SERGIO MAURICIO PREBIANCA

PERSPECTIVAS PROCESSUAIS

PARA OS CRIMES DE INFORMÁTICA

Curitiba

2002

SERGIO MAURICIO PREBIANCA

PERSPECTIVAS PROCESSUAIS

PARA OS CRIMES DE INFORMÁTICA

Monografia elaborada por Sergio Mauricio Prebianca, como requisito parcial à conclusão do curso de Direito, do Setor de Ciências Jurídicas da Universidade Federal do Paraná.

Orientador: Prof. Nilton Bussi

Curitiba

2002

TERMO DE APROVAÇÃO

SERGIO MAURICIO PREBIANCA

PERSPECTIVAS PROCESSUAIS PARA OS CRIMES DE INFORMÁTICA

Monografia aprovada como requisito parcial para conclusão do curso de Direito, do Setor de Ciências Jurídicas da Universidade Federal do Paraná, pela seguinte banca examinadora:

Orientador: Prof. Nilton Bussi
Departamento de Direito Penal, UFPR

Prof. Juliano Breda
Departamento de Direito Penal, UFPR

Prof. Rolf Koerner Jr.
Departamento de Direito Penal, UFPR

Prof. Ricardo Rachid de Oliveira
Departamento de Direito Penal, UFPR

Curitiba

2002

Aos meus pais Ruth e Pedro Prebianca.

Agradeço ao professor e orientador Nilton Bussi, pelo acompanhamento sério e contínuo prestado durante a elaboração deste trabalho.

SUMÁRIO

RESUMO

Este trabalho é direcionado aos operadores do Direito, portanto, sua transcrição não se deterá a considerações técnicas aprofundadas do campo da informática, tornando sua compreensão mais facilitada. Na primeira parte apresenta um histórico da internet, por sua relevância devido à revolução das comunicações que têm se operado. Portanto, expõe desde o surgimento da internet, sua evolução, suas aplicações e características, até suas tendências. Ainda traz uma reflexão sobre o que se entende por crimes de informática, o perfil dos problemas que a utilização criminosa dos modernos meios de comunicações têm originado e as modalidades delituosas cometidas mediante equipamentos de informática. Na segunda parte desvela algumas considerações que parecem relevantes no tocante aos aspectos processuais penais dos crimes de informática, sejam eles: a) As limitações que prejudicam a investigação, a falta de recurso material e humano; b) A obtenção da prova, face aos crimes por computadores e os métodos de obtenção destas; c) O exótico perfil do delinqüente que ameaça o ciberespaço; d) Uma reflexão pertinente sobre a questão da jurisdição, devido ao caráter internacional que podem permear os crimes perpetrados pela supervia da informação; e) A possibilidade da prisão em flagrante nesses crimes; f) As penas alternativas, como uma opção de pena adequada para a maioria dos delitos praticados por meio da informática. Traz, por fim a conclusão e um capítulo adicional com um glossário para facilitar a compreensão, contendo alguns dos termos técnicos mais usados nesse trabalho monográfico e pelo uso cotidiano daqueles que têm um contato com essa parafernália tecnológica.

Palavras-chave: Crimes de informática – crimes por computador– crimes virtuais – crimes digitais – crimes de alta tecnologia – cibercrimes – criminalidade informática – crimes pela Internet – delito informático – delito eletrônico – novas modalidades criminosas – segurança das informações.

ABSTRACT

This work is directed to law operators, so, its transcription won't be detained to deep technical considerations, concerning to the informatics' field. In so doing, the understanding becomes easy. The first part presents an Internet description, because of its significance due to the revolution of communication that has been taking place. Therefore, it relates since the beginning of Internet, its evolution, applications and characteristics, until its tendencies. Still in this part, there is a reflection about the conception of crimes via informatics' devices, the problems' outline originated from the criminal use of modern communication means and the criminal modalities perpetrated by informatics' devices. The second part shows some essential considerations about penal suit aspects of informatics crimes, such as: a) limitations that prejudice the investigation, the human and material resources deficiency; b) The obtainment of proofs concerning to computer crimes; c) The exotic outline of cyberspace delinquent; d) An essential reflection about the jurisdictional question, because of the international nature of these crimes; e) The possibility of catching the criminal in the act; f) Alternative punishments as an option of adequate punishment to the most crime perpetrated via informatics. Finally, you'll find out a conclusion and an additional chapter with a glossary to make the understanding easier. It contains the most used terms in this monographic work and some terms for daily.

