A TUTELA PENAL DOS *CYBERCRIMES* E O PROJETO DE LEI CONTRA OS CRIMES DE INFORMÁTICA*

José de Castro Meira Júnior

INTRODUÇÃO

Não há, nos dias atuais, quem imagine a vida sem o computador. Por mais que se diga que, antes de sua invenção, a vida funcionava perfeitamente sem a utilização do aparato, hoje, ninguém duvida que o computador é essencial para todos. É empregado para as mais diversas tarefas: trabalho, estudo, bate-papo e lazer.

Após a criação do computador, veio a Internet, a rede mundial de computadores, que promoveu uma verdadeira revolução nos conceitos de comunicação, educação, cultura e economia.

O baixo custo do acesso cobrado dos provedores ajuda na disseminação de informações e trocas de experiências. Por meio de suas redes interconectadas, podem-se fazer amigos, pesquisas escolares e profissionais – como jurisprudência, por exemplo – e até compras nos sítios (chamados *sites*) especializados.

Para Alberto Zacharias Toron, a definição mais simples e compreensível de Internet foi dada por Laquey Parker, para quem ela "é um amálgama de milhares de redes de computadores que conectam entre si a milhões de pessoas".[1]

A Rede Mundial surgiu da tecnologia militar dos Estados Unidos, na época da Guerra Fria, com o intuito de se tornar uma rede de telecomunicações o menos vulnerável possível a um ataque soviético.

Com a liberdade que dá aos usuários, juntamente com a permissão de tudo realizar ao redor do mundo sem que sua identidade seja revelada, a rede trouxe um tipo diferente de infrator. Vários tipos de delitos podem ser cometidos pelo computador, quais sejam: fraude, pornografia infantil, lavagem de dinheiro, sabotagem, vandalismo, entre outros tantos.

---

[1]TORON, Alberto Zacharias. Crimes na *Internet*. *Repertório de Jurisprudência,* nº 22, 3º Caderno. São Paulo: IOB, 2000, p. 476.

Ao Direito não é dado ficar silente às inovações das relações humanas. É inegável a transformação gerada na coletividade pelo avanço tecnológico. Não se pode olvidar da existência de uma verdadeira comunidade virtual e, portanto, faz-se necessário estudo jurídico a fim de acompanhar as novas formas de conviver em sociedade e adaptar-se a elas.

Túlio Vianna aponta semelhanças entre leis e programas de computador. Para ele, "ambos são mecanismos de controle. As leis visam ao controle da sociedade e os programas, ao controle das máquinas."[2] E, se o direito é o meio de controle social por excelência e *ubi societas ib jus*, impõe-se uma resposta imediata a esse fenômeno chamado informática.

A própria justiça rendeu-se aos amplos benefícios da rede de computadores, tanto que o Presidente Luís Inácio Lula da Silva sancionou, há pouco tempo, a Lei n. 11.419, de 19 de dezembro de 2006, que dispõe sobre a informatização do processo judicial e, logo no seu artigo 1º, determina que "o uso de meio eletrônico na tramitação de processos judiciais, comunicação de atos e transmissão de peças processuais será admitido nos termos desta Lei", com aplicação indistinta aos processos civis, penais e trabalhistas, além dos juizados especiais, em qualquer grau de jurisdição.

A freqüência da criminalidade por computador e suas drásticas conseqüências ensejaram, aliados à importância dos bens jurídicos em jogo, a iniciativa da escolha da temática da presente monografia.

O presente trabalho tem como objetivo examinar o direito de forma dogmático-normativa, por meio do estudo dos dispositivos já existentes acerca do tema, além de dar enfoque ao Projeto de Lei n. 84/99, de relatoria originária do Deputado Luiz Piauhylino, aprovado pela Câmara dos Deputados e atualmente em tramitação no Senado Federal, onde recebeu nova numeração (PLC 89/2003).

O capítulo inicial procura situar o leitor no assunto a ser tratado com mais vagar nos tópicos seguintes. Limita-se a apresentar um esboço histórico da cibernética e também da Internet, tendo em vista que, entre as redes existentes, ela é a preferida dos

---

[2]VIANNA, Túlio. *Fundamentos de Direito Penal Informático.* Rio de Janeiro: Forense, 2003, p. 11.

usuários e dos criminosos virtuais. Na seqüência, enumeram-se diversos conceitos de informática e Internet pesquisados nos mais diferentes autores.

O segundo capítulo tem o intuito de delimitar o tema comentado. Explica o crime cibernético em seus pormenores, desde o próprio conceito de crime em geral até o esgotamento do delito informático, analisando conceito, características, classificações e sujeito ativo. Ao final, comenta-se a Convenção do Conselho da Europa sobre crimes cibernéticos, realizada em Budapeste, o que demonstra a preocupação mundial com o tema.

O último capítulo analisa os aspectos legais para uma nova legislação sobre *cybercrimes*, o princípio da reserva legal, basilar em Direito de repressão, e traz, ainda, a atual discussão na doutrina relativamente à necessidade da elaboração de um novo diploma legal, pois há quem defenda que o Código Penal de hoje é suficiente em si mesmo. Empós, há comentário sobre as novidades trazidas pelo Projeto de Lei n. 84/99, cuja aprovação pretende-se no Congresso Nacional.

Finalizadas as análises a respeito dos crimes cibernéticos, faz-se conclusão de todo o exposto na presente monografia, na esperança da aprovação *in totum* do projeto comentado ao longo do texto.

CAPÍTULO I - INFORMÁTICA E INTERNET

1 BREVE ESBOÇO HISTÓRICO

A comunicação é uma necessidade do ser humano desde os tempos primitivos. Na Idade da Pedra, os homens procuravam-se fazer entender por meio de sons guturais, desenhos rupestres, hieróglifos e sinais. Tais veículos de comunicação podem ser catalogados como os primeiros passos da história da comunicação.

"Computar" é sinônimo de contar, calcular, orçar. A palavra foi-nos legada do latim *computare*. Segundo o Dicionário Etimológico Nova Fronteira, de Antônio Geraldo da Cunha, a palavra "computação" vem sendo usada desde o século XVI, enquanto

"computador" é vocábulo que vem sendo usado desde 1813. Daí por que a Enciclopédia Mirador Internacional assim conceitua: "Computadores são máquinas capazes de realizar várias operações matemáticas em curto espaço de tempo, de acordo com os programas previamente estabelecidos".[3]

Os computadores como conhecemos tiveram origem no ábaco criado na região hoje conhecida como China, por volta de 3.500 a.C. No Oriente Médio, tábuas de argila foram encontradas por arqueólogos, as quais continham cálculos matemáticos e tabuadas de multiplicação. Afirma-se que teriam sido criadas por volta de 1.700 a.C.[4]

Em 1617, John Naiper criou bastões que serviam para computação de dados e eram conhecidos como "Bastões de Naiper"[5] ou "Tábua de Naiper".[6] Em 1642, Blaise Pascal criou a Máquina Aritmética, tal como a máquina calculadora por nós conhecida hoje em dia. Já nos idos de 1822, Charles Babbage criou o projeto da Máquina Analítica.[7]

Na seqüência, apareceu a máquina de tear comandada por cartões perfurados construída pelo francês Jacquard, em 1801, que inspirou a máquina construída por Herman Hollerit, preocupado com o trabalho que executava no Departamento de Estatística dos Estados Unidos, na apuração do recenseamento.

> Sua máquina permitiu reduzir a apuração do censo de 1890 para apenas um ano, com apenas 43 funcionários, enquanto tarefa similar, quanto ao censo de 1880, consumiu 7 anos, com 500 funcionários. Hollerit é homenageado inconscientemente quando seu nome é tomado de empréstimo para referir-se aos contracheques de pagamento, sobretudo no âmbito das empresas.[8]

---

[3]MEIRA, José de Castro. *Crimes de Informática.* Disponível em: <http://buscalegis.ccj.ufsc.br/arquivos/crimes_informatica_meira.html>. Acesso em: 12. out. 2006.
[4]ROSSINI, Augusto. *Informática, Telemática e Direito Penal.* São Paulo: Memória Jurídica Editora, 2004, p. 23.
[5]ROSSINI, Augusto. *Informática, Telemática e Direito Penal.* São Paulo: Memória Jurídica Editora, 2004, p. 23.
[6]SILVA, Rita de Cássia Lopes da. *Direito Penal e Sistema Informático*. São Paulo: Revista dos Tribunais, 2003, p. 16.
[7]ROSSINI, Augusto. *Informática, Telemática e Direito Penal.* São Paulo: Memória Jurídica Editora, 2004, p. 24. Para Silva, foi em 1835. In: SILVA, Rita de Cássia Lopes da. *Direito Penal e Sistema Informático*. São Paulo: Revista dos Tribunais, 2003, p. 16.
[8]MEIRA, José de Castro. *Crimes de Informática.* Disponível em: <http://buscalegis.ccj.ufsc.br/arquivos/crimes_informatica_meira.html>. Acesso em: 12. out. 2006. p. 2.

Rita de Cássia Lopes da Silva[9] explica que a evolução do computador teve de passar por cinco gerações para chegar ao que conhecemos hoje como PC (*personal computer*).

O primeiro computador eletrônico de grande porte foi desenvolvido, entre 1934 e 1946, em laboratórios universitários, nos Estados Unidos, na Universidade da Pensilvânia, para resolver problemas balísticos. Era chamado inicialmente de Eniac – *Electronic, Numeric, Integrator and Calculator.*

Após o Eniac, surgiu o Edvac – *Electronic Discrete Variable Automatic Computer*, modelo experimental, que armazenava o programa, de forma codificada, na memória do computador. A primeira geração de computadores teve início no início da década de 50, como *Universal Automatic Computer* I, que utilizava válvulas eletrônicas em seu funcionamento.

No final da mesma década, surge a segunda geração, que apresenta transistores em lugar das válvulas. Essa passagem foi bastante importante para a popularização e o desenvolvimento da informática.

A terceira geração apareceu em meados dos anos 60 e passou a usar circuitos integrados. A geração seguinte de computadores caracterizou-se pela maior capacidade de armazenamento de informações, rapidez e precisão no desenvolvimento do processamento de dados, chamados de microcomputadores e *mainframe* (computadores de grande porte).

A quinta e atual geração de computadores caracteriza-se pela simplificação e pela miniaturização do computador (a chegada dos chamados *laptops* ou *noteboks*), além de ter capacidade de armazenamento gigantesca e facilidade em seu uso, tanto que, hoje, crianças são capazes de manusear um computador sem a necessidade da orientação de um adulto.

---

[9]SILVA, Rita de Cássia Lopes da. *Direito Penal e Sistema Informático.* São Paulo: Revista dos Tribunais, 2003, p. 17-19.

A Internet, como conhecemos hoje, surgiu do desenvolvimento contínuo das redes de computadores.

Teve início na década de 60, nos Estados Unidos, com fins exclusivos bélicos, na época da Guerra Fria, e consistia em "um sistema de comunicação de computadores, visando a garantir, no caso de uma guerra nuclear, o mínimo de controle sobre as instituições e garantir a possibilidade de coordenar um contra-ataque eficaz contra o inimigo de então, a União Soviética".[10]

Essa rede resultou num sistema descentralizado de máquinas que permitia o funcionamento das outras bases, caso uma delas fosse atacada. Havia, à época, apenas quatro servidores, na Universidade da Califórnia, em Los Angeles, em Stanford, na Universidade da Califórnia, em Santa Bárbara, e na Universidade de Utah.

O programa foi desenvolvido pela empresa Arpa (*Advanced Research and Projects Agency*) e, em 1969, "tinha o objectivo de conectar as bases militares e os departamentos de pesquisa do governo americano. Esta rede teve o seu berço dentro do Pentágono e foi batizada com o nome de Arpanet".[11] Em 1971, a rede abrangeu agências governamentais e militares, inclusive a Nasa. No ano seguinte, lançou-se o primeiro programa de correio eletrônico (*e-mail*), e, em 1973, foram estabelecidas as primeiras conexões internacionais, interligando Estados unidos, Inglaterra e Noruega.[12]

Dez anos mais tarde, criou-se a Usenet (do inglês *Unix User Network*) que se tratava de:

> um meio de comunicação onde usuários postam mensagens de texto (chamadas de "artigos") em fóruns que são agrupados por assunto (chamados de *newsgroups*). Ao contrário das mensagens de *e-mail*, que são transmitidas quase que diretamente do remetente para o destinatário,

[10]RAHAL, Flávia; GARCIA, Roberto Soares. Crimes e Internet – Breves Notas aos Crimes Praticados por Meio da Rede Mundial e Outras Considerações. *Boletim IBCCrim,* ano 9, n. 110, São Paulo: IBCCrim, 2002, p. 8.
[11]Disponível em: <http://pt.wikipedia.org/wiki/arpanet>.
[12]ROSSINI, Augusto. *Informática, Telemática e Direito Penal.* São Paulo: Memória Jurídica Editora, 2004, p. 27-28.

