o seu poder-dever de punir tais praticas criminosas cometidas mediante meios eletrônicos, e para tal é necessária a existência de uma legislação atualizada, que possibilite apontar a autoria de quem comete crime pela internet, o que atualmente é difícil, considerando-se que a referida modalidade criminosa muitas vezes não deixa sequer pistas da autoria delitiva. Infelizmente a Legislação Penal Pátria não avançou na mesma velocidade com que se desenvolveram as condutas criminosas cometidas

pelos meios eletrônicos, ficando muitas condutas lesivas cometidas pela internet, impunes, pelo fato de não haver ainda tipificação que as combata.

O presente estudo pretende demonstrar a dificuldade em outros casos a ausência da legislação penal pátria com suas leis atuais, em combater as já referidas modalidades criminosas pela falta de elementos que subsidiem a produção de provas, e também a ausência de tipificação penal de algumas condutas lesivas, para tal, analisa-se a Convenção sobre Cibercrime, importante documento em nível mundial, e em âmbito nacional o Projeto de Lei nº 84/1999, tentando demonstrar se suprirá a lacuna legislativa penal atual caso seja convertido em lei. Para tal, é de extrema necessidade, diferenciar as condutas lesivas que se utilizam da *internet* para o cometimento de crimes, daquelas que não possuem resultado exteriorizado, como invasão de rede, por exemplo.

É com essa intenção que abordaremos a possibilidade de aplicação da Lei nº 9.296/96 para a consecução de provas de crimes cometidos através da *internet* como medida amenizadora enquanto inexistir legislação específica relativa ao tema, bem como a aplicação do Código Penal em alguns casos, ao passo que em outros existe uma lacuna legislativa para a tipificação de delitos cometidos utilizando-se de meios eletrônicos.

CAPÍTULO I
CRIMES CIBERNÉTICOS – A NOVA MODALIDADE DE COMETIMENTO DE CRIMES

1.1 Crimes de Informática Próprios e Crimes de Informática Impróprios

Atualmente é forçoso reconhecer que os avanços tecnológicos causam transformações cada vez mais rápidas no mundo fático, proporcionando o desenvolvimento nos campos comercial, político e pessoal, em âmbito global, notadamente por possibilitarem maior acesso às informações, ao conhecimento de um modo geral, uma maior rapidez nas transações governamentais, pessoais e comerciais. Os avanços advindos da moderna tecnologia em uso atualmente, não se pode negar, são bons e proveitosos para a sociedade, porem, necessário é reconhecer que paralelamente às benesses trazidas pela tecnologia atual surgiram também indesejadas consequências, tais como as novas modalidades e condutas criminosas, os chamados *cibercrimes*[1], além de condutas outras que apesar de não serem ainda tipificadas como crimes, são deveras lesivas. Tais condutas são em sua quase totalidade praticadas com o auxilio da informática, notadamente com a utilização da rede mundial de computadores, a *internet.*

Nesse diapasão surge a necessidade de definirmos o que são crimes de informática próprios e impróprios; antes porém, entendemos ser de salutar didática trazer a lume o conceito de crime para melhor inteireza do assunto abordado. Noutro passo, reservamo-nos das discussões doutrinárias acerca das teorias do crime, vez que além de exaustivo, desviaria o foco do presente trabalho, de sorte que conceituaremos o vocábulo crime e seguidamente discorreremos sobre os crimes de informática próprios e crimes de informática impróprios.

Assim, na pacífica forma tripartida analítica de conceituação do delito, crime seria uma ação ou omissão típica, antijurídica e culpável. Por típica, devemos conceber a conduta dolosa ou culposa, omissiva ou comissiva que gera um resultado, devendo haver um nexo de causalidade entre a conduta e o resultado, devendo ainda ocorrer a tipicidade, que é a adequação do fato à norma descrita na lei penal. Antijuridicidade, por seu turno, é a oposição

[1] CONTI, Fátima. **Afinal, o que é cibercrime?**. 2008. Disponível em: < http://www.dicas-l.com.br/interessa/interessa_20080814.php>. Acesso em 10 abr. 2012. Nos termos conceituais apresentados por Conti, cibercrimes são: *Crimes de informática ou cibercrimes são condutas ilegais realizadas com o auxílio de um computador, normalmente conectado à internet*.

da conduta praticada em relação ao ordenamento jurídico, aos bens por ele tutelado. Por ultimo, a culpabilidade como ultimo elemento integrante da definição de crime, que é a reprovação do agente que praticou a conduta típica e antijurídica.

Assis Toledo conceitua o crime da seguinte maneira:

> Dentre as várias definições analíticas que têm sido propostas por importantes penalistas, parece-nos mais aceitável a que considera as três notas fundamentais do fato crime, a saber: ação típica (tipicidade), ilícita ou antijurídica (ilicitude) e culpável (culpabilidade). O crime, nessa concepção que adotamos, é, pois, ação típica, ilícita e culpável.[2]

No que, corrobora o argentino Eugenio Raul Zaffaroni:

> Delito é uma conduta humana individualizada mediante um dispositivo legal (tipo) que revela sua proibição (típica), que por não estar permitida por nenhum preceito jurídico (causa de justificação) é contrária ao ordenamento jurídico (antijurídica) e que, por ser exigível do autor que atuasse de outra maneira nessa circunstância, lhe é reprovável (culpável).[3]

Assim sendo, crime é fato típico, antijurídico e culpável, conforme a melhor doutrina.

Há crimes que podem ser praticados através de um computador conectado à *internet,* porém o próprio equipamento de informática também pode ser objeto do delito, variando conforme a utilização que se dê aos mesmos, sendo tais crimes classificados em crimes próprios e impróprios.

Diremos que são crimes próprios, aqueles praticados através de equipamento de informática visando atingir as suas funções, como por exemplo, provocar lentidão nos sistemas, mudar arquivos de seus locais habituais dificultando assim, sua localização, desconfigurar as características da maquina alvo do delito, ou seja, crimes que dificultem ou impossibilitem a utilização do equipamento de informática.

Em obra que trata sobre investigação criminal e informática, Eduardo Marcelo Castela conceitua que em informática os crimes próprios são todos aqueles relacionados diretamente com a informática. Especificam situações em que a ação está voltada para a máquina, aos comandos e às funções que ela armazena e exerce. [4]

---

[2] TOLEDO, Francisco de Assis *apud* GALVÃO, Fernando; GRECO, Rogério. **Estrutura Jurídica do Crime**. Belo Horizonte: Mandamentos. 1999. p. 30.
[3] ZAFFARONI, Eugênio Raúl *apud* GRECO, Rogério. **Curso de Direito Penal**.. 4.ed. Rio de Janeiro: Ímpetus, 2004, p. 159.
[4] CASTELA, Eduardo Marcelo. **Investigação Criminal e Informática**. Curitiba: Juruá, 2005, p. 110.

No que concerne às referidas condutas, é sabido que o sistema judicial brasileiro possui severas dificuldades em punir os infratores, tanto pela ausência de tipos penais específicos para os crimes de informática, quanto pela dificuldade de colheita de provas em relação a tais delitos. Castela argumenta inclusive que nesse contexto, existe um atraso de, pelo menos, 10 (dez) anos, em relação à Europa, onde vige legislação sobre o tema de forma muito específica. [5]

Por sua vez, são impróprios os crimes de informática praticados por indivíduos que apenas se utilizam do equipamento de informática como instrumento necessário para cometer o crime. Tais tipos de delitos encontram-se já tipificados na legislação penal pátria e na maior parte das vezes, produzem resultado naturalístico, ou seja, introduz alguma modificação no campo fático, contudo podem ser praticados de outro modo que não seja com o auxilio dos meios de informática. São exemplos os crimes de injuria, furto, dentre outros, que já se encontram tipificados em leis penais, podendo ser obviamente praticado de outros modos sem o auxilio da informática.

Nesse sentido, precisa é a lição de Castela que esclarece que os crimes de informática impróprios são:

> [...] (impuros), onde a máquina é tão-somente um meio, um instrumento para se alcançar o fim desejado. Nesta categoria, estão os delitos constantes no Código Penal e legislação especial [...] Notadamente, boa parte das ocorrências policiais está sendo tipificada como estelionato, mas nada impede a prática de furto, dano, ameaça, calúnia, injúria, difamação e até mesmo , de homicídio. Nesse último caso, pode-se imaginar aquela situação onde há um Hospital moderno ao extremo, cuja estrutura é totalmente informatizada. Chegando, mesmo, a ministrar medicamentos aos seus pacientes de UTI de forma automática, com poderosas máquinas que acompanham o tratamento e as reações. Se um *hacker*, bem preparado e com objetivos cruéis, obtiver o acesso e ingressar no sistema, poderá escolher a vítima, sem ao menos lhe dar qualquer chance de defesa e, para dificultar qualquer investigação, apaga o caminho percorrido. [6]

Assim sendo fica claro, que o crime de informática próprio tem a finalidade precípua de atingir o próprio equipamento eletrônico, o seu sistema, turbando o seu funcionamento, não podendo ser praticado de outra forma que não seja por intermédio do equipamento de informática, enquanto o crime de informática impróprio é aquele praticado através da máquina, utilizando-a como meio pelo qual deva atingir seu intento, o que quer dizer que o crime poderia ser praticado de outra maneira, preferindo o agente porém comete-lo com o auxílio de meios eletrônicos.

---

[5] CASTELA, Eduardo Marcelo. **Investigação Criminal e Informática**. Curitiba: Juruá, 2005, p. 110.
[6] CASTELA, Eduardo Marcelo. **Investigação Criminal e Informática**. Curitiba: Juruá, 2005, p. 110.

O mundo cibernético é dinâmico por natureza, além de ser invisível o crime que se dá nas redes sociais, possibilitando ao agente criminoso uma grande furtividade, vez que o mesmo não precisa se expor ao cometer crimes auxiliado por meios eletrônicos, o que torna extremamente difícil em ambas as modalidades de crimes cibernéticos, os próprios e impróprios, a colheita de provas que embasem uma posterior ação penal, sem contar uma série de condutas que apesar de serem danosas, não são tipificadas ainda como delito em nossa legislação.

Por esses motivos, Celso Ferro Júnior explica que hoje, o trabalho de instrução criminal está afetado por insuficiências de ordem técnica e científica. Auxilia para esta situação a falta de investimento, descredibilidade e legislação obsoleta quanto à produção da prova. [7]

1.2 Condutas lesivas praticadas por meio da internet

São variadas as condutas lesivas praticadas através da rede mundial de computadores, a *internet*. Em primeiro lugar veremos a invasão de sistemas de informática, quer sejam eles governamentais quer sejam de empresas privadas, por pessoas que se aproveitam de alguma falha no sistema, para visualizar dados podendo ou não apropriar-se deles, torná-lo lento ou impossibilitado de funcionar, dificultando o trabalho dos proprietários e administradores dos sistemas, prejudicando assim as pessoas que dependem do perfeito estado de funcionamento de tais sistemas de informática. Mais uma vez nos socorremos a Eduardo Marcelo Castela que esclarece que, esse tipo de invasor não visa lucro, quer a glória de praticar um ato não alcançado anteriormente por ninguém[8].

É interessante notar que a maioria das pessoas que realizam esse tipo de invasão a sistemas de informática ou a rede de computadores, visando torná-los lentos, ou impossibilitar o seu uso, não visam obter ilícitas vantagens financeiras. Segue a lição de Douro Moura:

> [...] muitas vezes são jovens que, com a ajuda da mídia, chegam aos lares e conseguem seu maior objetivo: notoriedade e fama. Os prejuízos causados pelas suas interferências, entretanto são maiores que qualquer campanha publicitária de sucesso internacional. Delegado Mauro Marcelo: "Esses adolescentes tem muito tempo para gastar, muita adrenalina para queimar e um computador na mão. Essa mistura, sem o devido acompanhamento se transforma numa mistura explosiva"[9]

---

[7] FERRO JUNIOR, Celso Moreira Ferro. **A tecnologia na Investigação Criminal**. Disponível em <http://www.datavenia.net/opiniao/celso.html> Acesso em 02. abr. 2012

[8] CASTELA, Eduardo Marcelo. **Investigação Criminal e Informática**. Curitiba: Juruá, 2005, p. 125.

[9] MOURA, Douro. **Crimes Virtuais no Brasil**. Disponível em: <http://www.buscalegis.ufsc.br/revistas/index.php/buscalegis/article/download/11605/11170>. Acesso em 13. Abr. 2012.

