UNIVERSIDADE FEDERAL DE JUIZ DE FORA
SAMUEL BRANDÃO BARROS LIMA

# CRIME CIBERNÉTICO E SUA PRÁTICA CADA VEZ MAIS FREQUENTE NO BRASIL

JUIZ DE FORA
2011

SAMUEL BRANDÃO BARROS LIMA

# CRIME CIBERNÉTICO E SUA PRÁTICA CADA VEZ MAIS FREQUENTE NO BRASIL

Monografia apresentada à Faculdade de Direito da Universidade Federal de Juiz de Fora como requisito parcial para obtenção do título de Bacharel em Direito.

Orientador: ABDALLA DANIEL CURI

Juiz de Fora

2011

SAMUEL BRANDÃO BARROS LIMA

# CRIME CIBERNÉTICO E SUA PRÁTICA CADA VEZ MAIS FREQUENTE NO BRASIL

Monografia apresentada à Faculdade de Direito da Universidade Federal de Juiz de Fora como requisito parcial para obtenção do título de Bacharel em Direito.

Aprovado em: _____/_____/_____

_____

Prof. Abdalla Daniel Curi

_____

Prof. Luiz Eduardo Moura Gomes

_____

Profª. Clarissa Diniz Guedes

Juiz de Fora

2011

**AGRADECIMENTOS**

Aos professores de toda a faculdade de Direito da Universidade Federal de Juiz de Fora, pelos ensinamentos que puderam me oferecer, e em especial, ao professor Abdalla Daniel Curi, pela orientação neste trabalho.

À minha família, que sempre esteve ao meu lado, em especial meu pai Wanderson, minha mãe Celi e meus irmãos Leonardo e Gabriela.

Aos meus amigos, que sempre me apoiaram e me deram conselhos nos momentos de dificuldade.

Dedico este trabalho à minha família, aos meus amigos, aos professores da faculdade de Direito da Universidade Federal de Juiz de Fora e a todos que me apoiaram durante o curso.

## RESUMO

A Internet trouxe inúmeros benefícios a todos nós, entretanto, ela também propiciou o surgimento de práticas ilícitas novas, bem como possibilitou a existência de outras formas de execução de crimes já existentes. O objetivo deste trabalho é demonstrar a prática cada vez mais freqüente dos crimes cibernéticos no Brasil e a necessidade de uma legislação penal para a proteção dos bens jurídicos que possam ser ofendidos por meio da Internet. Além disso, busca-se analisar os aspectos que dificultam a identificação de autoria, fator importante para o aumento da criminalidade no meio cibernético.


Palavras-chave: Crime cibernético. Internet.

**ABSTRACT**

The internet has brought numerous benefits to all of us however it has also made new methods of breaching the law possible as well as more innovative forms of performing already existing crimes. The objective of this paper is to demonstrate the ever more frequent practice of cybercrimes in Brazil and the need of protective legislation to ensure the rights that might be broken via the Internet. This paper also seeks to analyze some of the aspects that make harder the identification of the perpetrator an important fact in the rising of internet criminality.
Key words: Cybercrime. Internet.

**SUMÁRIO**

## 1. INTRODUÇÃO

Não há dúvidas que a Internet trouxe inúmeros benefícios a todos nós, entretanto, ela também propiciou o surgimento de práticas ilícitas novas, bem como possibilitou a existência de outras formas de execução de crimes já existentes.

Quem pratica crime através do computador tem a falsa sensação de que nada irá lhe ocorrer, pelo fato da Internet ser uma rede pública e com milhões de usuários pelo mundo. Tal sensação se sublima ainda com a falta de controle sobre o que é certo ou errado na rede e termina com a morosidade do poder público em combater ou conseguir resultados breves no andamento dos casos deste tipo de delito.

Foi na década de 90 que o Brasil, notadamente, experimentou as influências da globalização e seus efeitos, inclusive, pelo acesso a bens tecnológicos, sendo tudo isso propiciado pela abertura econômica. Atualmente um vasto número de atividades e de serviços pode ser realizado com o apoio da Internet, tais como: certificação digital; leilões virtuais, correios eletrônicos, comércio dos mais variados produtos; operações no mercado financeiro (como investimentos, compra e venda de ações e serviços bancários), conversas e interação em tempo real entre os internautas através de *chats* ou programas como *instant messenger* e etc.

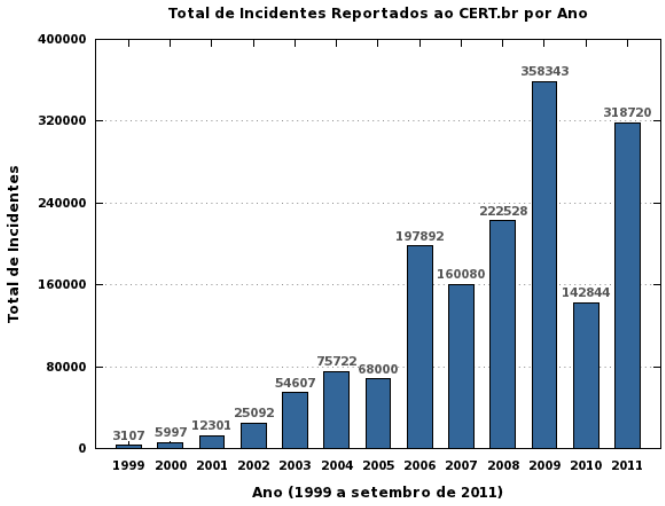
De acordo com Corrêa, no ano de 2000, mais de 7 milhões de internautas acessaram a *Web* a partir de computadores residenciais e navegaram, em média, mais de 9 horas por mês, passando mais tempo conectados que usuários de países como Inglaterra, França e Alemanha.[1]

Assim como aumenta o número de usuários que se conectam à Internet no Brasil, aumenta, também, o número de delitos praticados através dela. Como podemos verificar através das estatísticas feitas pelo CERT.br (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil), os incidentes reportados são muito maiores nos últimos anos.

---

[1] CORRÊA, Gustavo Testa. **Aspectos jurídicos da Internet**. São Paulo: Saraiva, 2000, p. 39

Gráfico 1 – Total de Incidentes Reportados ao CERT.br por ano




Fonte: CERT.br. Estatísticas do CERT.br. Disponível em: <http://www.cert.br/stats/incidentes/>. Acesso em: 5 nov. 2011.