> os artigos postados nos *newsgroups* são retransmitidos através de uma extensa rede de servidores interligados.[13]

Em 1985, surgiram os primeiros domínios de rede: edu (vinculado à educação), gov (relacionados a pessoas jurídicas de direito público) e org (ligado às empresas e às organizações). A partir daí, a rede começou a ser chamada de Internet, contendo várias conexões internacionais.

Em 1990, o Departamento de Defesa dos EUA desativou a empresa Arpanet e a substituiu pela NSFNET. Nesse mesmo ano, o Brasil foi conectado à nova empresa juntamente com Argentina, Chile, Índia, entre outros países.

Finalmente, em 1992, foi criada a *World Wide Web* (www) – ou "rede de alcance mundial" na tradução literal – que consiste em:

> uma rede de computadores na Internet que fornece informação em forma de hipermídia, como vídeos, sons, hipertextos e figuras. Para ver a informação, pode-se usar um *software* chamado navegador (*browser*) para descarregar informações (chamadas "documentos" ou "páginas") de servidores de Internet (ou "*sites*") e mostrá-los na tela do usuário. O usuário pode então seguir os *links* na página para outros documentos ou mesmo enviar informações de volta para o servidor para interagir com ele. O ato de seguir *links* é comumente chamado de "navegar" ou "surfar" na *Web*.[14]

Atualmente, existem aproximadamente 450.000.000 (quatrocentos e cinqüenta milhões) de computadores conectados à rede mundial em caráter permanente, segundo o sítio da Internet *System Consortium,*[15]e, por esse motivo, merece atenção especial da comunidade jurídica.

2 CONCEITO DE INFORMÁTICA E INTERNET

[13]Disponível em: <http://pt.wikipedia.org/wiki/Usenet.>.
[14]Disponível em: <http://pt.wikipedia.org/wiki/World_Wide_Web.>.
[15]Disponível em: <http://www.isc.org/index.pl?/ops/ds/.>.

Importante se faz definir os termos dos objetos do estudo que serão detalhados mais adiante.

O Dicionário Houaiss define informática como o ramo do conhecimento dedicado ao tratamento da informação mediante o uso de computadores e demais dispositivos de processamento de dados. Significa dizer que informática é a disciplina que faz o tratamento racional e sistemático da informação por meios automáticos. A informática existe em função do computador, uma vez que o manuseamento das informações é conseguido por meio dele.

Em termos técnicos, entende-se por informática o tratamento automático da informação, empregando computadores eletrônicos e tendo como base a informação resultante da evolução do conceito de documentação suportada pela teoria da informação.[16]

Outra definição é dada por Rui Moreira, para quem é opinião mais ou menos generalizada de que a informática é uma ciência cujo objeto de estudo relaciona-se com o tratamento lógico de conjuntos de dados, lançando mão de técnicas e equipamentos que possibilitam o seu processamento de modo a obter informação que depois poderá ser armazenada e/ou transmitida.[17]

A palavra "informática" foi um neologismo criado por Phillippe Dreyfus em 1962 e surgiu da contração das palavras "informação" e "automática" para designar as disciplinas que versam o tratamento automático da informação.

Já o conceito de Internet nos é dado pelo Dicionário Eletrônico Houaiss da Língua Portuguesa, como "rede de computadores dispersos por todo o planeta que trocam dados e mensagens utilizando um protocolo comum, unindo usuários particulares, entidades de pesquisa, órgãos culturais, institutos militares, bibliotecas e empresas de toda envergadura".

Para o Grande Dicionário Larousse Cultural da Língua Portuguesa, o significado da palavra Internet é o seguinte: "Rede internacional de computadores que, por

---

[16]FEDELI, Ricardo Daniel et alli. *Introdução à Ciência da Computação.* São Paulo: Thomson Pioneira, 2003, p. 55.

[17]MOREIRA, Rui. *Introdução à Informática.* Disponível em:< http://www2.ufp.pt/~rmoreira/MTC/Aula3_II.pdf>. Acesso em 22 abr 2007.

meio de diferentes tecnologias de comunicação e informática, permite a realização de atividades como correio eletrônico, grupos de discussão, computação de longa distância, transferência de arquivos, lazer, compras, etc."

Segundo leciona Joshua Eddings, a Internet

> é uma sociedade cooperativa que forma uma comunidade virtual, estendendo-se de um extremo a outro do globo. Como tal, a Internet é um portal para o espaço cibernético, que abrange um universo virtual de idéias e informações em que nós entramos sempre que lemos um livro ou usamos um computador, por exemplo.[18]

Fabrízio Rosa analisa o aspecto jurídico da Internet, entendendo como "uma rede transnacional de computadores interligados, com a finalidade de trocar informações diversas e na qual o usuário ingressa, por vários meios, mas sempre acaba por realizar fato jurídico, gerando conseqüências inúmeras nas mais variadas das localidades".[19] Portanto, as principais características da Internet relevantes para o direito são a formação de uma rede transnacional de computadores e a multiplicidade de objetivos visados: comercial, entretenimento e informação geral.

Relacionado à Internet, encontra-se o provedor de acesso que nada mais é do que uma "empresa ou organização que tem instalada uma conexão de alta capacidade com uma grande rede de computadores, e que põe à disposição de outros usuários o acesso a esta rede, por meio de linhas telefônicas ou cabos, cobrando ou não pelo serviço", segundo o Dicionário Eletrônico Houaiss da Língua Portuguesa.

O mestre pernambucano Pinto Ferreira apresenta, ainda, uma definição legal de Internet insculpida na Portaria n. 148, editada pelo Ministério das Telecomunicações em 31.5.1995, com a seguinte redação: "nome genérico que designa o conjunto de redes, os meios de transmissão e comutação, roteadores, equipamentos e

---

[18]EDDINGS, Joshua. Apud: ROSA, Fabrízio. *Crimes de Informática.* 2 . ed. Campinas: Bookseller, 2005, p. 35.

[19]ROSA, Fabrízio. *Crimes de Informática.* 2 . ed. Campinas: Bookseller, 2005, p. 36.

protocolos necessários à comunicação entre computadores, bem como o *software* e os dados contidos nestes computadores". [20]

A mesma Portaria, ainda segundo Ferreira, define provedor de serviço da seguinte maneira: "Provedor de Serviço de Conexão à Internet (PSCI): entidade que presta o serviço de conexão à Internet".[21]

Diante dos conceitos acima, podemos concluir que Internet é o meio pelo qual um conjunto de computadores é interligado em rede pelo mundo inteiro para transmissão de dados por meio de um provedor de acesso qualquer que lhe permite a disseminação e a distribuição de tais informações.

CAPÍTULO II - DOS CRIMES DE INFORMÁTICA

1 CONCEITO DE CRIME

O ser humano nasce cheio de necessidades, e, para satisfazê-las, são imprescindíveis certas coisas, materiais ou não. Essas coisas são chamadas de bens. Quando o homem começou a viver em sociedade, surgiu a obrigação de tutelar ditos bens para que uns respeitassem mutuamente o direito dos outros. Daí, nasce o conflito de interesse sobre o bem.

A tipificação do ilícito – conduta omissiva ou comissiva contrária ao direito, à moral e aos bons costumes – teve início com a taxação necessária de condutas que seriam danosas e prejudiciais ao próprio homem, que feria direito alheio e não poderia ser admitida na coletividade, sob o risco de desorganizá-la.[22]

Segundo o Professor Luiz Flávio Gomes, o objeto da teoria do delito é:

---

[20]FERREIRA, Pinto. A Era da Informática e a Juscibernética. *Revista da Academia Brasileira de Letras Jurídicas*, ano XIX, n. 22, Rio de Janeiro: Renovar, 2002, p. 143.
[21]FERREIRA, Pinto. A Era da Informática e a Juscibernética. *Revista da Academia Brasileira de Letras Jurídicas*, ano XIX, n. 22, Rio de Janeiro: Renovar, 2002, p. 143.
[22]BRITO, Eduardo Valadares de. *Crimes na Internet.* Disponível em: <http://www.ibdi.org.br.> Acesso em: 22 abr 2007.

> o estudo (a exposição sistemática) dos requisitos necessários para a configuração do crime. Esses requisitos constituem, ao mesmo tempo, pressupostos para a aplicação de uma pena ou medida de segurança a quem realizou um crime que, entendido como fato punível, nada mais é que um fato contrário ao Direito (antijuridicidade), descrito (previamente) numa lei penal (tipicidade) e ameaçado abstratamente com pena (punibilidade abstrata). Em outras palavras: fato adequado a uma lei penal (tipicidade material), ameaçado com pena (punibilidade abstrata) e contrário ao Direito (antijuridicidade).[23]

Sob o ponto de vista legal, o art. 1º da Lei de Introdução ao Código Penal nos dá o conceito formal de crime da seguinte forma:

> Art. 1º Considera-se crime a infração penal que a lei comina pena de reclusão ou de detenção, quer isoladamente, quer alternativa ou cumulativamente com a pena de multa; contravenção, a infração penal a que a lei comina, isoladamente, pena de prisão simples ou de multa, ou ambas, alternativa ou cumulativamente." (art. 1º da Lei de Introdução ao Código Penal e da Lei das Contravenções Penais – Decreto-Lei n. 3.914/41).

Assim, somente será considerado crime a conduta descrita em lei como tal, sendo imprescindível a cominação de uma determinada pena para aquele comportamento específico.

O conceito formal de crime está intimamente vinculado ao princípio da legalidade, pois, no dizer de Luiz Flávio Gomes, "delito, do ponto de vista puramente formal, é o que o Estado descreve numa lei como crime."[24]

O mesmo autor, mais adiante, encontra também um conceito material para crime. Para ele, seria "o fato humano lesivo ou perigoso (ofensivo) a um interesse

---

[23]GOMES, Luiz Flávio. *Direito Penal.* Vol. 3. 2. ed., rev., atual. e ampl. São Paulo: Revista dos Tribunais, 2006, p.13.
[24]GOMES, Luiz Flávio. *Direito Penal.* Vol. 3. 2. ed., rev., atual. e ampl. São Paulo: Revista dos Tribunais, 2006, p. 15.

relevante para a convivência social".[25] Essa conduta deve também ofender o bem jurídico protegido pelo sistema penal.

Em síntese, Luiz Flávio Gomes dá seu conceito de crime de maneira simples, porém abrangente, da seguinte forma: "crime é a ofensa grave (lesão ou perigo concreto de lesão intolerável) a um bem jurídico relevante (digno de proteção, merecedor de proteção) protegido pela lei penal."[26]

Por essa última parte da definição – "protegido pela lei penal" – é que se discute acerca da necessidade de tipificação legal para determinado fato, já que, sem lei, não há crime (princípio da reserva legal). Assim, os crimes virtuais seriam considerados atípicos e não haveria punição com base na legislação atual, segundo alguns autores. O tema será tratado com mais vagar mais adiante.

2 CONCEITO DE CRIME DE INFORMÁTICA

Faz-se imprescindível encontrar o conceito do objeto de estudo da presente pesquisa, a fim de dar forma e sentido ao trabalho em apreço.

Apesar da afirmação de Roberto Chacon de Albuquerque de que "qualquer tentativa de definir o termo 'crime informático', de conceituá-lo, apresenta desvantagens", porquanto, no pensamento do autor, dificilmente, pode-se elaborar uma definição sucinta e precisa sem que se deixem dúvidas, quer com relação ao seu objeto, quer com respeito à própria utilização da definição que lhe for conferida[27], aqui é feito um apanhado de diversas definições de renomados autores na tentativa de conceituar os delitos em análise.

Várias são as denominações encontradas nos mais diversos autores pesquisados: "crime informático", "crime por computador", "crime de informática", "crime

[25]GOMES, Luiz Flávio. *Direito Penal.* Vol. 3. 2. ed., rev., atual. e ampl. São Paulo: Revista dos Tribunais, 2006, p. 17.
[26]GOMES, Luiz Flávio. *Direito Penal.* Vol. 3. 2. ed., rev., atual. e ampl. São Paulo: Revista dos Tribunais, 2006, p. 17.
[27]ALBUQUERQUE, Roberto Chacon de. *A Criminalidade Informática.* São Paulo: Juarez de Oliveira, 2006, p. 40.

de computação", "delito informático", "delito virtual", "*computer* crimes", "*cybercrimes*", entre tantas outras nomenclaturas.