Tal tipo de invasor provoca prejuízos ao administrador do sistema, ao proprietário, e finalmente as pessoas que dele necessitam, porem para que sejam punidos é necessário que haja a tipificação de tais condutas na legislação penal pátria, suprindo a atual lacuna legislativa no tocante ao combate aos crimes cibernéticos, fato este que ainda não aconteceu, como continua nos esclarecendo Castela:

> Falar ou acreditar que os invasores de rede o fazem, somente, para testar a segurança, como forma de mostrar que há falhas, é o mesmo que se dissesse que os pichadores entram em nossas casas e sujam as paredes, alegando que só o fazem para mostrar as deficiências na segurança do condomínio ou da residência. Se alguém for contratado para agir e testar, é uma situação; se, no entanto, este alguém entra sem ser convidado ou sem estar agindo em nome dos proprietários, é uma afronta. [10]

Com o mesmo pensamento o palestrante Christopher Painter[11], durante seminário acontecido em 28/05/2008 no Conselho de altos estudos e avaliação tecnológica da Câmara dos Deputados, esclarece: "Eu sei que alguns anos atrás na Argentina alguns *hackers* entraram no *site* do Supremo Argentino. Mais uma vez, eles não roubaram nada tangível e não puderam ser processados. Isso ilustra a necessidade de haver esse tipo de legislação".

Fica claro que tal tipo de invasor não é punido porque esse tipo de conduta descrita não foi ainda tipificada como crime, nem tampouco há legislação que embase a produção de provas que comprovem a existência de materialidade delitiva além de indícios de autoria, o que impossibilita a punição do invasor, restando-lhes a impunidade.

Outro exemplo de conduta lesiva cometida através da rede mundial de computadores, é o envio de uma grande quantidade de mensagens de texto não solicitadas, mensagens estas que são enviadas simultaneamente a vários destinatários, principalmente através do correio eletrônico. Essas mensagens são chamadas de *spams*[12]. Tal tipo de conduta, segundo pesquisa realizada pela ISS/IBM[13] é a mais comum cometida pela *internet*. A conduta de enviar *spam* é além de comum é grave, pelo fato de a empresa ou mesmo o indivíduo ao enviar *spam*, visa o lucro, já que na maioria das vezes esse tipo de mensagem serve para oferecer algum tipo de produto ou serviço que não foi pedido pelo destinatário.

---

[10] CASTELA, Eduardo Marcelo. **Investigação Criminal e Informática**. Curitiba: Juruá, 2005, p. 127.

[11] Chefe do Departamento de Tecnologia da Informação e Propriedade Intelectual – Divisão Criminal do Departamento de Justiça dos Estados Unidos em palestra no Seminário realizado em 28/05/2008 no Conselho de Altos Estudos e Avaliação Tecnológica da Câmara dos Deputados. Disponível em <http://www2.camara.gov.br/a-camara/altosestudos/seminarios/crimes-programacao.html> Acesso em 08. Abr. 2012.

[12] Toda mensagem enviada para vários destinatários que não a solicitaram é considerada spam. Disponível em <http://email.uol.com.br/antispam/faq.jhtm>. Acesso em 08. abr. 2012.

[13] Disponível em: <http://www.iss.net>

Há ainda um tipo de *spam* mais grave, e além de tudo comum. É o que se denomina *pishing*[14], que consiste em uma mensagem não solicitada pelo remetente que simula uma comunicação entre alguma instituição financeira, como bancos ou empresas, além de órgãos governamentais, dentre outras instituições públicas e privadas. Tais mensagens, por serem atrativas induzem o destinatário a acessar páginas falsas que são desenvolvidas com o intuito de apropriar-se dos dados pessoais e principalmente financeiros, de quem as acessa.

O autor visa, com esse tipo de mensagem, induzir o usuário a acessar algum endereço eletrônico que consta da mensagem, e a partir dai tentar extrair dele informações pessoais e principalmente dados financeiros, sob o falso argumento de que trata-se de alguma promoção ou sorteio, ou ainda que trata-se de um recadastramento, pedindo assim os dados pessoais de quem recebe a mensagem, que inadvertidamente muitas vezes o fornece, possibilitando assim ao criminoso valiosas informações. O criminoso pode também, enviar algum programa de instalação em anexo à mensagem, onde o objetivo será o mesmo, qual seja o de persuadir o usuário a instalar o referido programa, argumentando tratar-se de uma atualização do sistema operacional, visando sempre apropriar-se dos dados pessoais e bancários do usuário. Pode ainda, a mensagem induzir o usuário a acessar determinado endereço eletrônico de alguma instituição bancária, muitas vezes aquela da qual o usuário é cliente, sendo, no entanto, um endereço falso, mais uma vez tendente a apropriar-se de dados sigilosos do usuário, para que de posse deles o autor do *pishing* possa apropriar-se de valores financeiros.

Conforme dados da *Symantec*[15], o *pishing* ocorre em maior quantidade dentre as mensagens não solicitadas que trafegam pela *internet*, ultrapassando em número as mensagens de propaganda, anúncios e pornografia.

Descreveremos as situações mais comuns da pratica de *pishing* na rede mundial de computadores:

a) O criminoso pode utilizar algum serviço de mensagens instantâneas que a vítima utiliza (ex: *Skype, Messenger)* e também o sistema de correio eletrônico, para enviar mensagens que atraia a atenção do usuário por um motivo qualquer, quase sempre lhes oferecendo uma vantagem econômica. A mensagem pode induzir o usuário a instalar algum programa que nela esteja em anexo, sob um argumento qualquer, no entanto, tal programa se

[14] A palavra *pishing* vem do inglês "*fishing"* e foi criada pelos próprios fraudadores que fizeram uma analogia, onde "iscas" (e-mails) são usadas para "pescar" senhas e dados financeiros de usuários da *internet.* SOARES. Diego de Almeida. *Spam: Legislação 2.0.* Caruaru: Asces, 2005, p. 16.

[15] AS VULNERABILIDADES dos aplicativos de desktop e o uso de técnicas de invisibilidade estão aumentando, Califórnia, 2006. Disponível em: < http://www.symantec.com/pt/br/about/news/release/article.jsp?prid=20061010_01>. Acesso em: 10. Abr. 2012.

presta a gravar os dados do usuário e repassá-los para o criminoso. A depender do caso, o programa é instalado automaticamente, sem a interferência do usuário, o que é ainda mais grave. Tais programas maliciosos, uma vez instalados, se utilizam de diversas facetas para apreender os dados financeiros e pessoais das vítimas, como por exemplo, gravar as ações do teclado e *mouse* do computador da vítima, muitas vezes inclusive criando uma janela falsa, sobreposta a verdadeira, porem idênticas, induzindo assim a vítima a inserir seus dados na janela falsa, dados esses que serão transmitidos ao criminoso autor do *pishing.* Geralmente os fraudadores utilizam-se desses dados, principalmente dos dados bancários para transações comerciais, muitas das vezes valendo-se da própria *internet.*

Os criminosos que praticam tal tipo de delito, obtêm para si valiosos informações acerca das vitimas. Conforme Diego Soares, os fraudadores poderão realizar diversas operações, incluindo a venda de dados para terceiros ou utilização dos dados financeiros para efetuar pagamentos, transferir valores para outras contas, entre outros ilícitos. [16]

È necessário que o usuário tome muito cuidado ao acessar sua caixa de mensagens, atentando para fatos como a logomarca da empresa ou órgão que enviou a mensagem, coerência textual além de erros ortográficos, evitando assim, abrir mensagens eletrônicas contendo programas maliciosos.

b) Outra modalidade de *pishing* bastante utilizada, é aquela na qual o usuário de *internet* recebe uma mensagem solicitando a confirmação ou recadastramento dos dados do usuário em alguma instituição financeira, induzindo o usuário a acessar através da mensagem, alguma imagem ou endereço eletrônico, que afinal um levará para uma outra página idêntica `a da instituição verdadeira, onde será pedido a atualização dos dados cadastrais do cliente, que mais uma vez, serão usados para subsidiar ações criminosas dos autores das mensagens, notadamente transações financeiras.

De sorte que ao usuário é de extrema importância atentar para o conteúdo de tais mensagens que são recebidas independentemente de serem solicitadas, bem como acessar a página da instituição que supostamente lhe enviou a mensagem para obter informações sobre o seu conteúdo, além de verificar se é politica da empresa o envio de tais mensagens. Além do mais, deve-se ter em mente que, por motivos de segurança, não é prática comum de instituições financeiras utilizarem-se de mensagens eletrônicas para atualizar dados cadastrais de seus clientes, uma vez que enquanto trafegam pela *internet* tais mensagens poderiam ser interceptadas, trazendo prejuízos para seus clientes.

---

[16] SOARES. Diego de Almeida. **Spam: Legislação 2.0**. Caruaru: Asces, 2005, p. 18.

c) Há ainda outro tipo de *pishing* onde o criminoso não invade um único computador e tenta extrair-lhes informações financeiras, mas sim invade um provedor de acesso à *internet,* modificando suas configurações, fazendo com que todos os usuários daquele provedor ao digitarem determinado endereço eletrônico sejam automaticamente redirecionados para uma falsa pagina, provavelmente de alguma instituição financeira, onde mais uma vez, os dados pessoais dos usuários lesados serão prontamente enviados aos criminosos.

Existe um agravante nesse tipo de *pishng,* que é o fato de o usuário não concorrer para ser vitima do engano, uma vez que, age normalmente digitando determinado endereço eletrônico que queria acessar, estando, no entanto, o provedor de acesso, por ter sido invadido por criminosos, configurado para redirecionar os usuários daquela página.

d) Para finalizar as modalidades de *pishing,* há a frequente modalidade de monitorar computadores públicos para gravar os dados financeiros daqueles usuários que inadvertidamente realizam transações financeiras em tais ambientes. Por tratarem-se de computadores públicos que são utilizadas por diversas pessoas os usuários dos mesmos podem ter suas ações monitoradas por programas específicos instalados previamente na máquina, portanto é recomendável cautela ao utilizar-se de computadores de uso público para determinados fins, como por exemplo, transações bancárias, que exigem a inserção de dados importantes que podem ser alvos de criminosos.

Fica claro então, ante o exposto que a invasão de computadores, através dos *spams e pishings* consiste em uma conduta extremamente lesiva aos usuários, pelo fato de que dentre outros motivos, criminosos podem valer-se da obtenção de dados pessoais, notadamente os bancários para apropriar-se de quantias pertencentes aos usuários vítimas destas fraudes, através de compras pela internet, transferências de valores entre instituições bancarias, entre outras transações financeiras, causando prejuízo patrimonial às vítimas. Analisando assim podemos identificar que o objetivo dos invasores nesta última modalidade é sempre obter lucro, realizando ações nos setores de comércio eletrônico e bancário.

É grande o numero de fraude pela *internet* o que levou o senador Eduardo Azeredo, em debate no seminário do Conselho de Altos Estudos e Avaliação Tecnológica da Câmara dos Deputados, a frisar:

> O volume de fraudes que acontece no sistema bancário, no dia-a-dia das relações pessoais e nas empresas é preocupante. Há crimes, como a difusão de vírus, que

> não estão previstos em nossa legislação. E não estão previstos porque são coisas novas que surgiram. [17]

Nos casos como os dos exemplos citados, em tese podemos verificar a ocorrência do crime de furto, por haver a subtração de coisa alheia móvel sem violência por parte do autor do delito, causando assim, prejuízo financeiro à vítima, podendo-se em tese aplicar o Código Penal, no entanto, ainda na há na legislação penal pátria, tipificação para a conduta de invadir-se, por exemplo, um provedor de acesso a internet e redirecionar o usuário dos mesmos para uma página falsa, de propaganda ou outros tipos de paginas, não podendo o invasor ser punido por esta conduta - salvo se utilizar os dados obtidos para furtar valores ou obter vantagem ilícita - embora ela seja de grande lesividade.

Visando preservar o sigilo de seus clientes, as instituições financeiras demonstram a vontade de refrear a obtenção de dados pessoais e bancários dos usuários seus, para que os mesmos possam ser utilizados por outras pessoas para pagamentos de contas, transferências bancárias, compras no comércio eletrônico, de forma que no já citado seminário ocorrido no Conselho de Altos Estudos e Avaliação Tecnológica da Câmara dos Deputados, o representante do Banco do Brasil Nilson Oliveira[18] esclareceu ao tempo em que advertiu que:

> [...] o Banco do Brasil considera fundamental a existência de uma legislação específica sobre isso. O que ocorre é que não pode existir aquela trilogia que constatamos diversas vezes, que é a facilidade de ataque, lucro fácil e impunidade. Esses três fatores juntos motivam muito não só o aparecimento, mas a disseminação das técnicas e a facilidade ou a vontade do pessoal realmente fazer [...].

Resumido o que fora exposto ate agora, o que ocorre é que, ao invasor restará a impunidade por ausência de legislação específica, caso o mesmo pratique a conduta de apreender os dados pessoais e bancários de clientes mediante a *internet* se de posse deles não os utilizar. De outro modo, uma vez utilizando-os será punido por crime contra o patrimônio se de posse dos referidos dados, apropriar-se de quantia da vitima, causando-lhe prejuízo patrimonial.