O CERT.br considera como um incidente de segurança qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de computação ou de redes de computadores, sendo que podemos exemplificá-los como: a)tentativas de ganhar acesso não autorizado a sistemas ou dados; b)ataques de negação de serviço; c)uso ou acesso não autorizado a um sistema; d)modificações em um sistema, sem o conhecimento, instruções ou consentimento prévio do dono do sistema; e)desrespeito à política de segurança ou à política de uso aceitável de uma empresa ou provedor de acesso.

Segundo Santos, o crime virtual já é mais lucrativo do que o narcotráfico. A Secretaria da Fazenda de São Paulo publicou (Informativo CAT n° 63), comentando que o comércio ilegal se expande na Internet e a pirataria que o acompanha já apresenta números superiores ao narcotráfico.[2]

O objetivo deste trabalho é demonstrar a prática cada vez mais freqüente dos crimes cibernéticos no Brasil e a necessidade de uma legislação penal para a

[2] SANTOS, Coriolano Aurélio de Almeida Camargo. **ATUAL CENÁRIO DOS CRIMES CIBERNÉTICOS NO BRASIL**. Disponível em: <http://www2.oabsp.org.br/asp/comissoes/sociedade_informacao/artigos/crimes_ciberneticos.pdf>. Acesso em: 15 set. 2011.

proteção dos bens jurídicos que possam ser ofendidos por meio da Internet. Além disso, busca-se analisar os aspectos que dificultam a identificação de autoria.

# 2. NOÇÕES GERAIS DE INTERNET

Para que haja uma melhor compreensão acerca do tema tratado no trabalho, far-se-á necessário um entendimento mais abrangente sobre a Internet, onde a evolução histórica, aspectos técnicos e jurídicos serão abordados neste capítulo.

## 2.1. EVOLUÇÃO HISTÓRICA

Com o lançamento do satélite artificial *Sputnik,* em 4 de outubro de 1957, pela União Soviética, o presidente dos EUA, Eisenhower, criou a *Advanced Research Projects Agency* (ARPA), com o intuito de obter novamente a liderança tecnológica perdida para os soviéticos durante a Guerra Fria.

O principal objetivo da ARPA era criar programas relacionados a satélites e ao espaço, tendo por norte o receio de uma guerra nuclear, buscando avigorar as forças armadas Norte Americanas.

Em 1969, a ARPA criou uma rede denominada ARPANET, que operaria através de inúmeras e pequenas redes locais, denominadas *Local Area Network* (LAN), ou seja, uma rede local responsável em ligar computadores em um mesmo edifício, as quais foram interligadas por meio de redes de telecomunicação geográficas, denominadas *Wide Area Network* (WAN), que significa rede de longo alcance, responsáveis pela conexão de computadores por todo o mundo, e assim, caso houvesse um ataque nuclear contra os EUA, as comunicações militares e governamentais não seriam interrompidas.[3]

A *National Science Foundations* (NSF) assumiu, em 1984, a manutenção da ARPANET e, mais tarde, interligou seus supercomputadores (nomeados de *backbones*) de seu centro de pesquisas e passou a denominar-se NSFNET. De

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

acordo com Zaniolo (2007, p. 100), o conjunto de todos os computadores e redes ligados aos *backbones*, passou a ser conhecido oficialmente como Internet.[4]

No início dos anos 90, Tim Berners-Lee, cientista da *European Organization for Nuclear Research* (CERN), cria a *World Wide Web* (WWW), hoje a principal interface da Internet, a fim de propiciar a interatividade e o uso de sons e imagens na rede.

No Brasil, em 1990, é lançada a Rede Nacional de Pesquisas (RNP) pelo Ministério da Ciência e Tecnologia para gerenciar a rede acadêmica brasileira, capacitar recursos humanos de alta tecnologia e difundir a tecnologia Internet. Em 1995, criou-se o Comitê Gestor da Internet (CGI.br), com participação do Ministério da Ciência e Tecnologia, Ministério das Comunicações, de entidades operadoras e gestoras de espinhas dorsais (*backbones*), de representantes de provedores de acesso ou de informações, de representantes de usuários e da comunidade acadêmica, com a tarefa de coordenar e integrar todas as iniciativas de serviços de Internet no país.[5]

Em nota conjunta editada pelos Ministérios acima citados, em maio de 1995, definiu o que era Internet: A Internet é um conjunto de redes interligadas, de abrangência mundial. Através da Internet estão disponíveis serviços como correio eletrônico, transferência de arquivos, acesso remoto a computadores, acesso a bases de dados e diversos tipos de serviços de informação, cobrindo praticamente todas as áreas de interesse da sociedade.[6]

Desde 1995, quando foi liberado o uso comercial da Internet no Brasil, o número de usuários vem aumentando de modo significativo, ao ponto que, em 2009, ultrapassava-se o número de 75 milhões de pessoas com acesso à Internet, deixando o país em quarto lugar no ranking feito pela *Central Intelligence Agency* (CIA).

---

[4] ZANIOLO, Pedro Augusto. **Crimes modernos**: o impacto da tecnologia no direito. Curitiba: Juruá, 2007, p. 100.
[5] BRASIL. Comitê Gestor da Internet no Brasil. **Sobre o CGI.br**: histórico. Disponível em: <http://www.cgi.br/sobre-cg/historia.htm>. Acesso em: 18 set. 2011.
[6] BRASIL, 1995, Nota Conjunta. Ministério das Comunicações e Ministério da Ciência e Tecnologia. Disponível em: <http://www.cgi.br/regulamentacao/notas.htm>. Acesso em: 18 set. 2011.

Tabela 1 – Ranking de países com maior número de usuários de Internet

| RANK | COUNTRY | INTERNET USERS | DATE OF INFORMATION |
|---|---|---|---|
| 1 | China | 389,000,000 | 2009 |
| 2 | United States | 245,000,000 | 2009 |
| 3 | Japan | 99,182,000 | 2009 |
| 4 | Brazil | 75,982,000 | 2009 |
| 5 | Germany | 65,125,000 | 2009 |
| 6 | India | 61,338,000 | 2009 |
| 7 | United Kingdom | 51,444,000 | 2009 |
| 8 | France | 45,262,000 | 2009 |

Fonte: CENTRAL INTELLIGENCE AGENCY. World factbook: internet users. Disponível em: <https://www.cia.gov/library/publications/the-worldfactbook/rankorder/2153rank.html>. Acesso em: 30 ago. 2011.