Para efeitos de estudo, prudente iniciar a conceituação de crime informáticos pela definição mais ampla encontrada, que é dada pela OECD – Organização para Cooperação Econômica e Desenvolvimento, para quem crime informático ou *computer crime* é qualquer conduta ilegal, não ética, ou não autorizada, que envolva processamento de dados e/ou a transmissão de dados.[28]

Para Sérgio Marcos Roque, crime de informática é: "a conduta definida em lei como crime em que o computador tiver sido utilizado como instrumento para a sua perpetração ou consistir em seu objeto material. Ao primeiro chamaremos de crime de informática impróprio ou comum, ao segundo de próprio ou autêntico".[29]

E continua afirmando que: "além de abrir 'novos horizontes' para o delinqüente, potencializando crimes tradicionais, como os patrimoniais, racistas, sexuais (pedofilia), contra a honra etc., dá ensejo aos delitos contra o computador (*hardware* e *software*) ou mesmo contra a informação."[30]

Já Fabrízio Rosa chama atenção para o fato de que nem toda conduta praticada contra ou por meio de computador será um crime cibernético. Dá, como exemplo, a cópia de programa de computador, cometendo pirataria de *software*, que não vai além de um crime de direitos autorais, com previsão na Lei n. 9.609/98.[31] Sua definição de crime de informática é a seguinte: "conduta típica, ilícita e culpável, praticada sempre com a utilização de dispositivos de sistemas de processamento ou comunicação de dados, da qual poderá ou não suceder a obtenção de uma vantagem indevida e ilícita."[32]

Outra excelente definição de delito virtual é encontrada em Eduardo Valadares de Brito, para quem "é o crime de rede, de computador, ou ainda de Internet. A definição deste crime é a seguinte: ofensa na qual uma rede de computadores é instrumento

---

[28]REIS, Maria Helena Junqueira. *Computer Crimes*. Belo Horizonte: Del Rey, 1997, p. 25.
[29]ROQUE, Sérgio Marcos. Apud: TORON, Alberto Zacharias. Crimes na Internet. In: *Repertório de Jurisprudência*, n. 22, 3º Caderno, São Paulo: IOB, 2000, p. 477.
[30]ROQUE, Sérgio Marcos. Apud: TORON, Alberto Zacharias. Crimes na Internet. In: *Repertório de Jurisprudência*, n. 22, 3º Caderno, São Paulo: IOB, 2000, p. 477.
[31]ROSA, Fabrízio. *Crimes de Informática.* 2. ed. Campinas: Bookseller, 2005, p. 57.
[32]ROSA, Fabrízio. *Crimes de Informática.* 2. ed. Campinas: Bookseller, 2005, p 58.

direto e significativo no cometimento do crime. Interconectividade de computadores é a característica essencial."[33]

Maria de La Luz Lima assevera que:

> em um sentido amplo é qualquer conduta criminógena ou criminal que em sua realização faz uso da tecnologia eletrônica seja como método, meio ou fim e que, em um sentido estrito, o delito informático é qualquer ato ilícito penal em que os computadores, suas técnicas e funções desempenham um papel, seja como método, meio ou fim.[34]

Marco Aurélio Rodrigues da Costa, em festejada monografia apresentada na PUC-RS, em 1995, conceitua o *computer crime* como:

> todo aquele procedimento que atenta contra os dados, que o faz na forma em que estejam armazenados, compilados, transmissíveis ou em transmissão. Assim, o crime de informática pressupõe dois elementos indissolúveis: contra os dados que estejam preparados às operações do computador e, também, através do computador utilizando-se *software* e *hardware*, para perpetrá-los.[35]

Por fim, cite-se o conceito dado pela Promotora de Justiça no Rio de Janeiro Carla Rodrigues de Castro, para quem crime de computador é:

> aquele praticado contra o sistema de informática ou através deste, compreendendo os crimes praticados contra o computador e seus acessórios e os perpetrados através do computador. Incluem-se, neste conceito, os delitos praticados através da Internet, pois pressuposto para acessar a rede é a utilização de um computador.[36]

Após as inúmeras definições acima elencadas, conclui-se que não basta o simples uso da tecnologia do computador para a caracterização do crime de informática.

---

[33]BRITO, Eduardo Valadares de. *Crimes na Internet.* Disponível em: <http://www.ibdi.org.br.> Acesso em: 22 abr 2007.
[34]LIMA, Maria de La Luz.Apud: ROSSINI, Augusto. *Informática, Telemática e Direito Penal.* São Paulo: Memória Jurídica Editora, 2004, p. 105.
[35]COSTA, Marco Aurélio Rodrigues da. *Crimes de Informática*. Disponível em: <http://jus2.uol.com.br/doutrina/texto.asp?id=1826>. Acesso em: 22 abr 2007.
[36]CASTRO, Carla Rodrigues Araújo de. *Crimes de Informática e seus Aspectos Processuais*. 2. ed., rev., atual. Rio de Janeiro: Lumen Juris, 2003, p. 9.

Para que este ocorra, faz-se imprescindível a presença da proteção da inviolabilidade de dados, a informação automatizada, como bem jurídico a ser protegido pelo direito.

3 CARACTERÍSTICAS DO CRIME DE INFORMÁTICA

Segundo Luiz Flávio Gomes[37] e Alberto Zacharias Toron,[38] a criminalidade no mundo informático tem as mesmas características da informatização global, quais sejam:

transnacionalidade, uma vez que todos os países do mundo têm acesso ilimitado ao conteúdo da rede, qualquer que seja seu grau de desenvolvimento econômico, social ou cultural, logo a criminalidade correspondente está em todas as partes e sob diferentes inserções culturais e jurídicas;

universalidade, como já foi dito, o uso da Internet é bastante difundido nos vários níveis sociais e econômicos devido ao seu baixo custo e facilidade de acesso; e

ubiqüidade, quer dizer, a *web* faz-se presente em todos os setores, seja público ou privado, e em qualquer lugar.

A questão mais controvertida dá-se quanto ao caráter de transnacionalidade que os crimes de computação apresentam, já que os sistemas informáticos não se deixam limitar por fronteiras territoriais.

É certo que a criminalidade virtual não conhece fronteiras. Um crime informático pode fragmentar-se: parte do *iter criminis* pode ser praticado em um país e outra metade em outro ou outros países, dependendo da situação.

Assim, qual teoria seria a melhor opção nos casos de cometimento de delitos informáticos para se determinar qual país teria a jurisdição para investigar, processar

---

[37]GOMES, Luiz Flávio. *Direito Penal.* Vol. 3. 2. ed., rev., atual. e ampl. São Paulo: Revista dos Tribunais, 2006, p. 6.
[38]TORON, Alberto Zacharias. Crimes na *Internet*. In: *Repertório de Jurisprudência,* nº 22, 3º Caderno. São Paulo: IOB, 2000, p. 477.

e julgar tais infrações penais? Deve-se, para responder à questão, analisar a lei de cada país, haja vista a jurisdição ser definida pelo direito interno e por tratados internacionais.

No caso de disseminação de vírus em que o agente estava no Brasil no momento do envio do *e-mail* ardiloso para uma pessoa na Argentina, mas que danificou o computador do provedor de acesso que é dos Estados Unidos, que país seria o mais indicado para o julgamento desse crime? Intenta-se, a seguir, dirimir tais questionamentos.

Nosso Código Penal adotou o princípio da territorialidade temperada, uma vez que determina a aplicação da lei brasileira aos crimes cometidos no território nacional, porém permite, excepcionalmente, a aplicação da lei estrangeira quando estabelecido em convenções, tratados ou regras de direito internacional, senão vejamos:

> Art. 5º Aplica-se a lei brasileira, sem prejuízo de convenções, tratados e regras de direito internacional, ao crime cometido no território nacional.

Quanto ao lugar do crime, o Código Penal brasileiro, em seu art. 6º, adotou a teoria da ubiqüidade (também conhecida como mista ou da unidade), segundo a qual o lugar do crime "é aquele em que se realizou qualquer dos momentos do *iter criminis*, seja da prática dos atos executórios, seja da consumação", conforme ensinamentos de Jesus.[39] Vejamos o que diz o mencionado dispositivo legal:

> Art. 6º Considera-se praticado o crime no lugar em que ocorreu a ação ou omissão, no todo ou em parte, bem como onde se produziu ou deveria produzir-se o resultado.

Significa dizer que, a partir do momento em que o crime "toca" o território brasileiro, ainda que transitoriamente, a lei local deverá ser aplicada.

Para Carla Rodrigues Araújo de Castro,[40] essa teoria deve ser aplicada normalmente também para crimes de informática, quando a ação, parte dela ou o resultado ocorrerem no território brasileiro. Lembra-se que é muito comum o chamado crime à distância, aquele em que a conduta é praticada fora do país e o resultado ocorre aqui, ou vice-versa.

---

[39]JESUS, Damásio Evangelista de. *Código Penal Anotado.* 11. ed., rev. e atual. São Paulo: Saraiva, 2001, p. 21.

[40]CASTRO, Carla Rodrigues Araújo de. *Crimes de Informática e seus Aspectos Processuais.* 2. ed., rev., atual. Rio de Janeiro: Lumen Juris, 2003, p. 14-5.

Em contrapartida, Celso Valin[41] chama a atenção para a segunda parte do citado dispositivo ("bem como onde se produziu ou deveria produzir-se o resultado"). Lembra o autor que a invasão de um sistema para danificar determinado servidor (ou provedor de acesso) surte resultados em qualquer parte do mundo, inclusive no Brasil.

Reconhece que, segundo a legislação pátria, poderia haver processo no Brasil, entretanto questiona se seria eficaz uma eventual lide em nosso país se o autor do delito nem o servidor estavam fisicamente em território nacional. Assim, para o mencionado autor, a teoria da ubiqüidade não resolveria o problema dos delitos informáticos.

Tampouco a teoria do resultado (também denominada do efeito, do evento ou *locus delicti*), que defende a tese do lugar do crime como o da produção de seu resultado, seria eficaz, pois a escolha do lugar do crime tornar-se-ia aleatória. Por exemplo, se um americano é esfaqueado no Brasil e falece em hospital na Argentina, este último país seria o competente para julgar o processo.

A solução trazida por Celso Valin é a de se adotar a teoria da atividade para os crimes virtuais, ou seja, o lugar do crime seria aquele em que o agente praticou o delito, a atividade delituosa. Dessa maneira, seria atribuída competência ao país com melhores condições de aplicar uma eventual pena, evitando-se, ainda, a extradição do agente para o país em que fosse condenado.[42]

A Alemanha, assim como o Brasil, adota, via de regra, a teoria da ubiqüidade, considerando lugar do crime o da prática do ato, onde ele se realizou ou teve seu resultado, conforme o art. 9º, § 1º, do Código Penal alemão. Não foi introduzido, nesse Código, dispositivo algum específico a fim de contemplar o lugar do delito virtual.

Diante disso, Roberto Chacon de Albuquerque chegou à seguinte conclusão quanto à responsabilidade dos provedores de acesso e de conteúdo na Internet:

---

[41]VALIN, Celso. A Questão da Jurisdição e da Territorialidade nos Crimes Praticados pela Internet. In: ROVER, Aires José (org.) *Direito, Sociedade e Informática*: Limites e Perspectivas da Vida Digital, Florianópolis: Fundação Boiteux, 2000, p. 116.

[42]VALIN, Celso. A Questão da Jurisdição e da Territorialidade nos Crimes Praticados pela Internet. In: ROVER, Aires José (org.) *Direito, Sociedade e Informática*: Limites e Perspectivas da Vida Digital, Florianópolis: Fundação Boiteux, 2000, p. 117.

> Precisa-se, para determinar a responsabilidade dos provedores de acesso à Internet, diferenciar entre provedores situados no território alemão e provedores situados no exterior. Se eles funcionarem na Alemanha, podem ser considerados responsáveis pelo conteúdo ilícito ao qual dão acesso até mesmo no exterior. Se o conteúdo estiver armazenado na Alemanha e for acessado a partir do exterior, pode-se ser enquadrado na própria Alemanha (art. 3º e art. 9º, § 1º). O provedor de conteúdo ilícito pode ser objeto de sanção penal a título de participação, mesmo se o ato principal não for passível de punição no exterior (art. 9º, § 2º). Se o provedor de acesso estiver situado no exterior, o direito alemão só incide caso haja um valor internacional (arts. 4º a 7º), ou se o lugar do resultado for o território alemão (arts 3º e 9º).[43]

Na Holanda, como o Código Penal local não define com precisão o lugar do crime, cabe à jurisprudência precisar onde o ilícito ocorreu. Já foi decidido que o lugar do crime pode ser onde se praticou o ato quando, em 1899, cartas eram enviadas dos Países Baixos para a França, num esquema fraudulento, no caso, os Países Baixos.

Decidiu também a Suprema Corte holandesa, em 1915, que se alguém pratica, por meio de um instrumento, a partir do exterior, um crime com conseqüências nos Países Baixos, a Justiça holandesa pode ser considerada competente para julgá-lo.

Já em 1958, adotou-se uma terceira teoria segundo a qual o lugar do crime ocorre onde este se consumou inteiramente, a partir de um caso em que uma carta foi enviada para o Reino Unido e decidiu-se, à época, que o crime ocorrera no local para onde a carta foi enviada.[44]

Na opinião de Roberto Chacon de Albuquerque, apesar de não ser a solução mais prática, por haver a possibilidade de gerar uma série de conflitos de jurisdição entre os diversos países que podem estar envolvidos em um crime informático e também

---

[43]ALBUQUERQUE, Roberto Chacon de. *A Criminalidade Informática.* São Paulo: Juarez de Oliveira, 2006, p. 69-70.
[44]ALBUQUERQUE, Roberto Chacon de. *A Criminalidade Informática.* São Paulo: Juarez de Oliveira, 2006, p. 70-72

por deixar a questão em aberto, a melhor saída seria admitir vários países competentes para julgar um crime informático em atenção ao princípio da ubiqüidade.