---

[17] Debate no Seminário realizado em 28/05/2008 no Conselho de Altos Estudos e Avaliação Tecnológica da Câmara dos Deputados. Disponível em <http://www2.camara.gov.br/a-camara/altosestudos/seminarios/crimes-programacao.html> Acesso em 10. Abr. 2012.

[18] Assessor Master da Diretoria de Gestão da Segurança do Banco do Brasil em palestra no Seminário realizado em 28/05/2008 no Conselho de Altos Estudos e Avaliação Tecnológica da Câmara dos Deputados. Disponível em <http://www2.camara.gov.br/a-camara/altosestudos/seminarios/crimes-programacao.html> Acesso em 10. Abr. 2012.

1.3 As particularidades da obtenção da prova de materialidade e indícios de autoria dos crimes cibernéticos.

A prova de materialidade do delito, bem como os indícios de autoria e materialidade trazidos pela investigação são imprescindíveis para qualquer providência judicial que se possa determinar acerca de alguma conduta criminosa. São esses os requisitos que devem ficar explícitos ao final da investigação, para que o Ministério Público ou o ofendido, a depender do caso, possam dar início à ação penal perante o judiciário.

Ocorre que é de extrema complexidade a investigação de crimes cibernéticos, uma vez que os mesmos podem não deixar resultados naturalísticos no mundo, tornando-se delitos sem rastros no mundo fático, já que os criminosos constroem e destroem seus próprios rastros. Tal complexidade se dá pela peculiaridade de como tais delitos são cometidos, qual seja, por meios eletrônicos, o que possibilita que novas formas de execuções desses tipos de crimes sejam mudadas frequentemente, dificultando assim a colheita de provas.

O primeiro passo na investigação de qualquer delito é o de constatar-se a materialidade do fato; posteriormente deve-se buscar indícios suficiente de autoria do crime já materializado. Por exemplo, deve-se constatar que determinada conta de um usuário qualquer foi acessada por outra pessoa através da internet e que dela foi feita transferência de valores para outra conta, ou realizados pagamentos, dentre outras transações financeiras, por outra pessoa não autorizada pela vítima. Nesse exemplo fica comprovada a materialidade do delito, qual seja, furto. É a partir desse momento que começa a parte mais difícil da investigação, que é a de descobrir a autoria do delito, reunindo indícios suficientes.

No mundo eletrônico os acontecimentos se dão de forma instantânea, possibilitando ao criminoso cibernético ocultar os vestígios da sua ação, ante a dinamicidade da *internet,* podendo inclusive modificá-los dificultando assim o trabalho de investigação.

Corroborando com o exposto, esclarece Eduardo Marcelo Castella:

> Não bastando as dificuldades que cercam uma investigação no mundo real, na internet, existem outros impeditivos de se chegar ao criminoso, criando a possibilidade do crime perfeito. Tal consiste na facilidade em se apagar sinais, indícios e provas, camuflando ou eliminando os rastros deixados. Bem como, ante a facilidade de se efetuar uma ação a longa distância, lançando-a bombástica de um local para atingir outra plaga a quilômetros de distância, incluindo-se, aí, outro país. Tudo isto está aliado às brechas da lei.[19]

Diante dessa dificuldade em coletar indícios de autoria dos crimes cibernéticos o Delegado Mauro Marcelo corrobora informando que a investigação num ambiente virtual é

[19] CASTELA, Eduardo Marcelo. **Investigação Criminal e Informática**. Curitiba: Juruá, 2005, p. 117.

muito dinâmica. Num clicar de mouse o acusado por apagar todas as provas e 'evidencia materialidade' de um crime[20].

O invasor, além de, no ambiente virtual, poder apagar e modificar provas pode cometer um crime de um lugar, fazendo como vítima pessoas em outro, como por exemplo, praticar o crime no Brasil lesando uma vitima em outro país, ou o inverso, de outro país lesando uma vitima em território nacional, o que obviamente dificulta a colheita de provas.

Existem ainda, aqueles que praticam a ação e deixam provas, porém as manipulam, para que jamais se possa localiza-los. Segundo Eduardo Marcelo Castela:

> O *hacker* que deseja o respeito e o reconhecimento da comunidade em que vive fará algo que deixe um sinal para que possa ser identificado como sendo ele o responsável pelo ato, mas evitará deixar vestígios que possam levar os investigadores a descobrir a sua localização[21]

São bastante propícios à pratica de crimes cibernéticos as *lan houses*[22] e os *cybercafés*[23] já que o usuário se dirige ate esses locais, usa os computadores após pagar determinada quantia, em seguida vai embora, não sendo realizada nenhum tipo de identificação do mesmo. Se o crime se deu através de um computador de uma *lan house* ou *cybercafé* a investigação torna-se ainda mais dificultosa, ficando muito difícil precisar o usuário que o cometeu. A depender do caso a investigação pode localizar o computador de onde foi realizada a conduta criminosa, no entanto isso não é suficiente, é de primordial importância saber ao certo quem foi a pessoa que cometeu o crime, o que no caso desses estabelecimentos torna-se quase sempre muito difícil por não manterem cadastro com dados de usuários.

Na Comissão Especial dos Centros de Inclusão Digital do Congresso Nacional[24] há discussão sobre a possibilidade ou não de se exigir, por meio de lei a identificação dos usuários de computadores públicos, para que os dados dos mesmos possam vir a ser usados em uma eventual investigação de crime cibernético, colocando-se contrario a essa proposta, o

---

[20] MOURA, Douro. **Crimes Virtuais no Brasil**. Disponível em: <http://www.buscalegis.ufsc.br/revistas/index.php/buscalegis/article/download/11605/11170>. Acesso em 13. Abr. 2012.

[21] CASTELA, Eduardo Marcelo. **Investigação Criminal e Informática**. Curitiba: Juruá, 2005, p. 125

[22][Ing.] Estabelecimento comercial que loca o uso de computadores para jogos virtuais de última geração. Os jogos, normalmente, de conteúdo violento, são disputados simultaneamente, em tempo real, por diversos participantes, cada qual controlando os movimentos de um personagem que confronta com outros. Esse conceito, que surgiu na Coréia em 1996, baseia-se no uso de uma rede local (LAN).

[23] Bar ou café que oferece em seu espaço computadores para acesso à *internet*.

[24]CADASTRO em lan houses deve conciliar liberdade e segurança, dizem especialistas. 2010. Disponível em < http://tecnologia.uol.com.br/ultimas-noticias/redacao/2010/05/11/cadastro-em-lan-houses-deve-conciliar-liberdade-e-seguranca-dizem-especialistas.jhtm> Acesso em 08. Abr. 2012.

professor Sérgio Amadeu, o qual esclarece que exigir a vinculação de um terminal de internet a um usuário significa o fim do anonimato, o que é quase igual à prisão de segurança máxima.[25] Discordamos do ilustre autor, vez que os dados seriam mantidos em sigilo, só sendo utilizado em caso de investigação criminal para a consecução de provas, caso este onde ninguém pode valer-se de anonimato para o cometimento de crimes.

É de nosso entendimento, que ainda que o cadastramento dos dados dos usuários de computadores públicos não possa a evitar o cometimento de crimes cibernéticos, pode sim diminuir sua incidência nos casos, por exemplo, de o criminoso não ter conseguido apagar os vestígios de sua ação, e descobrir-se de qual computador publico foi realizado o crime, e pelo cadastro descobrir quem o utilizava naquele momento.

Dentre as múltiplas possibilidades de crimes cibernéticos, há a de o infrator infectar um computador interligado à *internet* com códigos maliciosos, de modo a praticar algum crime de seu próprio computador, resultando apesar disso a identificação como sendo do computador infectado e não a do computador do infrator. O claro objetivo do invasor neste caso é o de dificultar a obtenção de provas em relação ao crime por ele praticado.

No estado de São Paulo, a lei 12.228/2006[26] com abrangência em todo o Estado disciplina a locação de máquinas para acesso à internet, obrigando os estabelecimentos que exploram tal atividade a criarem e manterem cadastro atualizado de todos os usuários, que devem ser armazenados pelo prazo de sessenta meses, sob pena de multa que varia de três a dez mil reais.

Disposição semelhante traz o estado de Santa Catarina, sob a lei 14.890/2009[27] que obriga referidos estabelecimentos a adotarem sistema de monitoramento de câmeras de vigilância, em especial nos acessos aos computadores, além de criarem e manterem pelo prazo de dois anos o cadastro de todos os usuários contendo a identificação do usuário, telefone e endereço, equipamento utilizado e horário de início e término da utilização, sob pena de sanções administrativas como advertência ou multa.

Essas leis podem ser consideradas uma tentativa de diminuir a incidência de crimes cometidos pela *internet,* apesar disso não conseguem combater o problema nem mesmo em âmbito regional. Porém a iniciativa da edição dessas leis pode abrir caminhos para

---

[25] Ibidem.

[26] SÃO PAULO. Lei 12.228, de 11 de janeiro de 2006. Dispõe sobre os estabelecimentos comerciais que colocam à disposição, mediante locação, computadores e máquinas para acesso à internet e dá outras providências. **Diário Oficial do Estado de São Paulo**, São Paulo, 12 Jan. 2006.

[27] SANTA CATARINA. Lei 14.890, de 22 de outubro de 2009. Disciplina o controle de usuários em estabelecimentos voltados a comercialização do acesso a internet no Estado de Santa Catarina. **Diário Oficial do Estado de Santa Catarina**, Florianópolis, 22 out. 2009.

uma discussão mais ampla, no sentido da elaboração de uma legislação que seja harmônica entre a liberdade de acesso, sigilo do mesmo, e a punição eficaz dos infratores.

Além de uma legislação eficaz, é necessário o uso da tecnologia moderna, como a usam os infratores, como bem elucida Eduardo Marcelo Castela: o Estado deverá produzir o contra-ataque necessário, utilizando as mesmas armas para o cometimento dos ilícitos, ou seja, tecnologia.[28]

[28] CASTELA, Eduardo Marcelo. **Investigação Criminal e Informática**. Curitiba: Juruá, 2005, p. 116.

CAPÍTULO II
A LACUNA LEGAL

2.1 **Aplicação do Código Penal e leis especiais em alguns casos e a ausência de previsão legal para a tipificação de determinadas condutas.**

A Constituição Federal em seu art. 5º, inc. XXXIX traz o princípio da legalidade ao prever que não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal. Da mesma forma, o código penal em seu artigo 1º disciplina que não há crime sem lei anterior que o defina. Não há pena sem prévia cominação legal.

Sendo assim, fica claro que o princípio da legalidade é um dos mais importantes do direito penal, já que garante ao cidadão não será vítima de abusos pelo poder público, garantindo-lhe não ter seu direito de liberdade restringido de forma sumária e irresponsável.

Interpretando-se o princípio da legalidade, observamos que no direito penal pátrio as condutas que especificam crimes devem estar descritas taxativamente na lei penal, atribuindo-se a pratica dessas condutas a cominação de uma pena.

Como preleciona Rogério Grecco:

> A lei é a única fonte do direito penal quando se quer proibir ou impor condutas sob a ameaça de sanção. Tudo o que não for expressamente proibido é licito em Direito Penal. Por essa razão, Von Liszt dizia que o Código Penal era a Carta Magna do delinquente.[29]

Depreende-se ainda do princípio da legalidade o princípio da reserva legal, ou seja, a tipificação de condutas criminosas e a imposição de penas para a prática de tais condutas é afeta tão somente à lei, não podendo haver a criação de crime que não seja por meio de lei.

Na lição de Paulo de Souza Queiroz:

> O princípio da reserva legal implica a máxima determinação e taxatividade dos tipos penais, impondo-se ao Poder Legislativo, na elaboração das leis, que redija tipos penais com a máxima precisão de seus elementos, bem como ao Judiciário que as interprete restritivamente, de modo a preservar a efetividade do princípio.[30]

O principio da legalidade tem ainda a função de proibir a retroatividade da lei penal, o que se denomina de "irretroatividade da lei penal", disciplinada no artigo 5º, inc. XL

---

[29] GRECO, Rogério. **Curso de Direito Penal**. 12ª Ed. Rio de Janeiro: Impetus, 2010, p. 105.
[30] QUEIROZ, Paulo de Souza *apud* GRECO, Rogério. **Curso de Direito Penal**. *12*ª Ed. Rio de Janeiro: Impetus, 2010, p. 108.

da Constituição Federal ao dispor que: a lei penal não retroagirá, salvo para beneficiar o réu. Desse modo, é necessário que além da obrigatoriedade da conduta estar prevista em lei, que essa lei seja anterior ao fato praticado, já que a lei penal não retroage, única exceção se dá no caso da lei penal passar a beneficiar o autor da prática de determinado fato, de forma que só nessa hipótese a lei penal retroagirá no sentido de ser aplicada ao fato anterior a sua existência, pois terá o condão de beneficiar.