## 2.2. ASPECTOS TÉCNICOS

A Internet é um enorme sistema de redes gateways e computadores interligados entre si a nível mundial e que funcionam como emissores e receptores de informação, utilizando para isso um conjunto de protocolos de comunicação denominados TCP/IP. A Internet permite interligar sistemas informáticos de todo o mundo, possibilitando a comunicação e a troca de informação de uma forma fácil e rápida. Os meios para efetuar essas ligações são diversos, e incluem rádio, linhas telefônicas, linhas digitais, satélite, ISDN, fibra-óptica, etc. No centro da Internet existe um *backbone* de linhas de comunicação de dados entre nós principais ou computadores *host*, composto por milhares de sistemas de computadores - um ou mais desses nós da Internet ou sistemas de computadores podem parar de

funcionar sem que isso impeça a Internet de funcionar como um todo, porque ela não é controlada por nenhum computador ou rede individual.[7]

O protocolo TCP/IP se assemelha ao endereço de um logradouro, onde se conhece exatamente o que irá mandar (pacote de dados) e para onde se quer direcionar tais pacotes (endereçamento). O *Transmission Control Protocol* (TCP) é o responsável pela entrega dos dados transmitidos a um endereço *Internet Protocol* (IP).

De acordo com Zaniolo:

> todo o endereçamento de equipamentos na internet é baseado em um identificador,que independe da tecnologia de rede envolvida: o *endereço IP*. Caracterizado pela unicidade, seu formato é representado por um número de 32 (trinta e dois) *bits*, dispostos em 4 números (inteiros de 0 a 255) de 8 *bits* separados por três pontos, permitindo assim a localização de um certo equipamento na grande rede. São exemplos de endereços IP: *110.27.99.3* e *200.17.94.197*.[8]

A estrutura da rede TCP/IP é feita para suportar diversas conexões, mas uma não dependerá exclusivamente da outra, ou seja, ela não é ligada em cascata ou série, mas sim com conexões independentes.

Para facilitar o uso da Internet, foram criados os domínios, que são associados aos números de IP com o objetivo de facilitar a memorização. Não seria fácil para as pessoas memorizarem seqüência de números como 110.27.99.3 e 200.17.94.17. Decorar vários números desses seria muito difícil e com isso a *Web* não teria o sucesso que tem hoje.

Possuir o seu próprio "domínio" é igual a ter um endereço postal onde as pessoas o localizam, a diferença é que será virtual, e poderá utilizar todos os serviços da rede como: "site", "e-mail", "ftp" entre outros. São exemplos de domínio: google.com e globo.com.

Na atual Internet a WWW ou *World Wide Web* é a estrutura arquitetônica que permite o acesso aos documentos vinculados e espalhados em milhares de máquinas conectadas à grande rede. Impende salientar que a WWW é uma das utilidades da Internet. Existem outros serviços a exemplo do FTP (protocolo de transferência de arquivos), SMTP (protocolo usado para enviar e-mails), entre outros.

---

[7] NUNES, Paulo. **Conceito de Internet**. Disponível em: <http://www.knoow.net/ciencinformtelec/informatica/internet.htm>. Acesso em: 2 out. 2011.
[8] ZANIOLO, 2007, p. 97.

As redes locais ou *Local Area Network* (LAN) como são conhecidas, são redes criadas entre computadores para facilitar e automatizar as tarefas atinentes entre eles. Sua utilização é bastante ampla, pois onde há mais de um computador surge a necessidade de se compartilhar recursos (arquivos, impressoras, Internet e etc.) entre eles.

Tanenbaum define Redes Locais:

> As redes locais, muitas vezes chamadas LANs, são redes privadas contidas em um único edifício ou campus universitário com até alguns quilômetros de extensão. Elas são amplamente usadas para conectar computadores pessoais e estações de trabalho em escritórios e instalações industriais de empresas, permitindo o compartilhamento de recursos (por exemplo, impressoras) e a troca de informações.[9]

Inúmeros são os conceitos relativos à Internet devido à sua enorme complexidade, porém, os ensinamentos aqui expostos podem ser considerados como o mínimo necessário para o entendimento do tema tratado no trabalho.

## 2.3. ASPECTOS JURÍDICOS

Através da Portaria Interministerial nº 147, de 31/05/1995, o Ministro de Estado das Comunicações e o Ministro de Estado da Ciência e Tecnologia, resolveram criar o Comitê Gestor de Internet do Brasil (CGI.br), para coordenar e integrar todas as iniciativas de serviços Internet no país, promovendo a qualidade técnica, a inovação e a disseminação dos serviços ofertados.[10]

As principais atribuições da CGI, para Corrêa, são: fomentar o desenvolvimento de serviços ligados à Internet em nível nacional; recomendar padrões e procedimentos técnicos e operacionais para a Internet no Brasil; coordenar a atribuição de endereços na Internet, registros de nomes de domínios e a interconexão sobre os serviços ligados à Internet e coletar, organizar e disseminar informações sobre os serviços ligados à Internet.[11]

---

[9] TANENBAUM, Andrew S. **Redes de Computadores**. São Paulo: Editora Campus, 2003, p. 29.
[10] BRASIL. Comitê Gestor da Internet no Brasil. Disponível em: <http://www.cgi.br/sobre-cg/definicao.htm>. Acesso em: 3 out. 2011.
[11] CORRÊA, 2000, p. 7.

Com isso, a atividade principal do CGI.br é manter grupos de trabalho, coordenando diversos projetos para o funcionamento e o desenvolvimento da Internet. São exemplos desses grupos o Registro.br e o CERT.br.

O Registro.br é o órgão responsável pela inscrição de *domain names*, sua administração e publicação do domínio ".br". Já o CERT.br – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil – cuida da segurança na Internet e realiza atividades de apoio a administradores de redes e usuários de Internet no país.

## 3. DOS CRIMES

A doutrina penal passou por muito tempo, até conseguir conceituar de modo coerente e homogêneo o que seria um delito cibernético, sendo este conceituada de forma abrangente como: ação típica, ilícita, cometida contra ou pela utilização de processamento automático de dados ou sua transmissão (ou seja, através da Internet).

Várias são as denominações utilizadas para a prática de delitos cometidos através da Internet: delitos computacionais, crimes de computador, crimes de informática, crimes informáticos, crimes eletrônicos, ciberdelitos, cibercrimes, crimes cibernéticos, entre outros.