A Convenção sobre a Criminalidade Cibernética do Conselho da Europa, sobre a qual se comentará mais adiante, prevê, em seu art. 22, § 5º, que, "quando mais de uma parte reivindicar jurisdição com relação a uma alegada infração estabelecida de acordo com esta Convenção, as partes envolvidas deverão, quando for apropriado, consultar-se a fim de determinar a jurisdição mais apropriada para processar".

Na nossa opinião, com escusas aos doutrinadores citados, a melhor solução seria adotar a teoria da atividade nos crimes informáticos, apegando-nos ao abalizado juízo de Celso Valin. Jurisdição significa não só processar e julgar, mas também investigar. O país onde foi cometido o crime seria o mais indicado para conceder, em sua plenitude, direito de defesa ao acusado, colher as provas com maior segurança e, provavelmente, o que teria mais facilidade em capturar o agente. Nada impediria, porém, que os demais países que sofreram, de alguma forma, com o delito cooperassem na investigação do delito. Além do mais evitaria a celeuma que haveria caso todos os países atingidos pelo delito fossem considerados competentes, evitando-se, ainda, o *bis in idem*.

4 CLASSIFICAÇÃO DOS CRIMES DE INFORMÁTICA

Em brilhante exposição, Túlio Vianna distribui os crimes informáticos em impróprios, próprios, mistos e mediatos (ou indiretos).

Os primeiros, os crimes informáticos impróprios, conforme o citado autor, "são aqueles nos quais o computador é usado como instrumento para a execução do crime, mas não há ofensa ao bem jurídico da inviolabilidade da informação automatizada (dados)".[45] Significa que tais crimes poderiam ser praticados de qualquer outra forma, porém, no caso, o agente escolhe o computador como meio, mero instrumento para execução da infração penal.

[45]VIANNA, Túlio. *Fundamentos de Direito Penal Informático.* Rio de Janeiro: Forense, 2003, p. 14.

Seriam considerados crimes informáticos impróprios, por exemplo, crimes contra a honra, instigação ou induzimento ao suicídio, violação de segredo profissional, apologia às drogas, entre outros delitos, quando cometidos por meio de envio de mensagem por correio eletrônico (*e-mail*) ou em salas de bate-papo virtual (chamados de *chat*) ou por meio de página da *web*.

Já os crimes informáticos próprios "são aqueles em que o bem jurídico protegido pela norma penal é a inviolabilidade das informações automatizadas (dados)".[46] É essa classe de delito que se encontra em crise no atual momento legislativo brasileiro. São os novos tipos penais que surgiram com a evolução da informática e que ainda não ingressaram no mundo jurídico brasileiro, uma vez que até hoje não encontraram ressonância típica.

Entretanto, a Lei n. 9.983/2000 inseriu os arts. 313-A e 313-B no Código Penal Brasileiro, prevendo novos tipos especiais, tendo como sujeito ativo o funcionário público, os quais podem ser chamados de delitos informáticos próprios:

> 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.

Outro crime de informática próprio previsto em nosso ordenamento jurídico é a interceptação ilegal, tipificado na Lei n. 9.296/1996, que dispõe em seu art. 10º:

> Art. 10. Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei.

---

[46]VIANNA, Túlio. *Fundamentos de Direito Penal Informático.* Rio de Janeiro: Forense, 2003, p. 16.

Os delitos informáticos mistos são crimes complexos, ou seja, a norma penal tutela dois ou mais bens jurídicos, há fusão de dois ou mais tipos penais. No caso em comento, além de proteger a inviolabilidade dos dados, a norma visa a tutelar bem jurídico de natureza diversa.[47] Mais ainda, "são delitos derivados do acesso não autorizado a sistemas computacionais que ganharam *status* de delitos *sui generis* dada à importância do bem jurídico protegido diverso da inviolabilidade dos dados informáticos".[48]

Há um exemplo de delito informático misto no ordenamento brasileiro. Trata-se do inciso I do art. 72 do Código Eleitoral (Lei n. 9.504/1997), que assim dispõe:

> 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; (…)

Vale lembrar que, ao contrário do que muitos pensam, o sistema eleitoral brasileiro é completamente vulnerável, por isso faz-se necessário tipificar a conduta de eventual criminoso que quebre, ou tente quebrar, o sigilo das fontes do TSE.

Por fim, apresenta-se o delito informático mediato ou indireto, que consiste em um "delito-fim não informático que herdou esta característica do delito-meio informático realizado para possibilitar a sua consumação".[49]

Explique-se. O que acontece no caso é o fenômeno da consunção, isto é, um fato definido em lei como crime atua como mera fase de preparação, execução ou exaurimento do crime mais grave, o crime-fim. Aquele fica absorvido por este.

Dá-se como exemplo a invasão de banco de dados de um banco e a posterior transferência de numerário de uma conta para outra. Há, *in casu*, dois delitos distintos: a invasão do sistema do banco pelo *hacker* – crime de informática (delito-meio) – e a subtração de coisa alheia móvel, furto – crime patrimonial (delito-fim). Apesar de o agente só ser punido pelo crime-fim, este será classificado de delito informático mediato ou indireto em razão da aplicação do princípio da consunção.

---

[47]VIANNA, Túlio. *Fundamentos de Direito Penal Informático.* Rio de Janeiro: Forense, 2003, p. 23.
[48]VIANNA, Túlio. *Fundamentos de Direito Penal Informático.* Rio de Janeiro: Forense, 2003, p. 23.
[49]VIANNA, Túlio. *Fundamentos de Direito Penal Informático.* Rio de Janeiro: Forense, 2003, p. 25.

Marco Aurélio Rodrigues da Costa, em monografia já citada, classifica os delitos informáticos quanto ao seu objetivo material em puros, mistos e comuns.[50]

Os delitos informáticos puros visam exclusivamente a violar o sistema de informática da vítima. Note-se que o *animus* do sujeito ativo é específico: o sistema de informação presente no computador do sujeito passivo, em todas as suas formas.

Apesar de bastante empregada, a classificação ora apresentada merece uma pequena crítica. Quando cita o autor que "o sujeito ativo visa especificamente ao sistema de informática, em todas as suas formas", inclui os meios de armazenamento externo, tais como fitas e disquetes.

Ora, não se pode conceber que a subtração de um disquete venha a ser considerado crime de computação. Para ser classificado como tal, há de estar presente o manejo de dispositivos de sistemas de processamento ou comunicação, conforme ensina Fabrízio Rosa, em trabalho já citado.

Os delitos informáticos mistos, segundo Marco Aurélio Rodrigues da Costa, dão-se quando o agente visa a um bem juridicamente protegido diverso da informática, porém, sem a utilização do sistema de informática, o crime não se pode consumar. Para exemplificar, serve-se do clássico caso da transferência ilícita de valores, em que o uso do sistema de informática da instituição financeira é imprescindível para alcançar o resultado pretendido.

Marco Aurélio Rodrigues da Costa conceitua os delitos informáticos comuns da seguinte maneira:

> São todas aquelas condutas em que o agente se utiliza do sistema de informática como mera ferramenta à perpetração de crime comum, tipificável na lei penal, ou seja, a via eleita do sistema de informática não é essencial à consumação do delito, que poderia ser praticado por meio de outra ferramenta.[51]

---

[50]COSTA, Marco Aurélio Rodrigues da. *Crimes de Informática*. Disponível em: <http://jus2.uol.com.br/doutrina/texto.asp?id=1826>. Acesso em: 22 abr 2007.

[51]COSTA, Marco Aurélio Rodrigues da. *Crimes de Informática*. Disponível em: <http://jus2.uol.com.br/doutrina/texto.asp?id=1826>. Acesso em: 22 abr 2007.

Nesses casos, o computador é mero meio de execução, mas o autor do delito poderia ter escolhido outro para perpetrar a conduta criminosa desejada, não se tornando imprescindível o uso da máquina.

Estes são equivalentes aos crimes informáticos impróprios acima mencionados na classificação de Túlio Vianna.

Marco Aurélio Rodrigues da Costa reconhece a aplicabilidade das normas penais nos casos em apreço, porém sugere a aplicação de uma agravante pelo uso de sistema de informática, uma "vez que é meio que necessita de capacitação profissional e a ação delituosa por esta via reduz a capacidade da vítima em evitar o delito."[52]

Outra classificação interessante é apresentada por Sérgio Marques Roque em que aduz duas categorias de *cybercrimes*:

> Aqueles praticados através do uso do computador e os perpetrados contra os dados ou sistemas informáticos. Nos primeiros, o computador será o instrumento, no segundo, o objeto material. Assim, quando o computador for utilizado apenas como instrumento de escolha pelo agente ativo para a consecução do crime, este será crime de informática comum, mas, quando a ação do criminoso se dirigir contra os dados contidos no sistema, será definido como crime de informática autêntico, porque nesse último o computador é essencial para a existência do delito".[53]

Maria de La Luz Lima classifica os delitos eletrônicos em três categorias:

(a) os que utilizam a tecnologia eletrônica como método, ou seja, condutas criminais nas quais os indivíduos utilizam métodos eletrônicos para obter um resultado ilícito;

(b) os que utilizam a tecnologia eletrônica como meio, ou seja, condutas criminais nas quais, para a realização de um delito, utiliza-se o computador como meio; e

---

[52]COSTA, Marco Aurélio Rodrigues da. *Crimes de Informática*. Disponível em: <http://jus2.uol.com.br/doutrina/texto.asp?id=1826>. Acesso em: 22 abr 2007.

[53]ROQUE, Sérgio Marques. Apud: ROSSINI, Augusto. *Informática, Telemática e Direito Penal.* São Paulo: Memória Jurídica Editora, 2004, p. 120.

(c) os que utilizam a tecnologia eletrônica como fim, ou seja, condutas dirigidas contra a entidade física do objeto ou máquina eletrônica ou seu material com o objetivo de danificá-la.

Existem outras classificações que seguem critérios diferenciados. Por exemplo, o Prof. Ulrich Sieber,[54] da Universidade de Würzburg, na Alemanha, classifica os crimes objeto de nosso estudo pelo critério da atuação do autor. Assim há

(a) fraude por manipulação de um computador contra um sistema de processamento de dados, que consiste na introdução de dados falsos, na modificação dos resultados de um programa, sempre com o intuito de obtenção de benefícios econômicos;

(b) espionagem informática e furto de *software,* que podem ser cometidos por meio de programas copiadores ou por meio de furto de periféricos (disquetes, CD-ROM, etc.);

(c) sabotagem informática, efetuada por meio de um tipo de "bomba" que destrói o programa, distorcendo seu funcionamento;

(d) furto de tempo ou de serviço é caracterizado quando empregados utilizam sem autorização horas do computador do empregador para realizar trabalhos particulares. Está incluso nesta classificação porque o Estado da Virgínia nos Estados Unidos considera propriedade o tempo de computador ou de serviços de processamento de dados e incrimina seu uso não autorizado;

(e) acesso não autorizado a sistemas de processamento de dados, que consiste na atividade de *hackers* e será exposto com mais vagar no tópico seguinte; e, finalmente,

(f) ofensas tradicionais, que se referem ao uso de computadores para mascarar ações puníveis, por exemplo, a supressão de dados contábeis e alteração em folhas de pagamento.

---

[54]SIEBER, Ulrich. Apud: REIS, Maria Helena Junqueira. *Computer Crimes*. Belo Horizonte: Del Rey, 1997, p. 29-31.

Há, ainda, a classificação de C. M. Romero Casabona,[55] professor catedrático da Universidade de La Laguna, na Espanha, que diferencia os "cdleitos" informáticos da seguinte maneira:

(a) *manipulação de entrada de dados (input)*: consiste na introdução de dados falsos no computador alheio, abarcando também a omissão do registro de dados;[56]

(b) manipulações no programa: inicialmente, parte de uma entrada de dados correta, porém, no processamento, conduz a resultados falsos por interferências no programa;

(c) manipulações na saída de dados (*output*): acontece quando os dados introduzidos no programa são verdadeiros, sem alteração alguma, mas, no momento da impressão ou da transmissão dos dados para outro computador, há manipulação;

(d) manipulação à distância: acontece quando o computador encontra-se conectado com outros terminais ou computadores por linha telefônica, satélite ou algo que o valha, mediante um *modem,* que codifica e decodifica as informações.

Como se pode ver, tamanha preocupação em classificar os delitos informáticos salienta a importância que deve ser dada ao tema em razão do caráter de novidade na esfera jurídica mundial.

5 DO SUJEITO ATIVO DO CRIME DE INFORMÁTICA

Qualquer pessoa pode ser sujeito ativo de crime por computador em sentido amplo. Entretanto, para a prática dos crimes informáticos próprios, segundo classificação acima explanada, faz-se necessário conhecimento pormenorizado do computador e suas nuances acessíveis apenas a um pequeno grupo de pessoas chamadas usualmente de *hackers*.