Esclarecendo tal questão, colacionamos a lição de Rogério Greco:

> O inciso XL do art. 5º da Constituição Federal, em reforço ao princípio da legalidade previsto no inciso XXXIX, diz que "a lei penal não retroagirá, salvo para beneficiar o agente". A regra constitucional, portanto, é a da irretroatividade da lei penal; a exceção é a retroatividade, desde que seja para beneficiar o agente. Com essa vertente do princípio da legalidade tem-se a certeza de que ninguém será punido por um fato que, ao tempo da ação ou da omissão, era tido como um indiferente penal, haja vista a inexistência de qualquer lei penal incriminando-o (*nullum crimen nulla poena sine lege praevia)*.[31]

Em relação ao objeto do nosso estudo, que são as condutas lesivas e criminosas praticadas por meio da informática (e da *internet*), verificamos que o Código Penal e a legislação penal extravagante são silentes em relação a tais condutas, de modo que a maioria delas, a exemplo da disseminação de programas maliciosos que capturam dados pessoais e bancários dos usuários e os remetem aos criminosos, as invasões em sistemas de informações de governos ou empresas no intuito de torná-los lentos, travá-los ou torná-los indisponíveis, não são dispostas em lei como proibidas e não possuem cominação de pena. Aplicando-se o principio da legalidade quando do cometimento dessas condutas, podemos dizer que elas apesar de serem lesivas aos usuários e administradores dos sistemas invadidos, não podem ser combatidas pelo fato de não serem expressamente proibidas pelo ordenamento jurídico penal pátrio.

Acontece que referidas condutas são muito lesivas aos usuários de sistemas de informática deviam portanto, ser tipificadas, tendo sua pratica proibida pela lei penal, bem como possuir a cominação de pena para o autor que a praticasse. Infelizmente, o Brasil não possui legislação específica para combater os delitos cibernéticos.

De outra sorte, caso o invasor apreenda os dados pessoas e bancários de determinada vítimas, e com esses dados acessar sua conta bancária e lhe subtrair dinheiro, seja transferindo valores, pagando contas, dentre outras condutas, estará cometendo crime contra o patrimônio da mesma, havendo no caso a possibilidade de aplicação do Código

[31] GRECO, Rogério. **Curso de Direito Penal**.12ª Ed. Rio de Janeiro: Impetus, 2010, p. 107.

Penal. No caso exposto, tal crime fora cometido pela *internet,* mas poderia ter sido cometido por qualquer meio alheio à mesma, sendo punido do mesmo modo que outros tipos penais contra o patrimônio, já que o Código Penal não diferencia a circunstancia de o crime ter sido cometido através ou não da *internet,* e após a obtenção dos dados por meio da rede mundial de computadores de forma censurável, o que é uma lacuna na legislação penal.

Para ilustrar o que acima fora exposto, insta colacionar jurisprudência do Superior Tribunal de Justiça, para viabilizar a possibilidade de aplicação do Código Penal, no que couber, às condutas lesivas praticadas por meio da *internet:*

> CRIMINAL. HC. FURTO QUALIFICADO. FRAUDES POR MEIO DA INTERNET. PROGRAMA TROJAN. OPERAÇÃO CONTROL ALT DEL. PRISÃO PREVENTIVA. POSSIBILIDADE CONCRETA DE REITERAÇÃO CRIMINOSA. NECESSIDADE DA CUSTÓDIA DEMONSTRADA. PRESENÇA DOS REQUISITOS AUTORIZADORES. ORDEM DENEGADA. Hipótese na qual o paciente **foi denunciado pela suposta prática do crime de furto qualificado, pois seria integrante de grupo organizado com o fim de praticar fraudes por meio da Internet, concernentes na subtração de valores de contas bancárias, em detrimento de diversas vítimas e instituições financeiras, entre elas a Caixa Econômica Federal, a partir da utilização de programa de computador denominado TROJAN**. Não há ilegalidade na decretação da custódia cautelar do paciente, tampouco no acórdão confirmatório da segregação, pois a fundamentação encontra amparo nos termos do art. 312 do Código de Processo Penal e na jurisprudência dominante. As peculiaridades concretas das práticas supostamente criminosas revelam que a liberdade do réu poderia ensejar, facilmente, a reiteração da atividade delitiva, indicando a necessidade de manutenção da custódia cautelar. **As eventuais fraudes podem ser perpetradas na privacidade da residência, do escritórios ou, sem muita dificuldade, em qualquer lugar em que se possa ter acesso à rede mundial de computadores**. A real possibilidade de reiteração criminosa, constatada pelas evidências concretas do caso em tela, é suficiente para fundamentar a segregação do paciente para garantia da ordem pública. Ordem denegada. (STJ – Habeas Corpus nº 2007/0087811-8 (HC81638 / PA), Quinta Turma, Relator Ministro Gilson Dipp, 12/06/2007)

> EMBARGOS DECLARATÓRIOS EM CONFLITO NEGATIVO DE COMPETÊNCIA. SUBTRAÇÃO MEDIANTE TRANSFERÊNCIA IRREGULAR DE VALORES DEPOSITADOS EM CONTA BANCÁRIA. FRAUDE VIA INTERNET. FURTO QUALIFICADO. CONSUMAÇÃO. SUBTRAÇÃO DO NUMERÁRIO. CONTA-CORRENTE DE ORIGEM. INEXISTÊNCIA DE CONTRADIÇÃO, MAS ENTENDIMENTO DIVERSO DO EMBARGANTE QUANTO AO LOCAL DO PREJUÍZO E DA CONSUMAÇÃO DO DELITO. EMBARGOS REJEITADOS. 1. No crime de furto, a infração consuma-se no local onde ocorre a retirada do bem da esfera de disponibilidade da vítima, isto é, no momento em que ocorre o prejuízo advindo da ação criminosa; **nas hipóteses de fraude eletrônica para subtração de valores, o desapossamento da res furtiva se dá de forma instantânea, já que o dinheiro é imediatamente tirado da esfera de disponibilidade do correntista**. Logo, a competência para processar e julgar o delito em questão é o do lugar de onde o dinheiro foi retirado, em obediência a norma do art. 70 do CPP. Precedentes da 3a. Seção deste STJ. 2. É desinfluente, para alterar esse raciocínio, que se considere a própria CEF ou o correntista como vítima, pois ambos foram lesados no instante da fraude; todavia, essa fraude não ocorreu na localidade onde retirado o dinheiro,

> mas naquela em que se constatou a perda da posse. A retirada do dinheiro, em outra localidade, é mero exaurimento do crime. 3. Não há contradição no acórdão embargado, mas entendimento diverso quanto ao local do desapossamento dos valores e do prejuízo suportado pela CEF, que o embargante entende que ocorreu com a retirada do valor subtraído da conta da agência de destino. 4. Embargos rejeitados. (STJ, Embargos de Declaração no Conflito de Competência nº 2007/0141978-0 (EDcl no CC 86913 / PR), Terceira Seção, Relator Ministro Napoleão Nunes Maia Filho), 08/10/2008)

Apesar das lacunas, há na legislação penal brasileira, crimes tipificados e que também possuem reprimenda quando são praticados em sistemas de informática ou por meio da *internet.*

Por crimes próprios de informática, citamos os crimes previstos no artigos 313-A e 313-B do Código Penal, que dispõem da seguinte maneira:

> Art. 313-A. Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano:
> Pena – reclusão, de 2 (dois) a 12 (doze) anos, e multa.

> Art. 313-B. Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente:
> Pena – detenção, de 3 (três) meses a 2 (dois) anos, e multa.
> Parágrafo único. As penas são aumentadas de um terço até a metade se da modificação ou alteração resulta dano para a Administração Pública ou para o administrado.[32]

Os mencionados crimes são próprios em relação ao sujeito ativo, já que apenas podem ser cometidos por funcionários públicos.

Outro exemplo de tipificação de crimes cometidos por meio da *internet* e tipificados na legislação pátria é o artigo 241-A do Estatuto da Criança e do Adolescente, incluído pela lei 11.829/2008 e que tipifica como crime a pornografia infantil praticada por meio de sistema de informática ou telemática, punindo o infrator com pena de reclusão de três a seis anos, e multa. Mencionado tipo penal prevê ainda a punição da pessoa que oferece o serviço de armazenamento de cenas ou imagens pornográficas envolvendo criança ou adolescente, bem como a pessoa que oferece o serviço de acesso à internet para a prática da conduta criminosa, assim dispondo:

> Art. 241-A. Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito

[32] BRASIL. Decreto-Lei 2.848/40 de 07 de dezembro de 1940. Código Penal. **Diário Oficial da União**, Brasília, 31 dez. 1940.

> ou pornográfica envolvendo criança ou adolescente: Pena – reclusão, de 3 (três) a 6 (seis) anos, e multa.
> § 1º Nas mesmas penas incorre quem:
> I – assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens de que trata o caput deste artigo;
> II – assegura, por qualquer meio, o acesso por rede de computadores às fotografias, cenas ou imagens de que trata o caput deste artigo.
> § 2º As condutas tipificadas nos incisos I e II do § 1º deste artigo são puníveis quando o responsável legal pela prestação do serviço, oficialmente notificado, deixa de desabilitar o acesso ao conteúdo ilícito de que trata o caput deste artigo.[33]

Apesar de referido dispositivo legal ser incluído no Estatuto da Criança e do Adolescente, apenas no ano de 2008, já havia o crime cuja conduta em tela era praticada ainda que não por meio da *internet,* tipificado no artigo 241, no entanto, o Supremo Tribunal Federal já mantinha entendimento acerca da possibilidade do agente que cometesse o crime com o auxilio da rede mundial de computadores, conforme jurisprudência:

> EMENTA: PROCESSO PENAL. COMPETÊNCIA. CRIME TIPIFICADO NO ESTATUTO DA CRIANÇA E DO ADOLESCENTE. CONSUMAÇÃO E EXAURIMENTO NO EXTERIOR. COMPETÊNCIA DA JUSTIÇA FEDERAL. I - Compete à Justiça Federal processar e julgar os crimes cuja consumação se deu em território estrangeiro (art. 109, V, CF). II - O crime tipificado no art. 241 do Estatuto da Criança e do Adolescente, consubstanciado na divulgação ou publicação, pela internet, de fotografias pornográficas ou de cenas de sexo explícito envolvendo crianças ou adolescentes, cujo acesso se deu além das fronteiras nacionais, atrai a competência da Justiça Federal para o seu processamento e julgamento. III - Ordem denegada. (STF, Habeas Corpus nº 86289 /GO – Goiás, Primeira Turma, Relator Min. Ricardo Lewandowski, 06/06/2006)

A inclusão do artigo 241 - A no Estatuto da Criança e do Adolescente foi fruto de pressão social, em virtude da grande quantidade de casos de pornografia infantis perpetradas por meio da *internet.* Somente no primeiro trimestre de 2010, segundo dados da organização Safernet[34], as denúncias relativas à pornografia infantil somaram 44% do total de denúncias recebidas para outros crimes praticados através da *internet.*

Outra conduta amplamente praticada através da rede mundial de computadores é a pirataria, que pode ser definida como a utilização ou fornecimento não autorizado de conteúdos protegidos por direitos autorais, tais como livros eletrônicos, músicas, vídeos e programas de computador, seja com o desígnio de lucro ou não. Essa conduta encontra-se tipificada no artigo 184 do Código Penal que assim dispõe:

---

[33] BRASIL. Lei 8.069/1990 de 13 de julho de 1990. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. **Diário Oficial da União**, Brasília, 27 set. 1990.
[34] CENTRAL Nacional de Denúncias, 2010. Disponível em: <http://www.safernet.org.br/site/indicadores>. Acesso em 27. out. 2010

> Art. 184. Violar direitos de autor e os que lhe são conexos:
> Pena – detenção, de 3 (três) meses a 1 (um) ano, ou multa.
> § 1º Se a violação consistir em reprodução total ou parcial, com intuito de lucro direto ou indireto, por qualquer meio ou processo, de obra intelectual, interpretação, execução ou fonograma, sem autorização expressa do autor, do artista intérprete ou executante, do produtor, conforme o caso, ou de quem os represente:
> Pena – reclusão, de 2 (dois) a 4 (quatro) anos, e multa.
> § 2º Na mesma pena do § 1º incorre quem, com o intuito de lucro direto ou indireto, distribui, vende, expõe à venda, aluga, introduz no País, adquire, oculta, tem em depósito, original ou cópia de obra intelectual ou fonograma reproduzido com violação do direito de autor, do direito de artista intérprete ou executante ou do direito do produtor de fonograma, ou, ainda, aluga original ou cópia de obra intelectual ou fonograma, sem a expressa autorização dos titulares dos direitos ou de quem os represente.
> **§ 3º Se a violação consistir no oferecimento ao público, mediante cabo, fibra ótica, satélite, ondas ou qualquer outro sistema que permita ao usuário realizar a seleção da obra ou produção para recebê-la em um tempo e lugar previamente determinados por quem formula a demanda, com intuito de lucro, direto ou indireto, sem autorização expressa, conforme o caso, do autor, do artista intérprete ou executante, do produtor de fonograma, ou de quem os represente:**
> **Pena – reclusão, de 2 (dois) a 4 (quatro) anos, e multa *(grifo nosso)***
> § 4º O disposto nos §§ 1º, 2º e 3º não se aplica quando se tratar de exceção ou limitação ao direito de autor ou os que lhe são conexos, em conformidade com o previsto na Lei nº 9.610, de 19 de fevereiro de 1998, nem a cópia de obra intelectual ou fonograma, em um só exemplar, para uso privado do copista, sem intuito de lucro direto ou indireto.[35]

O oferecimento ao público de obras com violação de direitos autorais por meio da *internet* enquadra-se no § 3º do artigo 184. Insta salientar que no § 3º é tipificada apenas a conduta de oferecer a obra e não a de adquirir, não podendo o adquirente da obra ser punido por tal conduta. De outro modo, o próprio § 4º trata da inaplicabilidade do disposto nos §§ 1º, 2º e 3º do artigo 184 quando a conduta consistir na cópia de obra intelectual ou fonograma em um só exemplar e se destinar ao uso privado do copista, sem desígnio de qualquer tipo de lucro.