Estes crimes podem ser classificados em puros (próprios) e impuros (impróprios). Os crimes puros ou próprios são aqueles que teriam como objeto de ataque um elemento informático, ou seja, dados e/ou sistemas informáticos. Neles, a informática (segurança dos sistemas, titularidade das informações e integridade dos dados, da maquina e periféricos) é o objeto jurídico tutelado. Já os crimes impuros ou impróprios são aqueles em que o agente se vale do computador como meio, ou seja, instrumento para produzir resultado naturalístico que ofenda o mundo físico ou o espaço "real", ameaçando ou lesando outros bens não-computacionais ou diversos da informática, como, por exemplo, pedofilia, tráfico de drogas e de pessoas, etc.[12]

Em relação aos crimes que podem vir a ser cometidos pela Internet, podemos fazer a seguinte separação:

a) Crimes genéricos – erro, negligência, omissão, conspiração, disputa civil.
b) Crimes contra o patrimônio – roubo, trapaça, plágio, espionagem.
c) Crimes contra a pessoa – pornografia, pedofilia, crimes raciais, preconceito, apologia ao suicídio, crimes contra a honra.
d) Crimes de propriedade intelectual – pirataria em geral, violação de dados e sistemas.
e) Crimes econômicos e financeiros – crimes que visam a obtenção de dinheiro por modo fraudulento e ilusório, como fraude e estelionato.

[12] FERREIRA, Érica Lourenço de Lima. **Criminalidade econômica, empresarial e cibernética:** o empresário como delinqüente econômico e os crimes cometidos através da Internet. Florianópolis: Momento Atual, 2004, p. 52.

Os criminosos cibernéticos, ou ciberdelinqüentes, foram batizados pela comunidade cibernética de *hackers, crackers* e *phreakers*.

Os primeiros são, em geral, simples invasores de sistemas, que atuam por espírito de emulação, desafiando seus próprios conhecimentos técnicos e a segurança de sistemas informatizados de grandes companhias e organizações governamentais. No início da cibercultura, eram tidos como heróis da revolução informática, porque teriam contribuído para o desenvolvimento da indústria do *software* e para o aperfeiçoamento dos computadores pessoais e da segurança dos sistemas informáticos.

Os *crackers*, por sua vez, são os "*hackers* aéticos". Invadem sistemas para adulterar programas e dados, furtar informações e valores e prejudicar pessoas. Praticam fraudes eletrônicas e derrubam redes informatizadas, causando prejuízos a vários usuários e à coletividade.

Por fim, os *phreakers* são especialistas em fraudar sistemas de telecomunicação, principalmente linhas telefônicas convencionais e celulares, fazendo uso desses meios gratuitamente ou às custas de terceiros.

Há ainda os *cyberpunks* e os *cyberterrorists*, que desenvolvem vírus de computador perigosos, como os *Trojan horses* (cavalos de Tróia) e as *Logic bombs*, com a finalidade de sabotar redes de computadores e em alguns casos propiciar a chamada *Denial of Service* (DoS), com a queda dos sistemas de grandes provedores, por exemplo, impossibilitando o acesso de usuários e causando prejuízos econômicos.

Diversos são os crimes que podem ser praticados através da Internet, contudo, alguns ocorrem com maior freqüência, merecendo destaque. Uma breve análise será feita acerca destes crimes mais comuns no universo virtual:[13]

a) Fraudes nos meios informáticos: a fraude ocorre quando o indivíduo ao comprar, vender ou investir via Internet é enganado de alguma forma. O vendedor pode descrever produtos ou serviços de maneira enganosa ou pode, ainda, receber o pedido e o dinheiro, mas não entregar o bem ao qual estava obrigado. As queixas mais freqüentes, no entanto, são casos de

[13] MARTINS, Renata Durval, et al. **Os delitos cibernéticos**. Disponível em: <http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=5381>. Acesso em: 12 out. 2011.

ofertas de cartões de créditos, oportunidades de negócios mirabolantes, entre outros.

b) Crime contra honra: são crimes de calúnia, injúria e difamação, presentes nos artigos 138 a 140 do código Penal. Podem ser cometidos através de salas de bate-papo, *homepage* e e-mail.

c) Acesso indevido/ ilegal/ não autorizado – *Hacking*: a violação de dados ou de sistemas é acesso não autorizado de alguém (hacker) a dados, programas e sistemas de natureza pessoal ou confidencial. Trata-se de um acesso a um determinado sistema por particular que tenha permissão insuficiente, ou usuário externo ao sistema, acessando-o sem permissão, ou quando o indivíduo acessa um banco de dados, sem autorização, por meio de um computador, conectado a uma rede, para destruir dados.

d) Envio de vírus: este tipo de conduta realizada pelo usuário tem como fundamental objetivo ocasionar o dano, mas para que esta prática seja configurada como crime é necessário que haja prejuízo econômico, pois havendo apenas uma destruição de e-mails sem muita importância, não se configura o crime.

## 4. LEGISLAÇÃO BRASILEIRA

O avanço tecnológico no Brasil e no mundo durante o século XX e início do século XXI é enorme. Já a legislação brasileira não avança tão rápido, de modo que o Congresso Nacional não consegue discutir e aprovar as leis com a necessária celeridade.

Não podemos dizer que nossa legislação é omissa em relação aos crimes cibernéticos, entretanto, ela possui várias lacunas, principalmente no que tange aos crimes puros ou próprios, em que as condutas perpetradas pelo agente são inéditas, fatos que nasceram na era digital. Nosso Código Penal data de 1940 e por motivos óbvios, não prevê tipos penais relacionados à informática. Apesar disso, muitas condutas praticadas com o uso do computador podem ser adequadas aos tipos previstos no Código Penal, resolvendo, assim, parte do problema da tipificação em relação aos crimes impróprios ou impuros.

Ocorre que nem sempre uma conduta irá se encaixar perfeitamente no tipo previsto na lei, como é o caso do envio de vírus, que como vimos, só cometerá o crime de dano previsto no artigo 163 do Código Penal o agente que causar prejuízo financeiro, deixando impune, assim, aquele que destruir apenas coisas sem muita importância, como e-mails.

Portanto, nem todas as práticas se enquadram perfeitamente no que já temos e, tendo em vista o princípio da legalidade, que norteia o Direito Penal pátrio, torna-se, muitas vezes, impossível uma punição pelos crimes cometidos em ambiente virtual.