---

[55]CASABONA, C. M. Romero. Apud: REIS, Maria Helena Junqueira. *Computer Crimes*. Belo Horizonte: Del Rey, 1997, p. 31-32.

[56]Esse tipo de sabotagem é chamada de "Cavalo de Tróia" por Sznick. SZNICK, Valdir. O Delito e o Computador. *Revista Trimestral de Jurisprudência dos Estados*, ano 8, vol. 26, São Paulo: Vellenich, 1984, p. 68.

Segundo Rita de Cássia da Silva,[57] a palavra *hacker* surgiu no início dos anos 80, no *Massachusetts Institute of Technology,* para designar estudantes de computação que passavam as madrugadas pesquisando dentro do laboratório. O termo era usado como sinônimo de especialista em computador. A melhor tradução para o termo seria "fuçador", ou seja, aquele que tem o costume de bisbilhotar, vasculhar a tecnologia, os sistemas disponíveis.

Hoje em dia, o termo é usado pejorativamente para referir-se aos invasores ilegais de sistemas de computador, aqueles que se aproveitam de seus conhecimentos de informática para conseguir alguma vantagem ilícita ou, até mesmo, os que, pelo simples desejo de aventura, despistam esquemas de segurança e invadem computadores alheios, principalmente de grandes empresas ou agências governamentais.

Há quem indique, porém, diferença entre conceito de *hacker* e *cracker*.[58] O primeiro seria o especialista em computação que usa seus vastos conhecimentos eticamente, enquanto o segundo seria uma versão criminosa do primeiro. Seriam exatamente opostos.

O *hacker* trabalharia para solucionar os problemas trazidos para um determinado sistema de informática pelo *cracker*. Esse seria o sujeito ativo nos crimes cibernéticos próprios, aquele que invade sem autorização os servidores de Internet e tenta destruir programas, alterá-los ou copiá-los. Tem conhecimento vasto, tanto quanto o *hacker*, porém o utilizaria para a prática de delitos. A mesma diferenciação entre *hacker* e *cracker* é feita por Luiz Flávio Gomes, citado por Vicente Lentini Plantullo.[59]

Os *crackers* mais evoluídos, ou seja, aqueles com mais experiência e conhecimento, são conhecidos como *wizards*, que em inglês significa mestre, mago ou guru. São criminosos idolatrados em seu meio e, pela sua capacidade de domínio incalculável da tecnologia, são mais perigosos e de difícil captura pelas autoridades.

---

[57]SILVA, Rita de Cássia Lopes da. *Direito Penal e Sistema Informático.* São Paulo: Revista dos Tribunais, 2003, p. 77.
[58]SILVA, Rita de Cássia Lopes da. *Direito Penal e Sistema Informático.* São Paulo: Revista dos Tribunais, 2003, p. 78.
[59]PLANTULLO, Vicente Lentini. *Estelionato Eletrônico*. Curitiba: Juruá, 2005, p. 80.

Entretanto, Alberto Zacharias Toron, além de apresentar características distintas das acima colacionadas, traz novos sujeitos ativos. Para ele, *cracker* "é um autodidata da informática que, sem ter os conhecimentos do *hacker*, tenta imitá-lo, mas sem grandes vôos. Fica no nível da realização de cópias-piratas de programas de informática", enquanto que *hackers* seriam "usuários da Rede que ardilosamente, sem autorização, invadem computadores ou sistemas, seja para acessar dados, seja para destruí-los ou até mesmo para obter vantagens ilícitas."[60]

O mesmo autor traz, ainda, outros dois conceitos de delinqüentes cibernéticos tais como *cyberpunk,* que são os vândalos da cibernética que agem com o intuito de destruir programas, dados ou suportes informáticos – afirma que seria como um *cracker*, porém com o intuito de penetrar de forma não autorizada em sistemas de informática mediando a corrupção de uma senha para destruir dados ou inserir no sistema um vírus que o destrua – e *sniffers,* que atuam na tentativa de entrar no disco rígido dos computadores conectados à grande Rede com o intuito de obter certo tipo de informação.

Vicente Lentini Plantullo, citando Luiz Flávio Gomes, brinda-nos com mais três conceitos de criminosos virtuais o *phreaker*, o *anarchist* e o *warez*. O primeiro é aquele que "possui talento para manipular a tecnologia de linhas telefônicas e celulares. Geralmente, associam tal talento ao computador para promover seus ataques com objetivo de não serem identificados".[61] São eles que "clonam" celulares, interceptam e rastreiam ligações e fazem uso de provedores sem pagar impulso.

Já o anarquista utiliza o computador com o mero intuito de prejudicar. Seu objetivo é danificar computadores, disseminar vírus, divulgar idéias contrárias à moral e aos bons costumes por meio de manuais de tortura ou instruções de como fazer o gás do riso, entre outras maneiras.

---

[60]TORON, Alberto Zacharias. Crimes na Internet. *Repertório de Jurisprudência*, nº 22, 3º Caderno. São Paulo: IOB, 2000, p. 477.
[61]GOMES, Luiz Flávio. Apud: PLANTULLO, Vicente Lentini. *Estelionato Eletrônico*. Curitiba: Juruá, 2005, p. 80.

O *warez* é aquele pirata de *software* que lança mão de seus conhecimentos adquiridos em telemática com puro objetivo de lucro. Ele vende programas piratas, desbloqueia códigos que evitam a pirataria, etc.[62]

Além dos sujeitos já denominados, Augusto Rossini[63] traz vários exemplos de sujeitos ativos de crime informático. Entretanto, no presente trabalho, serão tratados apenas aqueles que se mostram mais importantes.

Os *carders* são aqueles agentes especializados em adquirir números e senhas de cartões de crédito, telefônico ou magnéticos para utilização fraudulenta perante as empresas que atuam no ambiente de rede. Diferenciam-se dos estelionatários comuns porque atuam com exclusividade no *Ciberespaço*.

Os *sneakers* (que em inglês significa "gatunos") são espécie de *crackers,* que quebram proteção de sistemas de empresas para obter informações sigilosas (pirataria empresarial) com a particularidade de fazê-lo mediante paga ou qualquer outra vantagem. Quem oferecer mais benefícios poderá contar com seus serviços.

Outro perigoso agente do mundo virtual é o *virii* que tem como principal atividade a criação e a disseminação de vírus de computador. Foram eles que criaram os vermes eletrônicos (conhecidos como *worms*), que causam grande prejuízo à Rede e são combatidos diariamente pelos usuários.

Augusto Rossini[64] fez um excelente estudo acerca da mente criminosa dos sujeitos ativos dos delitos informáticos, revelando aspectos de sua origem social, do acesso ao conhecimento criminoso, da idade, do grau de culpabilidade e outras facetas que serão comentadas adiante.

Conforme o citado autor, os agentes de infrações penais são, geralmente, provenientes das classes média e alta da sociedade, com boa bagagem cultural. Por isso, mostram-se como criminosos diferenciados, não tendo os requisitos do criminoso-padrão.

---

[62]COHEN. Apud: PLANTULLO, Vicente Lentini. *Estelionato Eletrônico*. Curitiba: Juruá, 2005, p. 81.
[63]ROSSINI, Augusto. *Informática, Telemática e Direito Penal.* São Paulo: Memória Jurídica Editora, 2004, p. 147-155.
[64]ROSSINI, Augusto. *Informática, Telemática e Direito Penal.* São Paulo: Memória Jurídica Editora, 2004, p. 134-142.

Este, muitas vezes, não tem escolhas senão adentrar-se no crime, enquanto o criminoso informático age por opção, tornando-se até mais perigoso que o delinqüente comum.

Acrescente-se que o acesso à Internet e às informações no âmbito da informática é ilimitado e qualquer pessoa, independentemente da idade, pode ter a curiosidade de vasculhar, sem autorização, o computador alheio. O livre acesso, aliado à velocidade com que chegam as informações aos usuários – em tempo real –, contribui para que adolescentes tenham mais intimidade com a máquina. Augusto Rossini nos traz um impressionante dado: segundo especialistas a idade média dos *crackers* está entre 18 e 19 anos e o time dos que estão entre 14 e 15 é bastante grande.

Segundo Marcelo Antonio Sampaio Lemos Costa,[65] o Brasil foi citado em um relatório britânico como o país que abriga os dez grupos de *hackers* mais ativos do mundo, o que nos dá um indicativo do potencial de nossos *cybercriminosos*.

Diante disso, conclui-se que o sujeito ativo da infração penal telemática é bastante diferenciado do que se costuma tratar. É também o mais difícil de se identificar devido à facilidade em manter o anonimato, pois, ainda que se possa identificar o computador empregado para a prática delituosa através do número IP da máquina, não se indica, necessariamente, quem efetivamente fez uso do aparelho.

Daí a necessidade de se tratarem com mais cautela os crimes cometidos por meio dos sistemas de computadores e contra eles.

6 DA CONVENÇÃO SOBRE CRIMES CIBERNÉTICOS

Diante da nova forma de criminalidade e após os ataques de 11 de Setembro, constantes invasões de *hackers* a computadores de grandes empresas e sistemas governamentais e disseminação da pedofilia e transferência ilegal de valores de contas bancárias, chegou-se à conclusão de que a *ultima ratio* do Direito fosse convocado a agir com urgência para garantir a proteção a bens jurídicos preciosos da sociedade.

---

[65]COSTA, Marcelo Antonio Sampaio Lemos. *Computação Forense*. 2. ed. Campinas: Millennium, 2003. p. 6.

Essa preocupação deu origem à Convenção sobre *Cybercrime*, ocorrida em Budapeste em 23 de novembro de 2001, e lança paradigmas para o estudo sobre delitos informáticos. Tal encontro foi realizado entre os Estados-membros do Conselho da Europa e demais signatários deste.

No presente trabalho, utilizam-se tradução e comentários de Augusto Rossini,[66] uma vez que não há textos oficiais em nosso vernáculo. Limita-se, outrossim, à parte substantiva da Convenção, por não serem objeto da monografia os aspectos processuais da legislação sugeridos em Budapeste.

Já no preâmbulo, denotam-se o interesse e a preocupação com o tema "como matéria prioritária, uma política criminal comum direcionada à proteção da sociedade contra o *cybercrime*, *inter alia* por meio da adoção de legislação apropriada e promoção do crescimento da cooperação internacional".

Mais adiante, a Convenção reconhece a necessidade de cooperação entre os Estados e a iniciativa privada no combate ao *cybercrime,* por ser interesse de toda a coletividade. Entende que a cooperação dará mais efetividade ao combate perpetrado.

A Convenção lança, outrossim, definições que devem ser seguidas acerca de certos termos técnicos no ramo da informática. Eis alguns:

Sistema de computador significa qualquer equipamento ou um grupo de equipamentos conectados ou relacionados, um ou mais, os quais, viabilizados por um programa, realizam processamento automático de dados;

Dado de computador significa qualquer representação de fatos, informações ou conceitos em uma forma adequada para o processamento em um sistema de computador, incluindo um programa apropriado que possibilite ao sistema de computador realizar a função;

Provedor de serviços significa i) qualquer entidade pública ou privada que proporciona para os usuários de seus serviços a possibilidade de se comunicarem por meio de um sistema de computador, e ii) qualquer outra entidade que processa ou armazena

[66]ROSSINI, Augusto. *Informática, Telemática e Direito Penal.* São Paulo: Memória Jurídica Editora, 2004, p. 33-101.

dados de computador em benefício de tal serviço de comunicação ou usuários desse serviço;

Tráfego de dados significa qualquer dado de computador relacionado a uma comunicação por meio de um sistema de computador, gerado por um sistema de computador, que forma uma parte de uma cadeia de comunicação, indicando a origem da comunicação, o destino, a rota, o tempo, a data, o tamanho, a duração ou o tipo de base desse serviço.

Num terceiro ponto, a Convenção sobre Crimes Cibernéticos sugere a criação do tipo penal incriminador, sem impor uma redação específica a fim de respeitar as características de cada localidade. Nessa parte, é recomendada a adoção de medidas efetivas quando o crime for praticado de forma dolosa, não havendo referência a negligência, imprudência ou imperícia.

Os arts. 2º a 6º (Título I, Capítulo II) visam a proteger o computador como alvo do delito: acesso ilegal (acesso desautorizado no sistema de computador alheio), interceptação ilegal (interceptação desautorizada de transmissão privada de dados), interferência de dados (sem a interação com o sistema), interferência de sistema (com o interface com o sistema) e mau uso de equipamentos (sugere a responsabilização dos atos preparatórios).

O Título II visa a proteger "Danos relacionados a computador", ou seja, pretende a criminalização das condutas que tenham por objetivo a alteração de dados verdadeiros. Aqui, o computador não é mais visto como alvo – tal qual o título anterior –, mas como instrumento. O art. 7º trata da falsificação relacionada a computador, e o 8º da fraude relacionada a computador.

O título seguinte é composto tão-somente por um dispositivo (art. 9º) com a finalidade de proteger crianças e adolescentes de abusadores sexuais. Esse único artigo, porém, abarca diversas condutas, tais como produzir, oferecer ou disponibilizar, distribuir ou transmitir, comprar e possuir pornografia infantil em um sistema de computador ou armazenamento de dados, entre outros.