Diante de todo o exposto, fica demonstrada a lacuna legislativa no que se refere a tipificação de condutas lesivas praticadas através da *internet,* condutas essas que são velozes e dinâmicas e que atualmente são combatidas utilizando-se a legislação penal vigente quando acaso uma conduta se subsume a descrição típica. A nosso ver é de salutar importância que as condutas perpetradas através da rede mundial de computadores, que sejam lesivas e reprováveis pela sociedade tenham tipificação penal própria, além de modificações no Código Penal, para que haja ao menos a pena diferenciada nos crimes cometidos pela *internet,* a

[35] BRASIL. Decreto-Lei 2.848/40 de 07 de dezembro de 1940. Código Penal. **Diário Oficial da União**, Brasília, 31 dez. 1940.

exemplo do furto realizado com a obtenção dos dados pessoais e bancários pelo invasor e a posterior subtração de valores da conta bancária da vítima.

2.2 **Possibilidade de aplicação da lei 9.296/96 para a obtenção de provas nos crimes cibernéticos**

Tal como deve haver a descrição da conduta criminosa na lei penal, para que seu infrator possa ser punido, o processo penal necessita em seu decorrer da colheita de provas que demonstrem a materialidade e autoria delitiva, bem como a motivação do crime, e para tanto, são necessários provas, que nada mais são que elementos para que o julgador possa fazer um juízo de valor acerca da conduta criminosa, aplicando-se assim uma decisão justa.

Sendo assim, fica claro que as provas são de extrema importância para o processo penal, não se admitindo portanto provas obtidas por meios ilícitos, para que não se pratique injustiças, pois no processo penal uma injustiça pode cercear a liberdade de um inocente, ou assegurar a liberdade a um criminoso.

O artigo 157 do Código de Processo Penal assim dispõe:

> Art. 157. São inadmissíveis, devendo ser desentranhadas do processo, as provas ilícitas, assim entendidas as obtidas em violação a normas constitucionais ou legais.
> § 1º São também inadmissíveis as provas derivadas das ilícitas, salvo quando não evidenciado o nexo de causalidade entre umas e outras, ou quando as derivadas puderem ser obtidas por uma fonte independente das primeiras.[36]

Seguindo o raciocínio do Código de Processo Penal, Frederico Marques arremata afirmando que de um modo geral são inadmissíveis os meios de prova que a lei proíba e aqueles que são incompatíveis com o sistema processual penal em vigor.[37]

A legislação processual penal brasileira explicita no Código de Processo Penal as provas cuja utilização é mais frequente.

Nesse sentido, Edilson Mougenot Bonfim, esclarece que o rol de meios de prova é aberto e que na busca da verdade real, podendo as partes optar por meios de prova não especificados em lei.[38]

---

[36] BRASIL. Decreto-Lei 2.848/40 de 07 de dezembro de 1940. Código Penal. **Diário Oficial da União**, Brasília, 31 dez. 1940.
[37] MARQUES, Frederico *apud* LIMA, Marcellus Polastri. **Manual de Processo Penal**. 2 ed. Rio de Janeiro. Editora Lumen Juris. 2009, p. 339.
[38] BONFIM, Edilson Mongenout. **Curso de Processo Penal**. 2 ed. São Paulo. Editora Saraiva. 2007, p. 296

È necessária tal introdução para que possamos compreender a colheita de provas nos crimes cibernéticos, pois assim como não há tipificação penal para algumas condutas cometidas pela *internet,* não há na legislação processual penal disciplinamento sobre a colheita de provas nos delitos cibernéticos.

Sendo assim, as provas nos crimes cometidos por meios eletrônicos, devem ser colhidas respeitando-se os dispositivos constitucionais e legais, sobre penas de serem declaradas ilegais.

A Constituição Federal em seu artigo 5º, inciso XII assim dispõe:

> XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal[39]

Diante do texto constitucional, fica verificada a possibilidade de interceptação das comunicações telefônicas, sendo o texto silente no que se refere à interceptação de da de dados de informática, pois não há a exceção à interceptação de dados no texto magno.

A lei 9.296/96, visando suprir essa lacuna, foi introduzida no ordenamento jurídico com o sentido de regulamentar o inciso XII do artigo 5ª da Constituição Federal, trazendo no bojo de seu texto a possibilidade da interceptação do fluxo de comunicações em sistemas de informática e telemática, assim dispondo:

> Art. 1º A interceptação de comunicações telefônicas, de qualquer natureza, para prova em investigação criminal e em instrução processual penal, observará o disposto nesta Lei e dependerá de ordem do juiz competente da ação principal, sob segredo de justiça.
> Parágrafo único. O disposto nesta Lei aplica-se à interceptação do fluxo de comunicações em sistemas de informática e telemática.[40]

A partir de então a legislação penal ordinária passou a prever a possibilidade de interceptação nos sistemas de informática de telemática, mediante autorização judicial, possibilitando ao investigador a colheita de provas em meios informáticos.

Ocorre que a referida lei 9.296/96 impôs limitações à interceptação nela prevista, disciplinando em seu parágrafo 2º as hipóteses em que a interceptação pode ocorrer, dispondo da seguinte maneira:

---

[39] BRASIL. Constituição Federal da República Federativa do Brasil de 1988. **Diário Oficial da União**, Brasília, 05 out. 1988.
[40] BRASIL, Lei 9.296 de 24 de julho de 1996. Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal. **Diário Oficial da União**, Brasília, 25 jul. 1996.

> Art. 2° Não será admitida a interceptação de comunicações telefônicas quando ocorrer qualquer das seguintes hipóteses:
> I - não houver indícios razoáveis da autoria ou participação em infração penal;
> II - a prova puder ser feita por outros meios disponíveis;
> III - o fato investigado constituir infração penal punida, no máximo, com pena de detenção.[41]

Sendo assim, não há a possibilidade de concessão de autorização judicial para interceptação de comunicações em sistemas de informática e telemática quando o crime praticado por meio da *internet* seja punido com pena de detenção.

Sendo assim, surge a dúvida de como ocorreria uma investigação nos casos dos crimes de injúria, calúnia e difamação, praticados por meio da *internet,* já que os mesmos são punidos com detenção apenas[42].

È necessário que se verifique quando o caso estará protegido pelo sigilo do inciso XII do art. 5º da Constituição Federal, necessitando-se de autorização judicial nos termos da lei 9.296/96 para interceptá-las, e quando será um caso onde as informações não estejam protegidas pelo sigilo, hipótese em que não há necessidade de aplicação da lei 9.296/96.

No caso dos crimes de injúria, calúnia e difamação, em sua grande maioria, quando cometidos pela *internet,* são praticados em salas de bate papo, locais a que qualquer pessoa tem acesso, e também em páginas de relacionamento ou redes sociais, locais onde as informações são disponibilizadas na *internet* pelo próprio usuário das mesmas, não podendo-se por tanto admitir que tais informações sejam protegidas pelo sigilo constitucional e, embora os crimes sejam punidos com a pena de detenção, há a possibilidade de autorização judicial para que a empresa fornecedora do serviço de *internet* conceda as informações necessárias a elucidação do fato delituoso, vez que muitos dos crimes cibernéticos são cometidos por usuários que fornecem informações falsas nas já referidas redes sociais e que só com a disponibilização dos dados de acesso reais - dos quais as empresas prestadoras do serviço possuem - é que se pode concluir pela autoria do delito.

Nesse sentido, o STJ já se manifestou da seguinte maneira:

> RECURSO EM HABEAS CORPUS. PENAL. ART. 241. INTERNET. SALA DE BATE PAPO. SIGILO DAS COMUNICAÇÕES. INVIABILIDADE.

[41] BRASIL, Lei 9.296 de 24 de julho de 1996. Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal. **Diário Oficial da União**, Brasília, 25 jul. 1996.

[42] à exceção da injúria praticada com elementos referentes a raça, cor, etnia, religião, origem ou a condição de pessoa idosa ou portadora de deficiência, pois tal modalidade de injúria é punida com pena de reclusão, conforme § 3º do artigo 140 do Código Penal.

> TRANCAMENTO DO INQUÉRITO POLICIAL. NECESSIDADE DE EXAME APROFUNDADO DO CONJUNTO PROBATÓRIO. INADEQUAÇÃO DA VIA ELEITA.
> 1. A conversa realizada em "sala de bate papo" da internet, não está amparada pelo sigilo das comunicações, pois o ambiente virtual é de acesso irrestrito e destinado a conversas informais. 2. O trancamento do inquérito policial em sede de recurso em habeas corpus é medida excepcional, somente admitida quando constatada, prima facie, a atipicidade da conduta ou a negativa de autoria. 3. Recurso que se nega provimento, com a recomendação de que o juízo monocrático determine a realização imediata da perícia requerida pelo parquet nos autos, sob pena de trancamento da ação penal. (STJ. RHC 18116 / SP Relator Ministro HÉLIO QUAGLIA BARBOSA, sexta turma, julgado em 16/02/2006)

Tal possibilidade se sustenta ainda, porque nos casos de crimes contra a honra, que são cometidos pelo *internet*, os autores omitem sua real identidade, e o objetivo da invasão ao sigilo é o de descobrir o real autor do fato com fundamento no artigo 5º da Constituição Federal, inciso IV, última parte, que veda o anonimato.

2.2.1 A Inconstitucionalidade da interceptação do fluxo de comunicações em sistemas de informática e telemática

Questão bastante debatida na doutrina é o fato de o parágrafo único do artigo 1º da lei 9.296/096 ser ou não inconstitucional, pois como já relatado, a Constituição Federal prevê a inviolabilidade do sigilo das correspondências e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial. Acontece que a lei 9.296/96 como já demonstrado trouxe em seu bojo a possibilidade de interceptação do fluxo de comunicações em sistema de informática e telemática, o que suscita a discussão sobre a inconstitucionalidade de tal dispositivo.

Para esclarecer essa questão é necessário interpretar-se o dispositivo constitucional de modo a refletir a vontade do legislador constituinte originário. Na leitura do texto constitucional, observamos que ele escreve da seguinte maneira: “é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial”.

Ocorre que resta dúvida se a expressão “no último caso” estaria se referindo apenas as comunicações telefônicas, ou se é mais abrangente e faz referencia às comunicações de dados e das comunicações telefônicas e comunicações telegráficas. Observe que em todos os casos não há dúvida em relação ao sigilo da correspondência.