A Constituição Federal por ser muito recente (promulgada em 1988) acaba por ser bem focada nos fatos atuais e é Lei maior que garante todas as garantias individuais dos cidadãos brasileiros. Nela, em seu artigo 5º, estão as garantias de individualidade, direitos e proteções que todos nós temos amparado, cumprindo destacar alguns de seus incisos pertinentes ao assunto:

> Art. 5º. Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:

> II - ninguém será obrigado a fazer ou deixar de fazer alguma coisa senão em virtude de lei;
> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;
> 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;
> XXXIX - não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal;

Para preencher as lacunas existentes no ordenamento, aos poucos, algumas leis vão sendo criadas ou alteradas com o intuito de acabar com a impunidade no meio cibernético, apesar de, atualmente, não se mostrarem suficientes para tal. Destacaremos alguns dispositivos que regulam o meio cibernético.

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

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

O art. 10 da Lei Federal n. 9.296/96, considera crime, punível com reclusão de 2 a 4 anos e multa, "realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo de Justiça, sem autorização judicial ou com objetivos não autorizados em lei".

A Lei n. 9472/97 (Lei Geral de Telecomunicações), tem como objetivo regulamentar os órgãos prestadores de serviços nas diversas áreas e modalidades que envolvam as Telecomunicações, e em seu artigo 60, define o que são os serviços de Comunicações:

> Art. 60. Serviço de telecomunicações é o conjunto de atividades que possibilita a oferta de telecomunicação.

> § 1° Telecomunicação é a transmissão, emissão ou recepção, por fio, radioeletricidade, meios ópticos ou qualquer outro processo eletromagnético, de símbolos, caracteres, sinais, escritos, imagens, sons ou informações de qualquer natureza.
> § 2° Estação de telecomunicações é o conjunto de equipamentos ou aparelhos, dispositivos e demais meios necessários à realização de telecomunicação, seus acessórios e periféricos, e, quando for o caso, as instalações que os abrigam e complementam, inclusive terminais portáteis.

O art. 153, §1º-A, do Código Penal, com a redação dada pela Lei Federal n. 9.983/2000, tipifica o crime de divulgação de segredo: "Divulgar, sem justa causa, informações sigilosas ou reservadas, assim definidas em lei, contidas ou não nos sistemas de informações ou banco de dados da Administração Pública", punindo-o com detenção de 1 a 4 anos, e multa.

O art. 313-B, do Código Penal, introduzido pela Lei n. 9.983/2000, tipificou o crime de modificação ou alteração não autorizada de sistema de informações, com a seguinte redação: "Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente", cominando-lhe pena de detenção, de 3 (três) meses a 2 (dois) anos, e multa.

O art. 325, §1º, incisos I e II, introduzidos pela Lei n. 9.983/2000, tipificaram novas formas de violação de sigilo funcional, nas condutas de quem "I – permite ou facilita, mediante atribuição, fornecimento e empréstimo de senha ou qualquer outra forma, o acesso de pessoas não autorizadas a sistemas de informações ou banco de dados da Administração Pública" e de quem "II – se utiliza, indevidamente, do acesso restrito", ambos sancionados com penas de detenção de 6 meses a 2 anos, ou multa.

O art. 12, *caput*, §§1º e 2º, da Lei Federal n. 9.609/98, tipifica o crime de violação de direitos de autor de programa de computador, punindo-o com detenção de 6 meses a 2 anos, ou multa; ou com pena de reclusão de 1 a 4 anos e multa, se o agente visa ao lucro.

O art. 72 da Lei n. 9.504/97, cuida de três tipos penais eletrônicos de natureza eleitoral:

> Art. 72. Constituem crimes, puníveis com reclusão, de cinco a dez anos:
> I - obter acesso a sistema de tratamento automático de dados usado pelo serviço eleitoral, a fim de alterar a apuração ou a contagem de votos;
> II - desenvolver ou introduzir comando, instrução, ou programa de computador capaz de destruir, apagar, eliminar, alterar, gravar ou transmitir dado, instrução ou programa ou provocar qualquer outro resultado diverso do esperado em sistema de tratamento automático de dados usados pelo serviço eleitoral;

> III - causar, propositadamente, dano físico ao equipamento usado na votação ou na totalização de votos ou a suas partes.

No Código de Processo Penal estão contidas as normas necessárias para que o Estado possa buscar os autores de delitos e regras para que o mesmo não aja com arbitrariedade, garantindo os direitos previstos na Constituição Federal. Um dos pontos mais importantes contidos no Código de Processo Penal e que envolverá diretamente o processo de apuração dos crimes cibernéticos é a Busca e Apreensão, prevista no artigo 240 do mesmo.

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

De acordo com Paiva:

> O projeto citado não apenas cria tipos penais novos, mas estende o campo de incidência de algumas figuras já previstas no CP para novos fenômenos ocorrentes nos meios desmaterializados, impossíveis de terem sido previstos pelo legislador de 1940, ano de edição do atual Código Penal, como pretende inserir ainda a Seção V no Capítulo VI do Título I do Código Penal, onde seriam definidos os crimes contra a inviolabilidade dos sistemas informatizados.[14]

A impunidade é um dos principais fatores para o grande aumento dos crimes cibernéticos no Brasil. Se aprovado o Projeto de Lei, a tendência é de que o número de crimes cibernéticos diminua, uma vez que a punição aos crimes será muito mais contundente que a atual.

Entretanto, uma legislação adequada não é só o bastante, deve-se também aperfeiçoar os meios técnicos de investigação como também treinamento para capacitação das pessoas que trabalham nesse meio, práticas também importantes para uma boa solução de casos dessa natureza, assim como a conscientização de

[14] PAIVA, Luciano Carneiro de. **A prova nos crimes de informática**. Aspectos Técnicos e Jurídicos. Dissertação, 2006, p. 7.

usuários dos computadores e acordo entre esferas judiciais diferentes para abertura de dados e sistemas, apenas desse modo é que se pode ter um instrumento realmente eficaz de combate às práticas criminosas virtuais.

## 5. ASPECTOS QUE DIFICULTAM A IDENTIFICAÇÃO DE AUTORIA

Ao contrário do mundo "real", no ciberespaço o exame da identidade e a autenticação desta não podem ser feitos visualmente, ou pela verificação de documentos ou de elementos identificadores já em si evidentes, como, por exemplo, placas de veículos ou a aparência física.