No Brasil, a Lei n. 10.764/2003, inspirada na Convenção de Budapeste, alterou o art. 241 do Estatuto da Criança e do Adolescente (Lei n. 8.069/90), para incluir

mais condutas às que já existiam e acrescentou a possibilidade de propagação da pornografia infantil por meio da grande rede, conforme se colhe do mencionado dispositivo legal:

> Art. 241. Apresentar, produzir, vender, fornecer, divulgar ou publicar, por qualquer meio de comunicação, inclusive rede mundial de computadores ou Internet, fotografias ou imagens com pornografia ou cenas de sexo explícito envolvendo criança ou adolescente: (Redação da Lei n. 10.764/12.11.2003) (original sem grifos)

Danos relacionados à transgressão de direitos autorais e direitos correlatos é o tema do Título IV da Convenção em estudo. A reprodução não autorizada de documentos ou programas, de fato, merece total proteção devido à extrema facilidade de se copiarem tais bens jurídicos no âmbito da Internet.

A "pirataria" – como é chamada a transgressão de propriedade imaterial – vem crescendo absurdamente nos últimos anos, mormente após o advento da Rede Mundial de Computadores. Num primeiro momento, imaginou-se que não seria necessária a intervenção do Direito Penal – tido como *ultima ratio* – para solucionar conflitos envolvendo prejuízos causados com a prática dos delitos da espécie, tendo em vista que os demais ramos do direito seriam aptos a enfrentar tais problemas. Entretanto, fácil perceber que é um problema que atinge não só o proprietário, mas toda a coletividade de um Estado, haja vista a pirataria afetar o recolhimento de tributos e a criação de postos de trabalho.[67]

Os demais Títulos da Convenção tratam de questões secundárias, porém bastante importantes para a proteção dos bens jurídicos atingidos pela informática. Cuida de tentativa e concurso (chamados de ajuda ou encorajamento) no art. 11. Já o art. 12 preocupa-se com a responsabilidade das empresas (chamada de responsabilidade corporativa), atribuindo às pessoas jurídicas a capacidade de delinqüir.

O art. 13 trata das disposições finais e recomenda que, em qualquer caso, as ofensas criminais previstas na Convenção sejam puníveis por sanções efetivas, proporcionais e dissuasivas, que incluam privação de liberdade. Por efetividade, entenda-se

---

[67]ROSSINI, Augusto. *Informática, Telemática e Direito Penal.* São Paulo: Memória Jurídica Editora, 2004, p. 70-71.

que a resposta do Direito Penal deve ser eficaz e certa, sob pena de ser desmoralizado. Proporcionalidade preocupa-se com a exata medida da sanção penal, ou seja, a pena deve ser, antes de tudo, justa. Já dissuasividade está intimamente ligada ao caráter preventivo do Direito Penal, que assegura os direitos individuais do cidadão e previne que novas condutas sejam praticadas.[68]

Merece críticas o art. 21 da Convenção, uma vez que recomenda aos Estados-membros a adotar medidas a fim de cooperar e assistir as autoridades competentes na coleta ou na gravação de conteúdo de dados, em tempo real, de comunicações especificadas em seu território por meio de um sistema de computador.

A censura feita por José de Castro Meira é da seguinte ordem:

> Como se vê, a Convenção autoriza os serviços policiais a acessar dados, inclusive em tempo real, impossibilitando qualquer providência pelos usuários da rede, que ficam obrigados a guardar sigilo sobre as medidas, ainda que as considere absurdas e fora de propósito. Afinal, o critério quanto à "razoabilidade" das providências poderá ficar à mercê do entendimento dos serviços de segurança. As comunicações na Internet perderão a confiabilidade, quanto ao resguardo do sigilo, tendo em vista que o acesso pode ocorrer inclusive em tempo real, sem que fique sinal da interferência, com o propósito de realizar o objetivo buscado pelas autoridades policiais.[69]

Consoante se pode perceber, a atenção dirigida aos novos paradigmas trazidos pela informática é difundida em todo o mundo. A tendência mundial é contemplar os delitos informáticos com novas legislações, já que se trata de uma realidade de nosso cotidiano.

CAPÍTULO III - DO PROJETO DE LEI Nº 84/99

---

[68]ROSSINI, Augusto. *Informática, Telemática e Direito Penal.* São Paulo: Memória Jurídica Editora, 2004, p. 100.

[69]MEIRA, José de Castro. *Crimes de Informática.* Disponível em: <http://buscalegis.ccj.ufsc.br/arquivos/crimes_informatica_meira.html>. Acesso em: 12. out. 2006.

Finalmente, após as explanações acerca do conceito, das características e das diversas formas de classificar os crimes informáticos, chega-se ao ponto de se comentar o Projeto de Lei n. 84/99, de autoria do Deputado Luiz Piauhylino, na forma do substitutivo apresentado pelo relator Deputado Léo Alcântara, na Comissão de Constituição e Justiça e de Redação, em 2002. A matéria tramita em regime de urgência, e, a qualquer momento, podemos ser contemplados com mais uma norma penal.

Diante de tantos projetos de lei sobre o tema, o PL 84/99 (atual PLC 89/03) foi escolhido para comentários no presente trabalho por se tratar do mais amplo e abrangente deles e, também, por estar num estágio mais avançado no processo legislativo. Essa opinião se coaduna com a do Comitê de Direito e Tecnologia da Câmara Americana de Comércio de São Paulo (AmCham/SP).

Será discutido, neste tópico, se há, realmente, a necessidade de se criarem novos tipos penais para os delitos contra sistemas de informação contidos em computadores – tendo em vista que alguns defendem a atipicidade dos crimes virtuais, e, conseqüentemente, não podem esses crimes ser punidos com base na legislação penal vigente – ou se os crimes praticados pela via virtual já estão devidamente tipificados e apenados no Código Penal vigente, com uma simples modificação no *modus operandi*, significando que não há por que modificar a legislação atual.

Em todo o mundo, leis específicas para o combate e a punição dos tipos de delito em estudo já estão sendo promulgadas e aplicadas, como é o caso da Alemanha – que, em 1986, promulgou lei contra a criminalidade econômica, a qual contempla os delitos de espionagem e falsificação de dados e fraude eletrônica –, da Áustria – que reformou seu Código Penal para incluir os delitos de destruição de dados e fraude eletrônica –, da França – que criou lei, em 1988, que dispõe sobre acesso fraudulento a sistema de elaboração de dados, sabotagem, destruição de dados, falsificação de documentos eletrônicos e uso de documentos informatizados falsos – e dos Estados Unidos – que adotaram a Ata Federal de Abuso Computacional, direcionada a atos de transmissão de vírus.[70]

[70]PAIVA, Mário Antônio Lobato de. Delitos Virtuais. *Revista Jurídica Consulex*, Ano VI, n. 138. Brasília: Consulex, 2002, p. 61.

Carla Rodrigues Araújo de Castro[71] dá conta também de que há lei em Portugal, desde 1991, dispondo sobre a criminalidade informática, e, na Itália, houve alteração do Código Penal, acrescentando quinze preceitos sobre o tema. Mário Furlaneto Neto e Guimarães[72] acrescentam que houve recente atualização do Código Penal da Espanha para contemplar, como crimes, a pornografia infantil praticada via Internet e a posse de material pornográfico relacionado à pornografia infantil.

No Brasil, a matéria ainda se encontra em plena discussão, apesar de a tendência ser pela tipificação em lei especial dos crimes de informática, conforme se vê do adiantado estágio do Projeto de Lei n. 84/99 e da opinião dos principais doutrinadores especializados na matéria.

1 PRINCÍPIO DA RESERVA LEGAL

Nullo crimem nulla poena sine praevia lege, ou seja, não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal. Com esse brocardo, a Carta Magna de 1988 postula o Princípio da Reserva Legal no inciso XXXIX de seu art. 5º.

Dito preceito tem origem na Carta Inglesa de 1215, assinada pelo Rei João Sem Terra, após ceder às pressões dos barões feudais, e dispunha que:

> nenhum homem livre será detido ou sujeito à prisão, ou privado de seus bens ou colocados fora da lei, ou exilado, ou de qualquer modo molestado, e nós não procederemos nem mandaremos proceder contra ele se não mediante um julgamento regular sobre seus pares ou de harmonia com a lei do País" (*Nullus líber homo expiatur vel*

[71]CASTRO, Carla Rodrigues Araújo de. *Crimes de Informática e seus Aspectos Processuais.* 2. ed., rev., atual. Rio de Janeiro: Lumen Juris, 2003, p. 156-158.
[72]FURLANETO NETO, Mário *et alii*. Crimes na Internet: elementos para uma reflexão sobre a ética informacional. *Revista CEJ*, ano VII, n. 20, Brasília: Conselho da Justiça Federal, 2003, p. 71.

imprisoned, nisi per legale judicium purium suorim vel per legem terrae).[73]

Conforme ensinamento de José Afonso da Silva, o princípio da reserva legal distingue-se do da legalidade porque aquele consiste em estatuir que a regulamentação de determinadas matérias há de fazer-se necessariamente por lei formal. Outra diferença é que o princípio da legalidade (genérica) envolve primariamente uma situação de hierarquia das fontes normativas, enquanto o princípio da reserva de lei (legalidade específica) envolve questão de competência.

Rita de Cássia Lopes da Silva cita Crisafulli, segundo o qual, "tem-se, pois, reserva de lei quando uma norma constitucional atribui determinada matéria exclusivamente à lei formal (ou a atos equiparados, na interpretação firmada na praxe), subtraindo-a, com isso, à disciplina de outras fontes, àquela subordinada".[74]

Há, ainda, divisão do princípio da reserva legal em absoluta e relativa. Trata-se de reserva absoluta quando a matéria é reservada pela Constituição como exclusiva de lei, não se considerando a hipótese de haver qualquer outra fonte infralegal. A reserva relativa se dá quando se admite que parte da matéria seja buscada em outras fontes que não a lei.

Assim, pode-se dizer que a reserva legal absoluta proíbe o preenchimento de lacunas em normas penais por meio da analogia e dos costumes como fontes do Direito Penal. Logicamente que a proibição se dá apenas na aplicação para piorar a situação do acusado, podendo ser aplicado *in bonam parte*, ou seja, para beneficiar o réu.

O princípio em comento está historicamente presente nas nossas Constituições, inclusive na nossa primeira Constituição de 1824 e, sucessivamente, nas de 1891, 1934, 1946, 1967 e na Emenda Constitucional de nº 1 de 1969.[75]

Luiz Luisi lembra que a Declaração Universal dos Direitos do Homem, aprovada pela Assembléia Geral das Nações Unidas de 1948, dispõe em seu artigo II, 2:

---

[73]LUISI, Luiz. *Os Princípios Constitucionais Penais*. 2. ed. Porto Alegre: Sergio Antonio Fabris Editor, 2003, p. 119

[74]SILVA, Rita de Cássia Lopes da. *Direito Penal e Sistema Informático*. São Paulo: Revista dos Tribunais, 2003, p. 368.

[75]LUISI, Luiz. *Os Princípios Constitucionais Penais*. 2. ed. Porto Alegre: Sergio Antonio Fabris Editor, 2003, p. 18.

> Ninguém será condenado por atos ou omissões que no momento em que se cometerem não forem crimes segundo o direito nacional ou internacional. Tão pouco se imporá pena mais grave que a aplicável no momento da comissão do delito.

Especialistas discutem se a incriminação do agente de delitos informáticos estaria ferindo o princípio constitucional da reserva legal ou se o enquadramento do autor do crime deve ser feito nos modelos já existentes de crime. É o que será ventilado no próximo tópico.

2 DA DISCUSSÃO ACERCA DA NECESSIDADE DE NOVO DIPLOMA LEGAL

A discussão acerca da exigência de lei específica para penalizar os sujeitos ativos dos chamados crimes virtuais tem dividido a doutrina.

Vicente Greco Filho, motivado por um episódio em que jovens gaúchos obtiveram senhas de usuários de Internet, passando a utilizá-las em proveito próprio em prejuízo dos donos das contas bancárias em 2000, escreveu sobre o tema.

Em tom de desabafo, o citado professor entende que, no caso dos garotos do Rio Grande do Sul, foi praticado o conhecido crime de estelionato, tipificado no art. 171 do nosso Código Penal. Explica que houve vantagem ilícita (consistente em se beneficiar do usufruto do provedor, em prejuízo do titular da conta), mediante meio fraudulento (uso indevido de senha), induzindo e mantendo o provedor em erro.

Após afirmar que seria erro grave e perigoso de política penal querer definir crimes específicos, conclui que

> nada existe de especial na possível proteção aos bancos de dados informatizados. Isso porque, ou pertencem eles à esfera da intimidade, ou à esfera da prática comercial ou industrial e, nesses campos, sua proteção

> penal deve ser tratada, independentemente de a violação ocorrer por meio da informática.[76]

Finaliza com a afirmação de que o Direito Penal está perfeitamente apto a atender à proteção dos direitos básicos das pessoas e, caso haja modificação, esta deve ser feita dentro de uma perspectiva de proteção genérica de um bem jurídico.