Variadas são as opiniões emitidas pela doutrina, de modo que para Vicente Greco Filho o texto da lei 9.296/96 é inconstitucional, sustentando que a expressão “ultimo caso”

refere-se unicamente as comunicações telefônicas, sendo invioláveis o sigilo de correspondência e quaisquer outros tipos de comunicação que não a comunicação telefônica, discursando da seguinte maneira:

> Se a constituição quisesse dar a entender que as situações são apenas duas, e quisesse que a interceptação fosse possível nas comunicações telegráficas, de dados e das comunicações telefônicas, a ressalva estaria redigida não como "no ultimo caso", mas como "no segundo caso". Ademais, segundo os dicionários, último significa o derradeiro, o que encerra, e não, usualmente, o segundo.
> (...)
> Daí decorre que, em nosso entendimento, é inconstitucional o parágrafo único do art. 1º da lei comentada, porque não poderia estender a possibilidade de interceptação do fluxo de comunicações em sistemas de informática e telemática.[43]

Por outro lado, Paulo Rangel defende que a expressão "último caso" se refere às comunicações de dados e telefônicas, dessa forma, apenas o sigilo das correspondências e de comunicações telegráficas são invioláveis, sendo, portanto constitucional o texto da lei 9.296/96 assim esclarecendo:

> Pensamos, sem maiores delongas hermenêuticas, que o dispositivo constitucional está dividido em dois grupos, a saber: 1º grupo: sigilo da correspondência e das comunicações telegráficas; 2º grupo: de dados e das comunicações telefônicas. Assim, a expressão "último caso" açambarcaria dados e comunicações telefônicas, pois do contrário, o legislador deveria ter dito: "sigilo das correspondências, das comunicações telegráficas, de dados e das comunicações telefônicas onde a expressão "último caso" teria como ponto de apoio somente a expressão isolada pela disjuntiva e. Porém, não foi esta a opção do legislador constituinte. Quis e permitiu a quebra do sigilo de dados sejam das comunicações telefônicas sejam outros dados de comunicação.[44]

Acontece que ainda que o legislador tenha se referido apenas a hipótese de violação do sigilo das comunicações telefônicas mediante autorização judicial, os dados dos sistemas de informática e telemática trafegam, no mais das vezes pela estrutura física telefônica mantida pelas operadoras de telefonia, como bem explica Marcellus Polastri Lima ao afirmar: "Portanto, em se tratando de comunicação via Internet, a regra é que o sistema funcione através de linha telefônica, admitindo-se, a nosso ver, a interceptação de tal comunicação, desde que previamente autorizada judicialmente, na forma da lei".[45]

---

[43] GRECO FILHO, Vicente. **Interceptação telefônica: (considerações sobre a lei 9.296/96, de 24 de julho de 1996)**. 2. Ed. São Paulo: Saraiva, 2006, p.16.

[44] RANGEL, Paulo. **Breves considerações sobre a Lei 9296/96 (interceptação telefônica)**. Disponível em: <http://jus.uol.com.br/revista/texto/195/breves-consideracoes-sobre-a-lei-9296-96-interceptacao-telefonica/1>.Acesso em 04. Abr. 2012.

[45] LIMA, Marcellus Polastri. **Manual de Processo Penal**. 2 ed. Rio de Janeiro. Editora Lumen Juris. 2009, p. 374

A tese de que o sigilo das comunicações dos sistemas de informática e telemática podem ser violados por serem realizados por meio de comunicação é telefônica é tão palpável que o próprio STJ ao se referir à obtenção de provas nos crimes praticados por meio da internet, utiliza a expressão "interceptações telefônicas", senão vejamos:

> HABEAS CORPUS – FURTO EM CONTINUIDADE DELITIVA – OPERAÇÃO TROJAN - OBTENÇÃO DAS SENHAS DOS DEPOSITANTES EM CONTAS BANCÁRIAS- PROVA QUE
> PODE SER OBTIDA POR MEIOS DIVERSOS DA PERÍCIA NOS COMPUTADORES – AUSÊNCIA DE PREJUÍZO. ORDEM DENEGADA.
> 1- **Os crimes praticados pela internet podem ser comprovados por muitos meios de provas, como interceptações telefônicas**, testemunhas e outros e até por documento juntado aos autos, não constituindo a prova pericial nos computadores, difícil de ser realizada, o único meio de prova, não havendo ofensa ao artigo 158 do Código de Processo Penal. 2- Sem demonstração de prejuízo não se pode reconhecer qualquer nulidade. 3- Ordem denegada. (STJ, HC 92232 / RJ, Relatora Ministra Jane Silva (Desembargadora Convocada do TJ)MG), quinta turma, julgado em 08/11/2007).

O nosso entendimento é pela constitucionalidade do dispositivo constante do paragrafo único do artigo 1º da lei 9296/96, já que ainda que o constituinte possibilite a violação do sigilo das comunicações telefônicas, entendemos que as comunicações nos sistemas de informática e telemática são realizadas pelo mesmo modo, qual seja comunicação telefônica, sem falar na lição do constitucionalista Alexandre de Moraes, que esclarece que nada impede que nas outras espécies de inviolabilidade haja possibilidade de relativização da norma constitucional, devendo ser dada a norma constitucional a interpretação que lhe garanta maior eficácia.[46]

Se esse não fosse o entendimento, diríamos que seria impossível na maioria dos casos investigar-se os autores de crimes pela *internet,* instalando-se a plena sensação de impunidade para esta modalidade criminosa.

[46] MORAES, Alexandre *apud* FONSECA, Tiago Abud. **Interceptação Telefônica – A devassa em nome da lei**. Rio de Janeiro: Espaço Jurídico, 2008, p.72.

CAPÍTULO III
OS ESFORÇOS PARA TENTAR SUPRIR A LACUNA LEGISLATIVA

Notamos que algumas condutas praticadas em meios cibernéticos, apesar de lesar usuários e os próprios sistemas informáticos não são tipificadas na legislação penal pátria, impossibilitando a punição de quem as comete. São exemplos das mesmas: a elaboração e disseminação pela rede mundial de computadores; a interferência em sistema de informática; o ato de um invasor apagar um arquivo armazenado, dentre outras.

Neste capitulo abordaremos a Convenção sobre o Cibercrime e também o projeto de lei nº 84/1999 em tramitação no Congresso Nacional e que tem a intenção de tipificar crimes cometidos na área de informática.

3.1 A Convenção Sobre o Cibercrime

A Convenção sobre o Cibercrime foi elaborada através de deliberação dos Estados membros do Conselho da Europa, na cidade de Budapeste, em 23 de novembro de 2001, e é um documento internacional que demonstra a preocupação mundial em relação ao crescimento dos crimes e condutas danosas praticadas em âmbito virtual.

Em seu preambulo, justifica a necessidade de criação de uma politica criminal comum, visando proteger a sociedade dos crimes cibernéticos, uma vez que o uma vez que hoje, boa parte da população mundial, utiliza-se dos serviços de sistemas de informática.

A Convenção traz diretrizes de cooperação internacional na punição e investigação dos crimes praticados através da informática estabelecendo regras de acordo mutuo entre os signatários, além de estabelecer parâmetros para que cada pais signatário possa estabelecer medidas legislativas eficientes para tipificar as condutas lesivas mais comuns praticadas em meios cibernéticos.

É relevante frisar que a convenção sobre o Cibercrime, apesar de elaborada pela União Europeia está aberta à assinatura dos demais países, não tendo até o presente momento porém aderido à ela o Brasil, o que seria uma forma do Brasil aderir a um combate no plano intrernacional.

A Convenção sobre o Cibercrime, em seus artigos 2º, 3º, 4º e 5º, apresenta diretrizes para que os países signatários possam editar leis a respeito da punição de condutas

danosas cometidas em ambientes virtuais, quais sejam, o simples acesso ilegítimo a sistemas de informação, a interceptação ilegítima de dados transmitidos, a invasão de computadores para alteração de dados ou para provocar falhas em sistemas, assim dispondo:

> **Artigo 2º - Acesso ilegítimo**
> Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracção penal, no seu direito interno, o
> acesso intencional e ilegítimo à totalidade ou a parte de um sistema informático. As Partes podem exigir que a infracção seja cometida com a violação de medidas de segurança, com a intenção de obter dados informáticos ou outra intenção ilegítima, ou que seja relacionada com um sistema informático conectado a outro sistema informático.
> **Artigo 3º - Intercepção ilegítima**
> Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracção penal, no seu direito interno, a
> intercepção intencional e ilegítima de dados informáticos, efectuada por meios técnicos, em transmissões não públicas, para, de ou dentro de um sistema informático, incluindo emissões electromagnéticas provenientes de um sistema informático que veicule esses dados. As Partes podem exigir que a infracção seja com tida com dolo ou que seja relacionada com um sistema informático conectado com outro sistema informático.
> **Artigo 4º - Interferência em dados**
> 1. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracção penal, no seu direito interno, o acto de intencional e ilegitimamente danificar, apagar, deteriorar, alterar ou eliminar dados informáticos. 2. Uma Parte pode reservar-se o direito de exigir que a conduta descrita no n.º 1 provoque danos graves.
> **Artigo 5º - Interferência em sistemas**
> Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracção penal, no seu direito interno, a obstrução grave, intencional e ilegítima, ao funcionamento de um sistema informático, através da introdução, transmissão, danificação, eliminação, deterioração, modificação ou supressão de dados informáticos.[47]

É importante que mencionemos ainda os artigos 7º, 8º e 9º da já referida Convenção sobre o Cibercrime, pois, ainda que o Brasil não seja dela signatário os referidos artigos apresentam parâmetros para que sejam punidas determinadas condutas que atualmente já são punidas pelo ordenamento jurídico pátrio.

Os artigos 7º e 8º da Convenção em tela apresentam regras para que os signatários possam legislar acerca da punição de condutas como a introdução, alteração, eliminação ou supressão de dados informáticos, fazendo-os inverídicos mas com a finalidade de que sejam considerados autênticos, induzindo a erro os usuários dos dados, assim dispondo:

> **Artigo 7º - Falsidade informática**

[47] Convenção sobre o Cibercrime. Disponível em: <http://ccji.pgr.mpf.gov.br/atuacao-da-ccji/documentos/docs_documentos/convencao_cibercrime.pdf>. Acesso em: 02 abr 2012.

> Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracção penal, em conformidade com o seu direito interno, a introdução, a alteração, a eliminação ou a supressão intencional e ilegítima de dados informáticos, produzindo dados não autênticos, com a intenção de que estes sejam considerados ou utilizados para fins legais como se fossem autênticos, quer sejam ou não directamente legíveis e inteligíveis. Uma Parte pode exigir no direito interno uma intenção fraudulenta ou uma intenção ilegítima similar para que seja determinada a responsabilidade criminal.
>
> **Artigo 8º - Burla informática**
>
> Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracção penal, em conformidade com o seu direito interno, o acto intencional e ilegítimo, que origine a perda de bens a terceiros através:
>
> a) Da introdução, da alteração, da eliminação ou da supressão de dados informáticos, b) De qualquer intervenção no funcionamento de um sistema informático, com a intenção de obter um benefício económico ilegítimo para si ou para terceiros.[48]

No que se refere a tais artigos, já há disposição semelhante em nossa legislação penal pátria, mais precisamente no Código Penal o crime de Inserção de dados falsos em sistemas de informações, previsto no artigo 313-A do Código Penal e o crime de Modificação ou alteração não autorizada de sistema de informações, previsto no artigo 313-B do Diploma Penal Pátrio, conforme deles tratamos no item 2.1 do capítulo II do presente trabalho. É de se salientar que tais crimes foram incluídos no Código Penal Brasileiro em 14 de julho de 2000, através da lei 9.983/2000.

O artigo 9º da Convenção sobre o Cibercrime por seu turno, trata de normas genéricas para que sejam adotadas medidas legislativas que possibilitem a punição de praticas referentes a pornografia infantil por meio de sistemas informáticos, que é o mesmo que sistemas cibernéticos, montando um conjunto normativo e de políticas aos cibercrimes, dispondo da seguinte maneira:

> **Artigo 9º - Infracções relacionadas com pornografia infantil**
>
> 1. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracção penal, em conformidade com o seu direito interno, as seguintes condutas, quando cometidas de forma intencional e ilegítima:
>
> a) Produzir pornografia infantil com o objectivo da sua difusão através de um sistema informático;
>
> b) Oferecer ou disponibilizar pornografia infantil através de um sistema informático;
>
> c) Difundir ou transmitir pornografia infantil através de um sistema informático;
>
> d) Obter pornografia infantil através de um sistema informático para si próprio ou para terceiros;
>
> e) Possuir pornografia infantil num sistema informático ou num meio de armazenamento de dados informáticos.
>
> 2. Para efeitos do n.º 1, a expressão "pornografia infantil" inclui qualquer material pornográfico que represente visualmente:
>
> a) Um menor envolvido num comportamento sexualmente explícito;

[48] Convenção sobre o Cibercrime. Disponível em: <http://ccji.pgr.mpf.gov.br/atuacao-da-ccji/documentos/docs_documentos/convencao_cibercrime.pdf>. Acesso em: 02 abr 2012.

> b) Uma pessoa que aparente ser menor envolvida num comportamento sexualmente explícito;
> c) Imagens realísticas que representem um menor envolvido num comportamento sexualmente explícito;
> 3. Para efeitos do n.º 2, a expressão "menor" inclui qualquer pessoa com idade inferior a 18 anos. Uma Parte, pode, no entanto, exigir um limite de idade inferior, que não será menos que 16 anos.
> **4.** Cada Parte pode reservar-se o direito de não aplicar, no todo ou em parte, o disposto nos n.ºs1, alínea *d)*, e., 2, alíneas *b)* e *c)*.[49]

Em relação à pornografia infantil por meio de sistemas de informática, há no Brasil dispositivo legal que pune tal conduta, referimo-nos ao artigo 241-A da lei 8.069/90 – Estatuto da Criança e do Adolescente – sobre o qual já discorremos no item 2.1 do capítulo II deste trabalho. Tal dispositivo foi incluído no Estatuto da Criança e do Adolescente em 25 de novembro de 2008, por meio da lei 11.829/08.