Quando um indivíduo está conectado na rede, são-lhe necessários dois elementos identificadores: o endereço da máquina que envia as informações à Internet e o endereço da máquina que recebe tais dados. Esses endereços são os já citados *IP (Internet Protocol)*, sendo representados por números, onde não revelam nada sobre o usuário da Internet e muito pouco sobre os dados que estão sendo transmitidos.

No que se refere à atribuição da autoria do documento, mensagem ou da conduta ilícita, os problemas processuais persistem, porque, salvo quando o usuário do computador faça uso de uma assinatura digital, dificilmente se poderá determinar quem praticou determinada conduta. A assinatura digital confere credendidade ao documento ou mensagem, permitindo que se presuma que determinado indivíduo foi o autor da conduta investigada. Mas o problema reside exatamente aí, pois, para o Direito Penal, não servem presunções, ainda mais quando se admite a possibilidade de condenação.

Há mecanismos que somente validam acesso mediante a verificação de dados biométricos do indivíduo. Sem isso a entrada no sistema é vedada. As formas mais comuns são a análise do fundo do olho do usuário ou a leitura eletrônica de impressão digital, ou, ainda, a análise da voz do usuário.

Com isso, somente os mecanismos de assinatura eletrônica e certificação digital e de análise biométrica podem conferir algum grau de certeza quanto à autoria da mensagem, da informação, ou da transmissão, se considerado o problema no prisma penal.

Existe, porém, o acesso público da Internet onde não há registro dos usuários, como *cyber cafés*, *lan houses*, universidades e escolas, telecentros, e outros. Geralmente, estes locais não possuem registros de seus usuários, inviabilizando, assim, a identificação de autoria de eventual crime.

Portanto, podemos dizer que a falta de vinculação do usuário ao computador que acessou a Internet é o grande entrave na identificação da autoria de delitos cometidos através dela.

Para tentar impedir a falta de identificação de usuários na Internet, uma legislação Estadual, no Estado de São Paulo, com a Lei nº 12.228, de 11 de janeiro de 2006, impõe aos estabelecimentos comerciais que forneçam conexão à Internet, o registro de seus usuários:

> LEI Nº 12.228, DE 11 DE JANEIRO DE 2006.
> Dispõe sobre os estabelecimentos comerciais que colocam a disposição, mediante locação, computadores e máquinas para acesso à internet e dá outras providências.
> Artigo 1º - São regidos por esta lei os estabelecimentos comerciais instalados no Estado de São Paulo que ofertam a locação de computadores e máquinas para acesso à internet, utilização de programas e de jogos eletrônicos, abrangendo os designados como "lan houses", cibercafés e "cyber offices", entre outros.
> Artigo 2º - Os estabelecimentos de que trata esta lei ficam obrigados a criar e manter cadastro atualizado de seus usuários, contendo:
> I - nome completo;
> II - data de nascimento;
> III - endereço completo;
> IV - telefone;
> V - número de documento de identidade.
> § 1º - O responsável pelo estabelecimento deverá exigir dos interessados a exibição de documento de identidade, no ato de seu cadastramento e sempre que forem fazer uso de computador ou máquina.
> § 2º - O estabelecimento deverá registrar a hora inicial e final de cada acesso, com a identificação do usuário e do equipamento por ele utilizado.
> § 3º - Os estabelecimentos não permitirão o uso dos computadores ou máquinas:
> 1. a pessoas que não fornecerem os dados previstos neste artigo, ou o fizerem de forma incompleta;
> 2. a pessoas que não portarem documento de identidade, ou se negarem a exibi-lo;
> § 4º - As informações e o registro previstos neste artigo deverão ser mantidos por, no mínimo, 60 (sessenta) meses.
> § 5º - Os dados poderão ser armazenados em meio eletrônico.
> § 6º - O fornecimento dos dados cadastrais e demais informações de que trata este artigo só poderá ser feito mediante ordem ou autorização judicial.
> § 7º - Excetuada a hipótese prevista no § 6º, é vedada a divulgação dos dados cadastrais e demais informações de que trata este artigo, salvo se houver expressa autorização do usuário.[15]

[15] ESTADO DE SÃO PAULO. **Lei nº 12.228, de 11 de janeiro de 2006**. Dispõe sobre os estabelecimentos comerciais que colocam a disposição, mediante locação, computadores e máquinas para acesso à Internet e dá outras providências. Disponível em: <http://www.al.sp.gov.br/repositorio/legislacao/lei/2006/lei%20n.12.228,%20de%2011.01.2006.htm>. Acesso em: 23 out. 2011.

Outrossim, em nível nacional, cumpre transcrever o art. 22 do já citado Projeto de Lei substitutivo dos Projetos - PLS nº 76 de 2000, PLS nº 137 de 2000 e PLC nº 89 de 2003, que prescreve:

> Art. 22. O responsável pelo provimento de acesso à rede de computadores mundial, comercial ou do setor público é obrigado a:
> I – manter em ambiente controlado e de segurança, pelo prazo de 3 (três) anos, com o objetivo de provimento de investigação pública formalizada, os dados de endereçamento eletrônico da origem, hora, data e a referência GMT da conexão efetuada por meio de rede de computadores e fornecê-los exclusivamente à autoridade investigatória mediante prévia requisição judicial;
> II – preservar imediatamente, após requisição judicial, outras informações requisitadas em curso de investigação, respondendo civil e penalmente pela sua absoluta confidencialidade e inviolabilidade;
> III – informar, de maneira sigilosa, à autoridade competente, denúncia que tenha recebido e que contenha indícios da prática de crime sujeito a acionamento penal público incondicionado, cuja perpetração haja ocorrido no âmbito da rede de computadores sob sua responsabilidade.[16]

Por fim cite-se os denominados *proxy* de ponte, em que o usuário se utiliza de um servidor *proxy* para navegar anonimamente, ou melhor, dificultar a identificação do IP da máquina que acessou.

Diante do avanço tecnológico é inegável que novos instrumentos sejam desenvolvidos no sentido permitir, a cada momento da escalada de seu progresso, que se afira de forma mais segura a autoria e a materialidade. Entretanto, ao revés, o mesmo desenvolvimento poderá oportunizar ao autor do delito estudado outras formas de ocultar a autoria ou mesmo mascará-la, bem como dificultar a comprovação da materialidade.

[16] BRASIL .Senado Federal. **substitutivo ao PLS 76/2000, PLS 137/2000 e PLC 89/2003**. Disponível em: <http://legis.senado.gov.br/mate-pdf/13674.pdf>. Acesso em: 23 out. 2011.