Em artigo produzido em 1984 e publicado em diversas revistas jurídicas, Valdir Sznick, após elencar as principais técnicas de uso não autorizado do computador, tais como "lata de lixo" e "cavalo de Tróia", afirma que ditas condutas estão abrangidas pelo Código Penal atual e, por conseguinte, podem ser consideradas como crime.

Enumera uma série de modalidades criminosas que podem ser cometidas por meio do computador, quais sejam: estelionato, falsificação de documento público e particular, crimes contra a inviolabilidade de correspondência, expedição de duplicata simulada, crimes contra o privilégio de invenção, divulgação de segredo ou violação de segredo profissional, além dos crimes contra a honra.

Apesar de entender, tal como Vicente Greco Filho, que o Direito Penal se faz suficiente para proteger os bens jurídicos colocados em discussão, não descarta a possibilidade de criação de um novo tipo penal a fim de englobar mais especificamente essas condutas:

> Embora entendamos que o direito penal atual pelos tipo supra apontados já oferece proteção aos crimes cometidos por meio do computador – e de toda a parafernália da informática – somos de opinião que a ereção de um delito novo englobaria melhor todas as modalidades dessas condutas delitivas, obviando dificuldades oriundas da apuração do meio empregado e da fraude ocorrida. Assim sob a epígrafe do 'Uso indevido da computação', abranger-se-iam todas as condutas oriundas do 'uso indevido de computador' e o 'uso de computador por pessoa não autorizada'[77]

---

[76]GRECO FILHO, Vicente. Algumas Observações sobre o Direito Penal e a Internet. *Revista Direito Mackenzie*. São Paulo: Universidade Presbiteriana Mackenzie, 2000, p. 35.
[77]SZNICK, Valdir. O Delito e o Computador. *Revista Trimestral de Jurisprudência dos Estados,* ano 8, vol. 26, São Paulo: Vellenich, 1984, p. 70.

A maioria dos doutrinadores pesquisados é da opinião de que os crimes informáticos merecem uma tipificação específica, sob pena de serem os magistrados obrigados a absolver os acusados pela falta de lei em nosso ordenamento jurídico.

Mário Antônio Lobato de Paiva cita sentença proferida na Argentina em que o Juiz Federal foi obrigado a absolver os réus, acusados de violar o sistema da página *web* da Suprema Corte de Justiça da Nação, substituindo-a por outra, alusiva ao aniversário de falecimento do jornalista José Luis Cabazes.

> Entendeu o juiz que os artigos referem-se especificamente a ataques à materialidade, utilidade ou disponibilidade de coisas, encontrando, com isso, obstáculo no enquadramento de conduta em epígrafe como crime, o que culmina na atipicidade do feito sob julgamento. Para ele (o juiz), não é possível considerar página *web* de Corte Suprema de Justiça da Nação como uma coisa, nos termos em que esta deve ser entendida. "Coisa", definida no art. 2.311 do Código Civil da Nação, é objeto material suscetível de ter um valor.[78]

Ademais, o juiz destaca que uma interpretação extensiva implicaria claro menoscabo ao princípio da legalidade, uma vez que tais delitos não possuem enquadramento legal no Código Penal da Nação.

O autor concorda com o juiz argentino e defende a criação de leis específicas para tipificar essas condutas perpetradas pelo uso das novas tecnologias, acompanhadas de sanções penais específicas que coíbam a prática dos delitos virtuais que podem causar graves danos à comunidade.

Na mesma linha de pensamento, Maria Helena Junqueira Reis propõe a criação de uma lei específica sobre *computer crimes* – desde que não seja casuística devido à velocidade do avanço da tecnologia –, a ampliação do conceito de "coisa", "fraude" e "documento" para abarcar o mundo virtual e criminalizar o "acesso não autorizado a certos bancos de dados", como o das autarquias e do Poder Judiciário.[79]

---

[78]PAIVA, Mário Antônio Lobato de. A Atipicidade dos Delitos Cometidos na Internet. *Revista Síntese de Direito Penal e Processual Penal,* ano V, n. 26. Belo Horizonte: Síntese, 2004, p. 155-156.
[79]REIS, Maria Helena Junqueira. *Computer Crimes.* Belo Horizonte: Del Rey, 1997, p. 55.

Túlio Vianna também segue a tese de que se faz necessária a criação de dispositivos capazes de dar tipicidade aos delitos em comento, mas, diferentemente de Mário Antônio Lobato de Paiva, não acredita que a solução esteja na criação de novas leis específicas. Para Túlio Vianna, bastaria o acréscimo de um artigo ao Código Penal brasileiro e traz uma sugestão em sua obra. Trata-se da inserção do artigo 154-A na Parte Especial, Título I, Capítulo VI, da seguinte Seção V, por ele criada:

> Seção V – Dos Crimes contra a inviolabilidade de dados informáticos
>
> Art. 154-A. Acessar, sem autorização, dados ou programas em sistema computacional.
>
> Pena – prestação de serviços à comunidade ou a entidades públicas, de 1 (um) a 2 (dois) anos e multa.
>
> § 1º A pena será reduzida de um a dois terços ou o juiz aplicará somente a pena de multa se o agente não tinha intenção de lucro ou de obter vantagem de qualquer espécie para si ou para outrem e foi pequeno o prejuízo para a vítima.
>
> § 2º Aumenta-se a pena de um terço até metade:
>
> I – se o crime é cometido contra sistema computacional da União, Estado, Distrito Federal, Município, órgão ou entidade da administração direta ou indireta ou de empresa concessionária de serviços públicos;
>
> II – se o crime é cometido por funcionário público ou por quem exerça a função de administrador de sistemas ou assemelhada, com abuso de poder ou com violação de dever inerente a função;
>
> III – se o agente destrói ou danifica o sistema computacional ou dados nele armazenados;
>
> IV – se o agente divulga a terceiros as informações obtidas, causando dano material ou moral à vítima.
>
> § 3º A pena prevista neste artigo será cumprida preferencialmente por meio de tarefas que aproveitem as aptidões do condenado, especialmente no desenvolvimento de *softwares* com código aberto para entidades

> públicas e no treinamento em informática de funcionários públicos e da comunidade em geral.
>
> § 4º Somente se procede mediante representação, salvo na hipótese do § 2º, II, em que a ação é pública incondicionada.[80]

Na mesma esteira de pensamento encontra-se Augusto Rossini,[81] que sugere a modificação no campo penal, porém defende que não há necessidade de se criar uma nova estrutura. Augusto Rossini é pela adaptação dos delitos telemáticos à realidade brasileira, fazendo inserir novos tipos ao Código Penal existente. Inicia com a criação dos arts. 163-A e 163-B, cuja ação penal somente se procederia mediante queixa:

> Dano a dado, programa de computador, banco de dados ou mecanismos de acesso.
>
> Art. 163-A. Apagar, destruir, modificar ou de qualquer forma inutilizar, total ou parcialmente, dado, programa de computador, banco de dados ou mecanismos de acesso, armazenados em meios eletrônicos, com a utilização de meio fraudulento ou de forma não autorizada.
>
> Pena: detenção, de 3 (três) meses a 1 (um) ano e multa.
>
> Parágrafo único: Se o crime é cometido:
>
> I – contra o interesse da União, Estado, Distrito Federal, Município ou órgão ou entidade da administração direta ou indireta, ou de empresa concessionária de serviços públicos;
>
> II – com intuito de lucro ou vantagem de qualquer espécie, própria ou de terceiro; ou
>
> III – com o uso indevido de senha ou processo de identificação de terceiro.
>
> Pena: detenção, de 6 (seis) meses a 2 (dois) anos e multa.
>
> Art. 163-B. Disponibilizar ou utilizar dado ou programa de computador em meios eletrônicos com a finalidade de apagar, destruir, inutilizar ou modificar dado, programa de computador, banco de dados ou mecanismos

[80]VIANNA, Túlio Lima. *Fundamentos de Direito Penal Informático*. Rio de Janeiro: Forense, 2003, p. 91-92.
[81]ROSSINI, Augusto. *Informática, Telemática e Direito Penal.* São Paulo: Memória Jurídica Editora, 2004, p. 236-244.

> de acesso, ou se de qualquer forma dificultar ou impossibilitar total ou parcialmente a utilização de meios eletrônicos.
>
> Pena: detenção, de 1 (um) a 3 (três) anos e multa (...)"

Acrescenta, ainda, o mesmo autor um inciso no § 4º do art. 150 do CP, que trata dos crimes contra a inviolabilidade do domicílio para compreender, na expressão "casa", o "sistema informático ou telemático com acesso indevido ou não autorizado".

Cria, também, o art. 150-A para tipificar o acesso não autorizado ou fraudulento, com as mesmas qualificadoras sugeridas para o art. 163-A:

> Art. 150-A. Obter acesso não autorizado, ou com utilização de meio fraudulento, de dados, programas de computador, banco de dados ou mecanismos de acesso armazenados em meios eletrônicos, com a utilização de meio fraudulento ou de forma não autorizada.

Augusto Rossini vê necessidade de adicionar um parágrafo ao art. 150 do atual Código Penal que trata da violação de correspondência a fim de equiparar a figura do correio eletrônico (*e-mail*) à correspondência fechada.

E, por fim, indica mais uma possível inovação com a criação do seguinte art. 297-A no rol de crimes de falsidade documental:

> Art. 297-A. Considera-se documento a declaração escrita, de autoria identificável, idônea, a provar fato juridicamente relevante.
>
> Documento por equiparação
>
> § 1º Equipara-se a documento o impresso, a cópia ou a reprodução de documento, devidamente autenticados por pessoa ou processo mecânico legalmente autorizados, bem como todo o dado, instrução ou programa de computador constantes de processamento ou comunicação de dados ou de qualquer suporte físico.
>
> § 2º Equipara-se a documento público o emanado de entidade autárquica ou de fundação instituída pelo poder público.

Como se vê, salvo raras exceções, os especialistas em matéria de direito de informática são favoráveis a uma nova tipificação para alcançar os delitos praticados contra os sistemas de tecnologia de informatização. Essa tendência pode ser sentida não somente no Brasil, mas também em vários outros países conforme já foi explanado supra.

3 DE LEGE FERENDA

A nova lei a ser promulgada vem com a força do aval concedido pela maioria da doutrina especializada na matéria de direito de informática.

Como já foi dito anteriormente, o Projeto de Lei n. 84/99 (PLC 89/03) foi eleito para servir de base para o debate, por ser o mais completo entre aqueles que tramitam no Congresso Nacional.

O projeto em comento foi elaborado por uma comissão sob a coordenação do professor José Henrique Barbosa Moreira Lima Neto, atendendo a pedido do citado parlamentar, e composta por juristas de alto escalão como o Professor Damásio Evangelista de Jesus e o Dr. Carlos Alberto Etcheverry.[82]

O primeiro capítulo do Projeto de Lei – que regula o uso de bancos de dados, a prestação de serviços por redes de computadores e dispõe sobre os crimes cometidos na área de informática – estabelece os princípios reguladores da prestação de serviços por redes de computadores.

Dispõe o art. 2º do projeto que "o acesso, o processamento e a disseminação de informações através das redes de computadores devem estar a serviço do cidadão e da sociedade, respeitados os critérios de garantia dos direitos individuais e coletivos e de privacidade e segurança de pessoas físicas e jurídicas e da garantia de acesso às informações disseminadas pelos serviços da rede".

---

[82]BRITO, Eduardo Valadares de. *Crimes na Internet.* Disponível em: <http://www.ibdi.org.br.> Acesso em: 22 abr 2007.

No capítulo seguinte, regula o uso de informações disponíveis em computadores ou redes de computadores.

Para merecer proteção do uso do sistema de informática, o projeto indica que necessário faz-se a pessoa, física ou jurídica, ser identificada ou identificável. Prevê o PL 84/99 um cadastramento por meio do qual será dado conhecimento das informações privadas armazenadas a ela referentes, ou seja, as informações privadas somente serão divulgadas na rede sob a aquiescência da pessoa a que se referem. Obrigará, ainda, caso aprovado, que aqueles que se servem de informações privadas dos usuários da Internet expliquem os fins para que se destinam as informações.

Adotou, assim, o projeto de lei, mecanismo de controle sobre a coleta, o armazenamento, o processamento e a transmissão de dados.

O terceiro capítulo prevê os *computer crimes* propriamente ditos com suas conseqüentes penas, criando seis novos tipos penais, em seis seções diversas, quais sejam:

> Dos Crimes de Informática
>
> Seção I - Acesso indevido ou não autorizado
>
> Art. 9º Acesso, indevido ou não autorizado, a dados ou informações armazenadas no computador ou em rede de computadores.
>
> Pena - detenção, de um mês a um ano, e multa.
>
> Parágrafo único. Na mesma pena incorre quem, sem autorização ou indevidamente, obtém, mantém ou fornece a terceiro meio de acesso a computador ou rede de computadores.
>
> Seção II - Alteração de senha ou meio de acesso a programa de computador ou dados
>
> Art. 10. Apagar, destruir, alterar, ou de qualquer forma inutilizar senha ou qualquer outro meio de acesso a computador, programa de computador ou de dados, de forma indevida ou não autorizada.
>
> Pena - detenção, de seis meses a dois anos, e multa.