Key-words: informatics crimes – computer crime – virtual crimes – digital crimes – high technology crimes – cybercrimes – crimes via Internet – electronic crimes – new criminal modalities – information security.

1. INTRODUÇÃO

Estamos vendo o emergir de uma nova civilização. Afloram novos comportamentos, novos estilos de família, novos modos de trabalhar, de amar, novos modos, enfim, de viver. Estamos no alvorecer de um novo tempo, é esse estágio denominada pelo autor norte-americano Alvin TOFFLER de "terceira onda".

Segundo TOFFLER, o significado disso é que a humanidade enfrenta uma sublevação social e a reestruturação criativa mais profunda de todos os tempos. Sem nos darmos conta nitidamente, estamos criando desde os alicerces uma notável e nova civilização.

TOFFLER enxerga a história como uma sucessão de estágios de progresso, com a ocorrência de conflitos a cada vez que uma onda é substituída por outra.

A primeira onda, decorre da revolução agrícola. A segunda onda relativa à civilização industrial, que durou apenas uns poucos 300 anos.

A Terceira Onda evidencia a moribunda civilização industrial, gradativamente cedendo espaço à uma civilização emergente tocada por mudanças: **o avanço tecnológico**.

Nesta fase as relações econômicas são influenciadas pela informática e a informação é o negócio mais importante e que mais cresce no mundo. É a onda que estamos vivenciando[1].

A internet é o símbolo que sintetiza essa convergência da tecnologia e da informação.

A nossa rotina foi invadida por uma inundação eletrônica: As redes informatizadas, os caixas eletrônicos de banco, o voto

---

[1] TOFFLER, Alvin. **A Terceira Onda**. 10ª ed. Rio de Janeiro: Editora Record. 1980. p.18.

eletrônico, a telefonia móvel, a realidade virtual etc. Tudo isto tão recente e já faz parte íntima de nossas vidas.

Infelizmente esses novos instrumentos nas mãos dos delinqüentes vieram a fazer parte também de meios inéditos de cometer crimes.

Tornou-se necessário, portanto, o intercâmbio entre os ramos do conhecimento humano para poder dar conta dessas novas modalidades delituosas.

A moderna Ciência do Direto que já vinha sofrendo influências da Sociologia, da Filosofia, da Psicologia Forense, da Medicina Legal, e da Antropologia, por exemplo, agora terá de abrir espaço para novas confluências, ao passo que as relações intersubjetivas sofrem influxos com contornos diferentes, compondo um novo código de comportamento.

A evolução tecnológica também proporcionou uma nova dimensão da criminalidade. A tecnologia trouxe um "*modus operandi*" até então inimaginável para os legisladores que criaram o nosso Código Penal.

Essas novas modalidades criminosas têm encontrado espaço na supervia da informação, a Internet. Um ambiente digital que é muito atraente por facilitar o relacionamento "virtual" ilimitado, ou seja, com o mundo todo, permitindo que o sujeito permaneça no anonimato.

Nesse ambiente, o contato direto entre autor e vítima tornou-se apenas virtual e os meios de execução foram simplificados a um simples aparato eletrônico.

É difícil exprimir o número total de usuários da rede mundial de computadores, porque se desatualiza muito rapidamente, considerando a velocidade com que esse número cresce. Ora, temos hoje mais de 250 (duzentos e cinqüenta) milhões de usuários de

computador em todo o planeta e que, em mais de 190 países, acessam a Internet e trocam dados, sons e imagens[2]. Há previsão que dois bilhões de pessoas deverão ser usuárias da Internet em 2007.