Referente à investigação de crimes cibernéticos, a Convenção sobre o Cibercrime discorre em seu artigo 16º sobre a possibilidade de os signatários legislarem a respeito da guarda de informações de usuários e dados de tráfego que possam, posteriormente, ser utilizados na investigação de crimes, bem como sobre a possibilidade de obtenção dessas informações por parte das autoridades competentes. Dispõe o artigo 16º da Convenção:

> **Artigo 16º - Conservação expedita de dados informáticos armazenados**
> 1. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para permitir às suas autoridades competentes exigir ou obter de uma outra forma a conservação expedita de dados informáticos específicos, incluindo dados relativos ao tráfego, armazenados por meio de um sistema informático, nomeadamente nos casos em que existem motivos para pensar que os mesmos são susceptíveis de perda ou alteração.
> 2. Sempre que a Parte aplique o disposto no n.º 1, através de uma injunção ordenando a uma pessoa que conserve os dados informáticos específicos armazenados que estão na sua posse ou sob o seu controlo, esta Parte adoptará as medidas legislativas e outras que se revelem necessárias para obrigar essa pessoa a conservar e proteger a integridade dos referidos dados durante um período de tempo tão longo quanto necessário, até um máximo de 90 dias, de modo a permitir às autoridades competentes obter a sua divulgação. Uma Parte pode prever que essa injunção seja subsequentemente renovada.
> 3. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para obrigar o responsável pelos dados, ou outra pessoa encarregada de os conservar a manter segredo sobre a execução dos referidos procedimentos durante o período previsto pelo seu direito interno.[50]

Em seu bojo, traz a Convenção em comento importantes diretrizes relativas à interceptação de dados em sistemas de informática, dispondo em seu artigo 21º sobre normas genéricas para a adoção de medidas que respaldem a colheita em tempo real de dados

---

[49] Convenção sobre o Cibercrime. Disponível em: <http://ccji.pgr.mpf.gov.br/atuacao-da-ccji/documentos/docs_documentos/convencao_cibercrime.pdf>. Acesso em: 02 abr 2012.
[50] Ibidem.

essenciais às investigações, assim como a aplicação de meios técnicos que possibilitem às autoridades o registro desses dados, inclusive com a obrigatoriedade de fornecedores de serviços de informática em colaborarem com as investigações, como é o caso de algumas esparsas leis estaduais e municipais existentes em território nacional, algumas delas mostradas no presente trabalho, assim indicando:

> **Artigo 21º - Intercepção de dados relativos ao conteúdo**
> 1. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para habilitar as suas autoridades competentes relativamente a um leque de infracções graves, a definir em direito interno, a:
> a) Recolher ou registar, através da aplicação de meios técnicos existentes no seu território, e
> b) Obrigar um fornecedor de serviços, no âmbito da sua capacidade técnica existente, a:
> i. Recolher ou registar através da aplicação de meios técnicos no seu território, ou
> ii. Prestar às autoridades competentes o seu apoio e a sua assistência para recolher ou registar, em tempo real, dados relativos ao conteúdo de comunicações específicas no seu território, transmitidas através de um sistema informático.
> **2.** Quando a Parte em virtude dos princípios estabelecidos pela sua ordem jurídica interna, não pode adoptar as medidas descritas no n.º 1, alínea *a)*, pode, em alternativa, adoptar as medidas legislativas e outras que se revelem necessárias, para assegurar a recolha ou o registo em tempo real dos dados relativos ao conteúdo associados a comunicações específicas transmitidas no seu território através da aplicação de meios técnicos existentes nesse território.
> 3. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias, para obrigar um fornecedor de serviços a manter secreto o facto de
> qualquer um dos poderes previstos no presente artigo ter sido executado, bem como qualquer informação a esse respeito.[51]

Entendemos ainda ser salutar apresentar o artigo 35º da Convenção sobre o Cibercrime, o qual disciplina a criação de uma rede interligada entre os países signatários e que possa funcionar 24 horas por dias, 07 dias por semana, onde cada signatário deve disponibilizar um ponto de acesso interligado à rede na intenção de prestarem assistência técnica imediata de uma parte à outra para a investigação, procedimentos e colheitas de provas de infrações penais perpetradas por meio de sistemas de informática, o que é algo bastante importante, dada as peculiaridades dos crimes cibernéticos, onde um criminoso de um país pode agir, causando lesões jurídicas que só serão sentidas em um outro país. Senão vejamos:

> **Artigo 35º - Rede 24/7**
> 1. Cada Parte designará um ponto de contacto disponível 24 horas sobre 24 horas, 7 dias por semana, a fim de assegurar a prestação de assistência imediata a investigações ou procedimentos respeitantes a infracções penais relacionadas com dados e sistemas informáticos, ou a fim de recolher provas, sob forma electrónica,

[51] Convenção sobre o Cibercrime. Disponível em: <http://ccji.pgr.mpf.gov.br/atuacao-da-ccji/documentos/docs_documentos/convencao_cibercrime.pdf>. Acesso em: 02 abr 2012.

> de uma infracção penal. O auxílio incluirá a facilitação, ou se o direito e práticas internas o permitirem, a aplicação directa das seguintes medidas:
> a) A prestação de aconselhamento técnico;
> b) A conservação de dados em conformidade com os artigos 29º e 30º; e
> c) A recolha de provas, informações de carácter jurídico e localização de suspeitos.
> 2. a) O ponto de contacto de uma Parte deve ter capacidade técnica para corresponder-se com o ponto de contacto de outra Parte de uma forma rápida;
> b) Se o ponto de contacto designado por uma Parte não depender da autoridade ou autoridades dessa Parte responsáveis pela cooperação internacional ou extradição dessa Parte, o ponto de contacto assegurará que pode agir em coordenação com essa ou essas autoridades de forma rápida.
> 3. Cada Parte assegurará que pode dispor de pessoal formado e equipado a fim de facilitar o funcionamento da rede.[52]

Por fim, temos que a Convenção sobre o Cibercrime, firmada em Budapeste em 23.11.2001 é um importante instrumento que se traduz em avanço na preocupação mundial pela prevenção e combate aos delitos praticados através de sistemas informatizados, condutas estas cada vez mais freqüentes na sociedade hodierna, e que podem ser danosas a um sem numero de pessoas, uma vez que hoje grande parcela da população mundial encontra-se também inserida na vivencia que ocorre no mundo virtual, seja para se comunicar, para obter informação, estudar ou trabalhar.

3.2 O Projeto de Lei nº 84/1999

Em 24/02/1999 Luiz Piauhylino, até então deputado pelo estado de Pernambuco, apresentou na Câmara dos Deputados o projeto de lei nº 84/1999, que propõe a tipificar condutas lesivas perpetradas em sistemas de informática, além das lesões praticadas por meio da *internet,* possibilitando assim o suprimento da lacuna legal que existe em relação à punição dos autores dessas condutas, ate o presente sem tipificação.

Após sua tramitação na Câmara dos Deputados, o referido projeto de lei foi encaminhado ao Senado Federal, seguindo apenso aos projetos de lei 76/2000 e 137/2000, em virtude desses últimos guardarem a mesma natureza e identidade com a matéria do projeto de lei em comento. Após isso, retornou à Câmara dos Deputados para apreciação de algumas alterações, onde encontra-se em tramitação na Comissão de Segurança Pública e Combate ao Crime Organizado.[53]

---

[52] Convenção sobre o Cibercrime. Disponível em: <http://ccji.pgr.mpf.gov.br/atuacao-da-ccji/documentos/docs_documentos/convencao_cibercrime.pdf>. Acesso em: 02 abr 2012.

[53] PIAUHYLINO, Luiz. **Projeto de Lei da Câmara dos Deputados nº 84, de 1999**. Dispõe sobre os crimes cometidos na área de informática, suas penalidades e dá outras providências. Disponível em: <http://www.camara.gov.br/internet/sileg/Prop_Detalhe.asp?id=15028>. Acesso em: 12 mar. 2012.

Ainda que alguns crimes cibernéticos possam ser processados pelos artigos já existentes no Código Penal Brasileiro, é sabido que há um grande numero de condutas praticadas eletronicamente, que se proliferam e se modernizam, que lesam direitos patrimoniais ou de informações, e que não podem ser coibidas por ausência da legislação pátria que ainda não tipificou essas condutas.

O projeto de lei em tela propõe modificações no Código Penal Brasileiro para tipificar inúmeras condutas lesivas, além de alterações do Código Penal Militar, Leis 7.716/89 e 8.069/90.

Para o presente trabalho, resguardamo-nos às alterações propostas para o Código Penal Brasileiro, por serem alterações de maior vulto e se tratarem de condutas lesivas comumente vivenciadas.

A invasão a sistemas de informática e a obtenção não autorizada de dado ou informação são condutas contempladas pelo artigo 2º do projeto de lei em comento, que propõe a inclusão dos artigos 285-A e 285-B no Código Penal para a punição dessas condutas, assim dispondo:

> **Art. 2º** O Título VIII, da Parte Especial do Código Penal, fica acrescido do Capítulo IV, assim redigido: "Capítulo IV DOS CRIMES CONTRA A SEGURANÇA DOS SISTEMAS INFORMATIZADOS Acesso não autorizado a rede de computadores, dispositivo de comunicação ou sistema informatizado
> **Art. 285-A.** Acessar, mediante violação de segurança, rede de computadores, dispositivo de comunicação ou sistema informatizado, protegidos por expressa restrição de acesso: Pena - reclusão, de 1 (um) a 3 (três) anos, e multa.
> **Parágrafo único.** Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime, a pena é aumentada de sexta parte.
> **Obtenção, transferência ou fornecimento não autorizado de dado ou informação Art. 285-B.** Obter ou transferir, sem autorização ou em desconformidade com autorização do legítimo titular da rede de computadores, dispositivo de comunicação ou sistema informatizado, protegidos legalmente e com expressa restrição de acesso, dado ou informação neles disponível: Pena – reclusão, de 1 (um) a 3 (três) anos, e multa. **Parágrafo único.** Se o dado ou informação obtida desautorizadamente é fornecida a terceiros, a pena é aumentada de um terço.[54]

No que se refere ao dano em dados eletrônicos, a criação e difusão de códigos maliciosos em sistemas de informática, o projeto de lei mencionado propõe a alteração do artigo 163 do Código Penal e a inserção do artigo 163-A no Diploma Penal, com o intuito de tipificar tais condutas, sendo proposto do seguinte modo:

> **Art. 4º O caput do art. 163, do Código Penal, passa a vigorar com a seguinte**

[54] PIAUHYLINO, Luiz. **Projeto de Lei da Câmara dos Deputados nº 84, de 1999**. Dispõe sobre os crimes cometidos na área de informática, suas penalidades e dá outras providências. Disponível em: <http://www.camara.gov.br/internet/sileg/Prop_Detalhe.asp?id=15028>. Acesso em: 24 nov. 2010

> **redação: "Dano Art. 163 -** Destruir, inutilizar ou deteriorar coisa alheia ou dado eletrônico alheio: ....."
> **Art. 5º O Capítulo IV, do Título II, da Parte Especial, do Código Penal, fica acrescido do art. 163-A, assim redigido: "Inserção ou difusão de código malicioso**
> **Art. 163-A.** Inserir ou difundir código malicioso em dispositivo de comunicação, rede de computadores, ou sistema informatizado: Pena – reclusão, de 1 (um) a 3 (três) anos, e multa. **Inserção ou difusão de código malicioso seguido de dano**
> **§ 1º.** Produzir intencionalmente ou vender código malicioso destinados ao uso em dispositivo de comunicação, rede de computadores ou sistema informatizado. Pena – reclusão de 1 (um) a 3 (três) anos, e multa.
> **§ 2º.** Se do crime resulta destruição, inutilização, deterioração, alteração, dificultação do funcionamento, ou funcionamento desautorizado pelo legítimo titular, de dispositivo de comunicação, de rede de computadores, ou de sistema informatizado: Pena – reclusão, de 2 (dois) a 4 (quatro) anos, e multa.
> **§ 3º.** Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime, a pena é aumentada de sexta parte."[55]

Já se a difusão de códigos maliciosos se der com a intenção de obter-se vantagem financeira do agente ou de terceiro em detrimento de outrem, a punição deve ocorrer de acordo com o artigo 171 do Código Penal, de acordo com o projeto de lei em comento que propõe a inclusão de inciso VII e de § 3º ao artigo 171 do Código Penal, da seguinte maneira:

> **Art. 6º O art. 171, do Código Penal, passa a vigorar acrescido dos seguintes dispositivos:**"Art. 171. ....§ 2º Nas mesmas penas incorre quem:.....
> **Estelionato Eletrônico**
> **VII –** difunde, por qualquer meio, código malicioso com intuito de devastar, copiar, alterar, destruir, facilitar ou permitir acesso indevido à rede de computadores, dispositivo de comunicação ou sistema informatizado, visando o favorecimento econômico de ou de terceiro em detrimento de outrem.
> **§ 3º.** Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime previsto no inciso VII, do § 2º,deste artigo, a pena é aumentada de sexta[56]

Quanto ao crime de atentado a segurança dos serviços de utilidade pública, previsto no artigo 265 do Código Penal, o referido projeto de lei propõe a alteração deste artigo para tipificar como crime também o atentado a segurança ou funcionamento de informação ou telecomunicação, assim prevendo:

> **Art. 7º O art. 265, do Código Penal, passam a vigorar com as seguintes redações:**
> **"Atentado contra a segurança de serviço de utilidade pública**

[55] PIAUHYLINO, Luiz. **Projeto de Lei da Câmara dos Deputados nº 84, de 1999**. Dispõe sobre os crimes cometidos na área de informática, suas penalidades e dá outras providências. Disponível em: <http://www.camara.gov.br/internet/sileg/Prop_Detalhe.asp?id=15028>. Acesso em: 12mar. 2012.
[56] Ibidem.