## 6. CONCLUSÃO

A análise histórica da Internet mostrou que este importante e valioso espaço de disponibilização de informações revolucionou o cotidiano da sociedade alterando hábitos e costumes, porém também trouxe as condutas criminosas cometidas com o uso das tecnologias de informação, os chamados crimes cibernéticos.

Os avanços tecnológicos da Internet apresentam dois aspectos: um positivo, onde a tecnologia combinou comportamentos tradicionais com velocidade, cultura e acesso à informação. No outro aspecto, existe um campo negativo ligado às modernas tecnologias, um rico campo para as mais variadas atividades ilícitas.

A Rede Mundial de Computadores, esta nova sociedade virtual, acaba por ser apenas mais um meio para a realização de condutas criminosas. Faz-se necessário reconhecer que a informática permite não só o cometimento de novos delitos, como potencializa alguns outros tradicionais.

O avanço tecnológico é enorme, enquanto a legislação brasileira não avança tão rápido, de modo que o Congresso Nacional não consegue discutir e aprovar as leis com a necessária celeridade.

Apesar de já existirem algumas leis que versam sobre o tema, elas não são suficientes, necessitando-se novas leis para preencher as lacunas existentes. O Projeto de Lei substitutivo dos Projetos - PLS nº 76 de 2000, PLS nº 137 de 2000 e PLC nº 89 de 2003 não resolve por completo o problema das lacunas, mas trata-se de um grande avanço para o Direito brasileiro.

A dificuldade em determinar a autoria dos crimes cibernéticos é um importante fator para o aumento da criminalidade neste meio. Foram constatados alguns problemas quanto à identificação de autoria, como o controle remoto de computador, por meio de invasão; o acesso público da Internet onde não há registro dos usuários, como *cyber* cafés, *lan houses*, universidades e escolas, telecentros; acesso sem fio (*wireless*) aberto, em que os usuários não são identificados; e os denominados *proxy* de ponte, em que o usuário utiliza-se de um servidor para dificultar a identificação do IP da máquina e origem.

Para tentar impedir a falta de identificação de usuários na Internet, podemos citar a lei estadual nº 12.228/06, do estado de São Paulo, e, em nível nacional, o

Projeto de Lei substitutivo dos Projetos - PLS nº 76 de 2000, PLS nº 137 de 2000 e PLC nº 89 de 2003.

O combate aos crimes cibernéticos depende estritamente da excelente relação entre a justiça e as empresas privadas de todos os países, de policiais e agentes políticos especializados, jurídica e tecnicamente, para o tratamento dessas questões.

## BIBLIOGRAFIA

BRASIL, 1995, Nota Conjunta. Ministério das Comunicações e Ministério da Ciência e Tecnologia. Disponível em: <http://www.cgi.br/regulamentacao/notas.htm>. Acesso em: 18 set. 2011.

BRASIL. Comitê Gestor da Internet no Brasil. **Sobre o CGI.br: definição**. Disponível em: <http://www.cgi.br/sobre-cg/definicao.htm>. Acesso em: 3 out. 2011.

BRASIL. Comitê Gestor da Internet no Brasil. **Sobre o CGI.br**: **histórico**. Disponível em: <http://www.cgi.br/sobre-cg/historia.htm>. Acesso em: 18 set. 2011.

BRASIL .Senado Federal. **substitutivo ao PLS 76/2000, PLS 137/2000 e PLC 89/2003**. Disponível em: <http://legis.senado.gov.br/mate-pdf/13674.pdf>. Acesso em: 23 out. 2011.

CENTRAL INTELLIGENCE AGENCY. **World factbook: internet users**. Disponível em: <https://www.cia.gov/library/publications/theworldfactbook/rankorder/2153rank.html>. Acesso em: 30 ago. 2011.

CERT.br. **Estatísticas do CERT.br**. Disponível em: <http://www.cert.br/stats/incidentes>. Acesso em: 5 nov. 2011.

CORRÊA, Gustavo Testa. **Aspectos jurídicos da Internet**. São Paulo: Saraiva, 2000.

ESTADO DE SÃO PAULO. **Lei nº 12.228, de 11 de janeiro de 2006**. Dispõe sobre os estabelecimentos comerciais que colocam a disposição, mediante locação, computadores e máquinas para acesso à Internet e dá outras providências. Disponível em:

<http://www.al.sp.gov.br/repositorio/legislacao/lei/2006/lei%20n.12.228,%20de%2011.01.2006.htm>. Acesso em: 23 out. 2011.

FERREIRA, Érica Lourenço de Lima. **Criminalidade econômica, empresarial e cibernética:** o empresário como delinqüente econômico e os crimes cometidos através da Internet. Florianópolis: Momento Atual, 2004.

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

MARTINS, Renata Durval, et al. **Os delitos cibernéticos**. Disponível em: <http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=5381>. Acesso em: 12 out. 2011.

NUNES, Paulo. **Conceito de Internet**. Disponível em: <http://www.knoow.net/ciencinformtelec/informatica/internet.htm>. Acesso em: 2 out. 2011.

PAIVA, Luciano Carneiro de. **A prova nos crimes de informática**. Aspectos Técnicos e Jurídicos. Dissertação, 2006.

SANTOS, Coriolano Aurélio de Almeida Camargo. **ATUAL CENÁRIO DOS CRIMES CIBERNÉTICOS NO BRASIL**. Disponível em: <http://www2.oabsp.org.br/asp/comissoes/sociedade_informacao/artigos/crimes_ciberneticos.pdf>. Acesso em: 15 set. 2011.

TANENBAUM, Andrew S. **Redes de Computadores**. São Paulo: Editora Campus, 2003.

ZANIOLO, Pedro Augusto. **Crimes modernos**: o impacto da tecnologia no direito. Curitiba: Juruá, 2007.

## ANEXO – SUBSTITUTIVO AO PROJETO DE LEI DA CÂMARA Nº 89/2003

### COMISSÃO DIRETORA PARECER Nº 657, DE 2008

Redação final do Substitutivo do Senado ao Projeto de Lei da Câmara nº 89, de 2003 (nº 84, de 1999, na Casa de origem).