O Direito Penal e Processual Penal não podem, sob o argumento de estar em desconsonância com a tecnologia, deixar de tutelar bens jurídicos confiados por esses bilhões de sujeitos.

Toda reflexão atual sobre os crimes de informática está sendo muito conveniente, considerando que estão prestes a serem aprovadas uma série de leis que regularão o ciberespaço.

Se faz necessário aprimorar e estimular a discussão sobre questões modernas e polêmicas que têm surgido com a popularização da rede mundial de computadores, a Internet. Por conta disso, objetivou-se neste trabalho descrever as origens da grande rede, sua estrutura e suas limitações, tendo-a sempre em foco como meio da prática de delitos, como evitá-los e como puni-los.

Aponta-se algumas questões processuais relevantes, tais como: o procedimento investigatório da polícia na persecução do delinqüente do ciberespaço, bem como o perfil desta espécie de criminoso; da validade da prova virtual no processo; dos recursos deficientes para combater os crimes de informática; da polêmica em torno do lugar do crime; da falta de legislação específica etc.

Não se pretendeu, nem de longe esgotar algum dos assuntos aqui tratados, mas colher das poucas sementes que já foram lançadas e nos debruçar principalmente sobre as questões do Direito Processual Penal, devido ao pequeno espaço a que se destina tal pesquisa.

---

[2] Fonte: http://www.uol.com.br/aprendiz/n_noticias/cbn/id130801.htm, acessado em 03/08/2001

2. DIREITO E INTERNET

2.1 EVOLUÇÃO DA REDE MUNDIAL

"Internet é o nosso jornal diário, o nosso correio, a nossa ferramenta de trabalho, o nosso campo de investigação ou até o nosso refúgio onde se dão grandes passeios ao domingo..." [3]

As comunicações abriram fronteiras através da transmissão de dados de um computador para outro e que, atualmente, demonstra sua força maior na grande rede mundial, a Internet.

A Internet é uma rede internacional de interconexão governamental, educacional e negocial – em essência: "a rede das redes".

Ela deve seu modo e arquitetura incomum por sua origem no projeto Departamento de Defesa norte-americano da ARPAnet em 1969 (o nome deriva de "*Advanced Research Project Agency*", o grupo do Pentágono responsável pelo projeto).

No auge da guerra fria, planejadores militares buscaram projetar uma rede de computador que poderia resistir à uma destruição parcial (como de um ataque nuclear), e continuar funcionando. [4]

Esta rede não possuía um computador central, todos os computadores se intercomunicariam entre si independentemente, buscando vias alternativas de comunicação automaticamente se preciso fosse. Outros muitos fatores tal como a interrupção de energia, linhas de telecomunicações sobrecarregadas, falhas de

---

[3] Fonte: http://www.centroatl.pt/ciberlei/clintro.html. Em 14/05/2002

[4] Fonte: Enciclopédia Digital Grolier. Versão 8.01 (inglês). The 1996 Grolier multimedia encyclopedia.

equipamentos podem degradar o desempenho de uma rede, a solução da ARPAnet também era atraente para redes fora do meio militar.

E foi no início dos anos 80, mais precisamente em 1983, com a adoção dos protocolos TCP/IP ("*Transmission Control Protocol / Internet Protocol*") na ARPAnet (da qual se separou a componente estritamente militar formando a MILnet), a criação da CSNet ("*Computer Science Network*") e a sua ligação à ARPAnet, que surgiu a verdadeira Internet. Entre a década de 80 e o início dos anos 90, a rede é aperfeiçoada: começam a surgir os serviços que dão à Internet sua feição atual.

A economia alcançada com o uso de correio eletrônico (ou "E-mail") foi bastante para o induzimento de muitos empresários investirem pesadamente em equipamento e conexões de rede no começo dos anos 90.

Os empregados de uma grande corporação podiam enviar centenas de milhares de "E-mail" pela Internet todos os meses a um custo muito baixo. Este serviço, atualmente, está substituindo gradativamente os métodos tradicionais da comunicação via correio, telefone e fax que são bem mais caros.