> **Art. 265 -** Atentar contra a segurança ou o funcionamento de serviço de água, luz, força, calor, informação ou telecomunicação, ou qualquer outro de utilidade pública: ....."[57]

Por fim, é proposta a alteração dos artigos 297 e 298 do Código Penal, ao inserir a expressão "dado informático" nos crimes de falsificação de documento público e falsificação de documento particular, conforme se apresenta:

> **Art. 8º O caput do art. 297, do Código Penal, passa a vigorar com a seguinte redação:**
> **"Falsificação ou Alteração de dado informático ou documento público**
> **Art. 297 –** Falsificar ou alterar, no todo ou em parte, dado informático ou documento público verdadeiro:....."
> **Art. 9º O caput do art. 298, do Código Penal, passa a vigorar com a seguinte redação:**
> **"Falsificação ou alteração de dado informático ou documento particular**
> **Art. 298 –** Falsificar ou alterar, no todo ou em parte, dado informático ou documento particular verdadeiro:....."[58]

É necessário frisar que o projeto de lei 84/1999 propõe que os provedores de acesso à rede mundial de computadores mantenham em seus arquivos de forma segura e para fins de investigação pública os dados de endereçamento eletrônico da origem, destino, horário e data da conexão efetuada por meio da rede, devendo tais dados serem mantidos pelo prazo de três anos e fornecidos às autoridades policiais e Ministério Públicos sempre que forem requisitadas, o que já ocorre em algumas localidades mediante a edição de leis locais (municipais ou estaduais). Se os provedores por ventura descumprirem tal regra, o projeto propõe a punição dos mesmos com multas que variam de R$ 2.000,00 (dois mil reais) a R$ 100.000,00(cem mil reais), o que entendemos ser uma medida bastante salutar, evitando assim que criminosos utilizem-se de computadores públicos para perpetrar crimes cibernéticos sem serem identificados.

Observamos que o projeto de lei explanado mostra-se propicio ao suprimento da atual lacuna legislativa, podendo vir a diminuir a dificuldade legal em combater-se os crimes cibernéticos, muito embora ainda esteja tramitando no Congresso Nacional, não sendo ainda possível a sua aplicação já que não foi convertido em lei ainda.

---

[57] Ibidem.
[58] Ibidem.

CONSIDERAÇÕES FINAIS

Através da pesquisa realizada para a produção do presente estudo, foi possível perceber a grande quantidade de condutas lesivas praticadas através da *internet* e que não podem ser punidas por ausência de tipificação penal dessas condutas.

Foi possível verificar as fraudes mais comuns cometidas mediante o uso da rede mundial de computadores, onde algumas delas a exemplo do furto de valores em contas bancárias praticado por meio eletrônico é processado pela tipificação do Código Penal, mas as condutas de criação e disseminação de códigos maliciosos, bem como as invasões em sistemas de informática não são ainda tipificadas no ordenamento jurídico pátrio, sendo ainda impossível a punição dos agentes que praticam tais ações. Tais condutas poderão, no entanto, serem punidas, caso haja a aprovação do projeto de lei 84/1999 que propõe a tipificação das condutas lesivas praticadas atualmente por meio da *internet.*

É evidente a dificuldade do braço coercitivo estatal em proceder às investigações dessas novas modalidades criminosas e ainda das condutas lesivas, seja pelo fato da pouca aparelhagem das instituições, seja por falta de subsidio legal para o processamento das investigações. Entendemos, no entanto, pela aplicabilidade da lei 9.296/96 na colheita de provas de infrações perpetradas por meio da *internet,* pois todo o sistema de *internet* funciona por meio de sistemas telefônicos e, ademais, advogamos o posicionamento de que o sigilo dos dados podem ser violados por meio de autorização judicial, nos termos da lei 9.296/96, conforme prevê o artigo 5º, inciso XII da Constituição Federal, por fim, acreditando ainda que era esse afinal, o desígnio do legislador a editar a presente lei, visando sobretudo diminuir a impunidade que ronda tais tipos de delito.

A *internet* evolui em uma grande velocidade, não podemos negar, advindo desse avanço novas espécies de redes sociais, o que possibilita outras modalidades criminosas e novas condutas que lesam os usuários da grande rede mundial de computadores e até mesmo os próprios sistemas de informática. É imperioso que haja legislação específica no sentido de coibir, com a tipificação de novas condutas e a criação de mecanismos processuais preventivos e repressivos, a fim de se proporcionar a Polícia Judiciária e ao Ministério Público, detentor da ação penal pública um combate efetivo à essa nova forma de criminalidade.

Em âmbito mundial importante documento é a Convenção sobre o Cibercrime, onde as nações signatárias buscam disciplinar uniformemente suas regras materiais e

processuais no que se referente ao combate aos crimes cibernéticos, evitando que ocorram vazios que coloquem em risco as investigações, possibilitando após elas a punição dos criminosos. Seria bastante importante que um número maior de países aderisse à Convenção de Budapeste, com o fito de possibilitar uma maior uniformidade nas diretrizes a serem seguidas e uma maior cooperação internacional no combate ao crime cibernético, dado as características dinâmicas desse tipo de delito.

Somos, no Brasil, ansiosos pela aprovação do projeto de lei 84/1999, para que determinadas condutas atualmente impossíveis de serem punidas passem a ter tipificação penal e os infratores possam ser punidos. É de pouca efetividade a criação de grupos especializados na investigação de crimes por meio da *internet* se não houver à disposição dos investigadores ferramentas legais e técnicas que sejam capazes de combater de forma efetiva o cibercrime, notadamente legais, que é o que efetivamente permite que esse tipo de criminoso possa vir a ser punido caso cometa esse tipo de conduta.

É bem verdade que o projeto de lei 84/1999 tramita no Congresso Nacional por longos 13 (treze) anos, mas é notável que representa um avanço no sentido de buscar preservar a ordem no ambiente virtual, punindo as novas modalidades delituosas inerentes ao ritmo dinâmico da sociedade contemporânea. O direito não pode ser estático, deve mover-se na mesma velocidade da sociedade que ele regula.

REFERÊNCIAS

AS VULNERABILIDADES dos aplicativos de desktop e o uso de técnicas de invisibilidade estão aumentando, Califórnia, 2006. Disponível em: < http://www.symantec.com/pt/br/about/news/release/article.jsp?prid=20061010_01>. Acesso em: 10. abr. 2012.

BRASIL. Constituição Federal da República Federativa do Brasil de 1988. **Diário Oficial da União**, Brasília, 05 out. 1988.

_____. Decreto-Lei 2.848/40 de 07 de dezembro de 1940. Código Penal. **Diário Oficial da União**, Brasília, 31 dez. 1940.

_____. Lei 8.069/1990 de 13 de julho de 1990. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. **Diário Oficial da União**, Brasília, 27 set. 1990.

_____. Lei 9.296 de 24 de julho de 1996. Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal. **Diário Oficial da União**, Brasília, 25 jul. 1996.

_____. **Superior Tribunal de Justiça**. Embargos de Declaração no Conflito de Competência nº 2007/0141978-0 (EDcl no CC 86913 / PR), Terceira Seção, Relator Ministro Napoleão Nunes Maia Filho), 08/10/2008. Disponível em: <www.stj.jus.br>. Acesso em 02. abr. 2012.

_____. **Superior Tribunal de Justiça** – Habeas Corpus nº 2007/0087811-8 (HC81638 / PA), Quinta Turma, Relator Ministro Gilson Dipp, 12/06/2007. Disponível em: <www.stj.jus.br>. Acesso em 06. Abr 2012.

_____. **Superior Tribunal de Justiça**. RHC 18116 / SP Relator Ministro Hélio Quaglia Barbosa, sexta turma, julgado em 16/02/2006. Disponível em: <www.stj.jus.br>. Acesso em 05. Abr. 2012.

BONFIM, Eduardo Mougenot. **Curso de Processo Penal.** São Paulo: Saraiva, 2007.

CAPEZ, Fernando. **Curso de Direito Penal, parte geral.** São Paulo: Saraiva, 2005.
CADASTRO em lan houses deve conciliar liberdade e segurança, dizem especialistas. 2010. Disponível em < http://tecnologia.uol.com.br/ultimas-noticias/redacao/2010/05/11/cadastro-

em-lan-houses-deve-conciliar-liberdade-e-seguranca-dizem-especialistas.jhtm> Acesso em 10. Mai. 2012.

CASTELA, Eduardo Marcelo. **Investigação Criminal e Informática**. Curitiba: Juruá, 2005.

CENTRAL Nacional de Denúncias, 2010. Disponível em: <http://www.safernet.org.br/site/indicadores>. Acesso em 23. mai. 2012

CONTI, Fátima. **Afinal, o que é cibercrime?**. 2008. Disponível em: < http://www.dicas-l.com.br/interessa/interessa_20080814.php>. Acesso em 10 abr. 2012.

CONVENÇÃO SOBRE O CIBERCRIME. Disponível em: <http://ccji.pgr.mpf.gov.br/atuacao-da-ccji/documentos/docs_documentos/convencao_cibercrime.pdf >. Acesso em: 23 mai 2012.

FONSECA, Tiago Abud. **Interceptação Telefônica – A devassa em nome da lei**. Rio de Janeiro: Espaço Jurídico, 2008.

GRECO, Rogério. **Curso de Direito Penal**.. 12.ed. Rio de Janeiro: Ímpetus, 2010.

GRECO FILHO, Vicente. **Interceptação telefônica: (considerações sobre a lei 9.296/96, de 24 de julho de 1996)**. 2. Ed. São Paulo: Saraiva, 2006.

JUNIOR, Celso Moreira Ferro. **A tecnologia na Investigação Criminal**. Disponível em <http://www.datavenia.net/opiniao/celso.html> Acesso em 02. abr. 2012.

LIMA, Marcellus Polastri. **Manual de Processo Penal**. 2 ed. Rio de Janeiro. Editora Lumen Juris. 2009.

MOURA, Douro. **Crimes Virtuais no Brasil**. Disponível em: <http://www.buscalegis.ufsc.br/revistas/index.php/buscalegis/article/download/11605/11170> . Acesso em 13. Abr. 2012.

PIAUHYLINO, Luiz. **Projeto de Lei da Câmara dos Deputados nº 84, de 1999**. Dispõe sobre os crimes cometidos na área de informática, suas penalidades e dá outras providências. Disponível em: <http://www.camara.gov.br/internet/sileg/Prop_Detalhe.asp?id=15028>. Acesso em: 25 mai. 2012.

RANGEL, Paulo. **Breves considerações sobre a Lei 9296/96 (interceptação telefônica)**. Disponível em: <http://jus.uol.com.br/revista/texto/195/breves-consideracoes-sobre-a-lei-9296-96-interceptacao-telefonica/1>.Acesso em 25. abr. 2012.

SANTA CATARINA. Lei 14.890, de 22 de outubro de 2009. Disciplina o controle de usuários em estabelecimentos voltados a comercialização do acesso a internet no Estado de Santa Catarina. **Diário Oficial do Estado de Santa Catarina**, Florianópolis, 22 out. 2009.

SÃO PAULO. Lei 12.228, de 11 de janeiro de 2006. Dispõe sobre os estabelecimentos comerciais que colocam à disposição, mediante locação, computadores e máquinas para acesso à internet e dá outras providências. **Diário Oficial do Estado de São Paulo**, São Paulo, 12 Jan. 2006.

SOARES. Diego de Almeida. **Spam: Legislação 2.0**. Caruaru: Asces, 2005.

TOLEDO, Francisco de Assis *apud* GALVÃO, Fernando; GRECO, Rogério. **Estrutura Jurídica do Crime**. Belo Horizonte: Mandamentos. 1999.