A **Comissão Diretora** apresenta a redação final do Substitutivo do Senado ao Projeto de Lei da Câmara nº 89, de 2003 (nº 84, de 1999, na Casa de origem)., que *altera o Decreto-Lei nº 2848, de 07 de dezembro de 1940 - Código Penal e a Lei nº 9296, de 24 de julho de 1996, e dá outras providências. (Dispõe sobre os crimes cometidos na área de informática, e suas penalidades, dispondo que o acesso de terceiros, não autorizados pelos respectivos interessados, a informações privadas mantidas em redes de computadores, dependerá de prévia autorização judicial)*, consolidando as Emendas aprovadas pelo Plenário no turno suplementar.

Sala de Reuniões da Comissão, em 9 de julho de 2008.

**ANEXO AO PARECER Nº 657, DE 2008.**

Redação final do Substitutivo do Senado ao Projeto de Lei da Câmara nº 89, de 2003 (nº 84, de 1999, na Casa de origem).

Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), o Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar), a Lei nº 7.716, de 5 de janeiro de 1989, a Lei nº 8.069, de 13 de julho de 1990, e a Lei nº 10.446, de 8 de maio de 2002, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, de rede de computadores, ou que sejam praticadas contra dispositivos de comunicação ou sistemas informatizados e similares, e dá outras providências.

O CONGRESSO NACIONAL decreta:

Art. 1º Esta Lei altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), o Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar), a Lei nº 7.716, de 5 de janeiro de 1989, a Lei nº 8.069, de 13 de julho de 1990, e a Lei nº 10.446, de 8 de maio de 2002, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, de rede de computadores, ou que sejam praticadas contra dispositivos de comunicação ou sistemas informatizados e similares, e dá outras providências.

Art. 2º O Título VIII da Parte Especial do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal) fica acrescido do Capítulo IV, com a seguinte redação:

"CAPÍTULO IV
DOS CRIMES CONTRA A SEGURANÇA
DOS SISTEMAS INFORMATIZADOS

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

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

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

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

**Obtenção, transferência ou fornecimento não autorizado de dado ou informação**

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

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

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

**Ação Penal**

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

Art. 3º O Título I da Parte Especial do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal) fica acrescido do seguinte artigo, com a seguinte redação: "**Divulgação ou utilização indevida de informações e dados pessoais**

Art. 154-A. Divulgar, utilizar, comercializar ou disponibilizar dados e informações pessoais contidas em sistema informatizado com finalidade distinta da

que motivou seu registro, salvo nos casos previstos em lei ou mediante expressa anuência da pessoa a que se referem, ou de seu representante legal:

Pena – detenção, de 1 (um) a 2 (dois) anos, e multa.

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

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

"**Dano**

Art. 163. Destruir, inutilizar ou deteriorar coisa alheia ou dado eletrônico alheio:

....." (NR)

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

"**Inserção ou difusão de código malicioso**

Art. 163-A. Inserir ou difundir código malicioso em dispositivo de comunicação, rede de computadores, ou sistema informatizado:

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

**Inserção ou difusão de código malicioso seguido de dano**

§ 1º Se do crime resulta destruição, inutilização, deterioração, alteração, 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.

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

Art. 6º O art. 171 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal) passa a vigorar acrescido dos seguintes dispositivos:

"Art. 171. .....

.....

§ 2º Nas mesmas penas incorre quem:

.....

**Estelionato Eletrônico**

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

§ 3º Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime previsto no inciso VII do § 2º, a pena é aumentada de sexta parte." (NR)

Art. 7º Os arts. 265 e 266 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal) passam a vigorar com as seguintes redações:

"**Atentado contra a segurança de serviço de utilidade pública**

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

....." (NR)

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

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

....." (NR)

Art. 8º O *caput* do art. 297 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal) passa a vigorar com a seguinte redação:

"**Falsificação de dado eletrônico ou documento público**

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

....." (NR)

Art. 9º O *caput* do art. 298 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal) passa a vigorar com a seguinte redação:

"**Falsificação de dado eletrônico ou documento particular**

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

....." (NR)

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

"Art. 251. .....

§ 1º Nas mesmas penas incorre quem:

.....

**Estelionato Eletrônico**

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

.....

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

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

"**Dano Simples**

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

....." (NR)

"**Dano em material ou aparelhamento de guerra ou dado eletrônico**

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

....." (NR)

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

"**Inserção ou difusão de código malicioso**

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

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

**Inserção ou difusão de código malicioso seguido de dano**

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

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

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

Art. 13. O Título VII da Parte Especial do Livro I do Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar), fica acrescido do Capítulo VIII, com a seguinte redação:

"CAPÍTULO VIII

DOS CRIMES CONTRA A SEGURANÇA DOS SISTEMAS INFORMATIZADOS

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

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

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

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

**Obtenção, transferência ou fornecimento não autorizado de dado ou informação**

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

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

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

**Divulgação ou utilização indevida de informações e dados pessoais**

Art. 339-C. Divulgar, utilizar, comercializar ou disponibilizar dados e informações pessoais contidas em sistema informatizado sob administração militar com finalidade distinta da que motivou seu registro, salvo nos casos previstos em lei

ou mediante expressa anuência da pessoa a que se referem, ou de seu representante legal:

Pena – detenção, de 1 (um) a 2 (dois) anos, e multa.

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

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

"**Falsificação de documento**

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

....." (NR)

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

"CAPÍTULO I

DA TRAIÇÃO

**Favor ao inimigo**

Art. 356. .....

.....

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

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

....." (NR)

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

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

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

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

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

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

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

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

Art. 18. Os órgãos da polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado.

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

"Art. 20 .....

.....

§ 3º.....

.....

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

....." (NR)

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

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

....." (NR)

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

"Art. 1º .....

.....

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

....." (NR)

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

I – manter em ambiente controlado e de segurança, pelo prazo de 3 (três) anos, com o objetivo de provimento de investigação pública formalizada, os dados de endereçamento eletrônico da origem, hora, data e a referência GMT da conexão efetuada por meio de rede de computadores e fornecê-los exclusivamente à autoridade investigatória mediante prévia requisição judicial;

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

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

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

§ 2º O responsável citado no *caput* deste artigo, independentemente do ressarcimento por perdas e danos ao lesado, estará sujeito ao pagamento de multa variável de R$ 2.000,00 (dois mil reais) a R$ 100.000,00 (cem mil reais) a cada

requisição, aplicada em dobro em caso de reincidência, que será imposta pela autoridade judicial desatendida, considerando-se a natureza, a gravidade e o prejuízo resultante da infração, assegurada a oportunidade de ampla defesa e contraditório.

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

Art. 23. Esta Lei entra em vigor 120 (cento e vinte) dias após a data de sua publicação.