Seção III - Obtenção, manutenção ou fornecimento indevido, ou não autorizado, de dado ou instrução de computador

Art. 11. Obter, manter ou fornecer, de forma indevida ou não autorizada, dado ou instrução de computador.

Pena - detenção, de um mês a um ano, e multa.

Seção IV - Dano a dado ou programa de computador

Art. 12. Apagar, destruir, modificar ou de qualquer forma inutilizar, total ou parcialmente, dado ou programa de computador, de forma indevida ou não autorizada.

Pena - detenção, de um a seis meses, e multa.

Seção V - Criação, desenvolvimento ou inserção em computador de dados ou programa de computador com fins nocivos

Art. 13. Criar, desenvolver, inserir ou fazer inserir, dado ou programa de computador, em computador ou rede de computadores, de forma indevida ou não autorizada, com a finalidade de apagar, destruir, inutilizar ou modificar dado ou programa de computador, ou de qualquer forma dificultar ou impossibilitar, total ou parcialmente, a utilização de computador ou rede de computadores, ou o acesso a estes.

Pena - detenção, de um ano a dois anos, e multa.

Seção VI - Violação de segredo armazenado em computador, meio magnético, de natureza magnética, óptica ou similar

Art. 14. Obter ou fornecer segredos, de indústria ou comércio, ou informações pessoais armazenadas em computador, rede de computadores, meio eletrônico de natureza magnética, óptica ou similar, de forma indevida ou não autorizada.

Pena - detenção, de seis meses a dois anos, e multa."

Diante dos dispositivos acima, pode-se dizer que os reclames da doutrina foram atendidos. Contempla o projeto o acesso a sistemas computacionais sem autorização, apenando também o dano causado aos *softwares* de computadores.

Para Roberto Chacon de Albuquerque, não é o acesso aos dados ou às informações armazenadas que deve ser objeto de sanção penal, mas "a tomada de conhecimento de dados armazenados, processados ou transmitidos por sistemas informáticos, desde que se infrinja alguma medida de segurança para sua proteção".[83]

O mesmo autor critica o art. 13 do PL 84/99, pois, para ele, não se deve penalizar aquele que cria dado ou programa de computador, em computador ou rede de computadores de forma indevida ou não autorizada, uma vez que a criação pode ocorrer com fins educativos.

O derradeiro capítulo é o das disposições finais que regulam os requisitos formais e instrumentais da lei para a coação legal dos crimes.

É previsto aumento da pena de um sexto até metade caso qualquer dos crimes elencados seja praticado no exercício de atividade profissional ou funcional. Há, outrossim, qualificadoras no caso de o crime ser cometido contra a administração direta ou indireta, com considerável prejuízo para a vítima, com intuito de lucro ou vantagem de qualquer espécie, própria ou de terceiro, com abuso de confiança, por motivo fútil, com o uso indevido de senha ou processo de identificação de terceiro ou com a utilização de qualquer outro meio fraudulento, a pena sobe para reclusão de dois a seis anos e multa.

A pena pode ser considerada severa, tendo em vista que o crime de estelionato (art. 171 do CP) é apenado com reclusão de um a cinco anos e multa e, na modalidade mais grave, aumenta-se a pena em um terço.

Finaliza declarando que os crimes somente se procedem mediante queixa ou representação do ofendido, salvo exceções, casos em que será de ação penal pública incondicionada, por exemplo, quando cometidos contra interesse da União, de Estado, do Distrito Federal ou de Município.

Após os breves comentários a respeito da nova lei sobre crimes informáticos, pode-se perceber que o diploma legal responde aos anseios da sociedade, porque confere segurança à população e retira a sensação de impunidade, além de atender

[83]ALBUQUERQUE, Roberto Chacon de. *A Criminalidade Informática.* São Paulo: Juarez de Oliveira, 2006, p. 148.

às normas de técnica legislativa e aos reclames do mundo jurídico, de magistrados e de doutrinadores.

CONSIDERAÇÕES FINAIS

Ao longo do presente trabalho monográfico, tentou-se explicar a informática e a Internet por meio de seus contextos históricos e definições a fim de demonstrar a importância do tema, tendo em vista a verdadeira invasão tecnológica a que presenciamos.

E, diante da constante mutação da sociedade, pois é dinâmica, o jurista deve estar preparado para enfrentar esses novos desafios que se apresentam. Por isso, a informática merece estudo aprofundado e a preocupação dos operadores do direito.

A despeito das opiniões em contrário, mormente a do célebre Professor Vicente Greco Filho, no nosso sentir, faz-se necessária, sim, a elaboração de um novo diploma legal para abarcar delitos virtuais e desfazer esse vácuo legislativo que testemunhamos nos dias atuais. Não fosse assim, em certos casos, seríamos obrigados a aplicar a analogia e os costumes para enquadrar criminosos, o que, conforme já foi dito, não traduz melhor técnica de política criminal, tendo em vista que o uso dessas fontes em prejuízo do acusado é proibido.

A existência do princípio da reserva legal implica segurança jurídica. No Direito Penal, como *ultima ratio*, é subsidiário de todos os outros ramos do direito; o princípio da reserva legal deve ser absoluto, somente podendo privar alguém de sua liberdade mediante lei prévia, certa e determinada.

Repise-se que precisamos de novas tipificações de crimes informáticos, entretanto somente os classificados como próprios ou puros supra, entendendo-se como aqueles praticados contra o sistema de computadores em si mesmos. Os chamados impróprios (ou impuros), mistos e comuns já se encontram devidamente tipificados no ordenamento jurídico pátrio, uma vez que o manuseio do computador e da Internet é mero meio, simples modificação no *modus operandi* do delito, não implicando novo delito.

Quanto à discussão acerca da maneira como deve ser modificada a legislação – se se deve atualizar o Código Penal ou criar novo diploma legal –, somos pela segunda corrente. Isso porque permitiria aos magistrados a aplicação de uma norma certa, mais específica do que a mera introdução de artigos, parágrafos e incisos no Código atual.

A futura lei penal geral sobre delitos informáticos trará, em seu bojo, princípios específicos relacionados ao tema, permitindo uma penalização própria aos delitos ali preconizados, e, mais importante, admitirá uma análise pormenorizada dos crimes informáticos. Além do mais, a elaboração de uma lei específica sobre os crimes cometidos na área de informática facilitará a interpretação de forma sistemática, segundo a qual uma lei não existe isoladamente, mas em conjunto com outras pertencentes à sua mesma classe.

Merece elogios o Projeto de Lei n. 84/99 quanto à sua forma. Trata-se de lei específica sobre crimes informáticos, mas não é fechada o bastante para impedir que novos delitos sejam enquadrados. Considerando a constante evolução do mundo virtual, devemos estar preparados para a possibilidade de surgimento de novos tipos penais.

Assim, entendemos que há urgência na aprovação do Projeto de Lei ora comentado. Não é concebível deixar de se condenarem verdadeiros criminosos virtuais por falta de legislação. O projeto foi proposto há sete anos e daquela época aos dias atuais inúmeros malfeitores informáticos deixaram de ser condenados porque a justiça esbarrou na burocracia a que somos dependentes no nosso país.

BIBLIOGRAFIA

ALBUQUERQUE, Roberto Chacon de. *A Criminalidade Informática.* São Paulo: Juarez de Oliveira, 2006.

ARAS, Vladimir. *Crimes de Informática. Uma Nova Criminalidade.* Disponível em: <http://www1.jus.com.br/doutrina/texto.asp?id=2250>. Acesso em 12 out 2006.

BRITO, Eduardo Valadares de. *Crimes na Internet.* Disponível em: <http://www.ibdi.org.br> Acesso em 22 abr. 2007.

CASTRO, Carla Rodrigues Araújo de. *Crimes de Informática e seus Aspectos Processuais.* 2. ed., rev., atual. Rio de Janeiro: Lumen Juris, 2003.

_____. *Impunidade na Internet.* Disponível em: <http://www.direitonaweb.adv.br/doutrina/dinfo/Carla_R_A_Castro_(DINFO_0001).htm>. Acesso em: 12 out. 2006.

COSTA, Marcelo Antonio Sampaio Lemos. *Computação Forense.* 2. ed. Campinas: Millennium, 2003.

COSTA, Marco Aurélio Rodrigues da. *Crimes de Informática*. Disponível em: <http://jus2.uol.com.br/doutrina/texto.asp?id=1826>. Acesso em: 22 abr. 2007.

FEDELI, Ricardo Daniel *et alli. Introdução à Ciência da Computação.* São Paulo: Thomson Pioneira, 2003.

FERREIRA, Pinto. A Era da Informática e a Juscibernética. *Revista da Academia Brasileira de Letras Jurídicas,* ano XIX, n. 22. Rio de Janeiro: Renovar, 2002.

FURLANETO NETO, Mário *et alii*. Crimes na Internet: elementos para uma reflexão sobre a ética informacional. *Revista CEJ,* ano VII, n. 20. Brasília: Conselho da Justiça Federal, 2003.

GOMES, Luiz Flávio. *Direito Penal*. Vol. 3. 2. ed., rev., atual. e ampl. São Paulo: Revista dos Tribunais, 2006.

GRECO FILHO, Vicente. Algumas Observações sobre o Direito Penal e a Internet. *Revista Direito Mackenzie*, nº 1, São Paulo: Universidade Presbiteriana Mackenzie, 2000.

JESUS, Damásio Evangelista de. *Código Penal Anotado.* 11. ed., rev. e atual. São Paulo: Saraiva, 2001.

LUISI, Luiz. *Os Princípios Constitucionais Penais*. 2. ed. Porto Alegre: Sergio Antonio Fabris Editor, 2003.

MEIRA, José de Castro. *Crimes de Informática*. Disponível em: <http://buscalegis.ccj.ufsc.br/arquivos/crimes_informatica_meira.html>. Acesso em: 12 out. 2006.

MOREIRA, Rui. *Introdução à Informática.* Disponível em: <http://www2.ufp.pt/~rmoreira/ MTC/Aula3_II.pdf>. Acesso em: 22 abr. 2007.

PAIVA, Mário Antônio Lobato de. A Atipicidade dos Delitos Cometidos na Internet. *Revista Síntese de Direito Penal e Processual Penal,* ano V, n. 26. Belo Horizonte: Síntese, 2004.

_____. Delitos Virtuais. *Revista Jurídica Consulex*, ano VI, n. 138. Brasília: Consulex, 2002.

PLANTULLO, Vicente Lentini. *Estelionato Eletrônico.* Curitiba: Juruá, 2005.

RAHAL, Flávia; GARCIA, Roberto Soares. Crimes e Internet – Breves Notas aos Crimes Praticados por Meio da Rede Mundial e Outras Considerações. *Boletim IBCCrim,* ano 9, n. 110, São Paulo: IBCCrim, 2002.

REINALDO FILHO, Demócrito. Crimes Cometidos na Internet: Questões Técnicas Dificultam Condenações. *Revista Síntese de Direito Penal e Processual Penal,* ano V, n. 26, Belo Horizonte: Síntese, 2004.

REIS, Maria Helena Junqueira. *Computer Crimes.* Belo Horizonte: Del Rey, 1997.

RODRIGUES, Francisco de Assis. *A Tutela Penal dos Sistemas de Computadores.* Disponível em: <http://www1.jus.com.br/doutrina/texto.asp?id=2813>. Acesso em: 12 out. 2006.

ROSA, Antônio José M. Feu. Dos Crimes Virtuais. *Revista Jurídica Consulex,* ano V, n. 105, Brasília: Consulex, 2001.

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

ROSSINI, Augusto. *Informática, Telemática e Direito Penal.* São Paulo: Memória Jurídica Editora, 2004.

SILVA, Rita de Cássia Lopes da. *Direito Penal e Sistema Informático.* São Paulo: Revista dos Tribunais, 2003.

SZNICK, Valdir. O Delito e o Computador. *Revista Trimestral de Jurisprudência dos Estados,* ano 8, vol. 26, São Paulo: Vellenich, 1984.

TORON, Alberto Zacharias. Crimes na Internet. *Repertório de Jurisprudência,* n. 22, 3º Caderno. São Paulo: IOB, 2000.

VALIN, Celso. A Questão da Jurisdição e da Territorialidade nos Crimes Praticados pela Internet. In: ROVER, Aires José (org). *Direito, Sociedade e Informática:* Limites e Perspectivas da Vida Digital. Florianópolis: Fundação Boiteux, 2000.

VIANNA, Túlio Lima. Dos Crimes por Computador. *Revista dos Tribunais,* ano 91, vol. 801, São Paulo: Revista dos Tribunais, 2002.

_____. *Fundamentos de Direito Penal Informático.* Rio de Janeiro: Forense, 2003.