A partir de 1994, a Internet amplia suas funções: além de ser uma rede de circulação de informações, também torna-se um meio de comercialização de produtos e serviços.

É o início do comércio eletrônico. Nos últimos cinco anos o interesse comercial pela internet cresceu substancialmente. Por conta disso haverá um grande incentivo à popularização da grande rede mundial como um novo nicho de mercado prestes a expandir e transformar a rotina das pessoas.

Serviços oferecidos na Internet – Hoje os serviços mais populares da Internet são o "E-mail" (correio eletrônico) e a "*World Wide Web*" (WWW). Pelo "**E-mail**" é possível trocar mensagens com

pessoas ou empresas do mundo inteiro. Na **WWW** encontram-se os chamados "*sites*" ou "*homepages*", páginas criadas por pessoas, empresas, instituições e órgãos governamentais. Elas trazem informações em forma de texto, imagens (fotografia, ilustrações), vídeo e som.

Outros serviços bastante procurados também são o "*listserv*", o "*chat*" e o "*telnet*".

A rede mundial não pertence a nenhum governo ou empresa, é hoje símbolo do fenômeno da globalização e da revolução tecnológica, que traz consigo o mal do desemprego estrutural. Está ocasionando a extinção de várias profissões ao passo que facilita o surgimento de outras tantas. As transformações ocasionadas pelo surgimento da Internet têm se operado gradativamente.

Fala-se hodiernamente em exclusão digital ou "os sem-terra do ciberespaço", devido à pequena porcentagem a quem a Internet é restrita. O acesso da população esbarra ainda no obstáculo do alto preço do microcomputador.[5]

A Internet móvel é outro campo de aplicação da Internet, ampliando as possibilidades de sua utilização.

A Internet2 é uma iniciativa norte-americana existente desde 1996, que envolve 180 universidades norte-americanas, além de agências do governo e indústria; visa o desenvolvimento de novas aplicações como telemedicina, bibliotecas digitais, laboratórios virtuais, dentre outras que não são viáveis com a tecnologia da Internet atual. A infra-estrutura avançada da internet2 a torna muito mais veloz.[6]

---

[5] Rodrigo Pinto **Em defesa dos Sem-Terra do Ciberespaço**. Artigo in http:\\www.cg.com.br em 20/05/2002

2.2 DEFINIÇÃO DE CRIME DE INFORMÁTICA

A partir dessa nova cultura instalada pelo casamento entre tecnologia e comunicação, novas maneiras de praticar atos ilícitos também vieram com a correnteza.

Crimes anteriormente realizados com armas, pelo contato pessoal, agora encontram meios alternativos, onde as distâncias não representam barreiras, os agentes permanecem sentados diante de um computador e a violência é dispensada.

A Internet, que apesar de ser, inegavelmente, um marco na divisão da história da humanidade, ao lado de tantos benefícios que propicia, tem também o seu lado nefasto: pode ser instrumento de crime.

Quando falamos sobre os crimes praticados utilizando os recursos da informática, o primeiro problema que surge é a nomenclatura, em que destacam-se as seguintes: crimes de informática, crimes cibernéticos, crimes por computador, crimes virtuais, crimes digitais, crimes de alta tecnologia, criminalidade informática, crimes pela Internet, delito informático, delito eletrônico. Neste nosso trabalho monográfico adotaremos preferivelmente "crimes de informática".

Definição é uma operação lógica por meio da qual concretizamos os traços essenciais do objeto definido, e, ao mesmo tempo, o diferenciamos de todos objetos que lhe são semelhantes. Nesse ato lógico do pensamento há de residir sempre o propósito de se lograr uma comunicação sem equívoco.

---

[6] Fonte: **http://www.internet2.edu**. Em 29/05/2002

A definição é, portanto, meio para um fim que consiste em indicar a significação de um nome, mas precisá-lo pela determinação do seu conceito.

O conceito de crime de informática não é uniforme entre os doutrinadores. A definição adotada pelo Conselho da Europa e das Comunidades Européias e pela OECD (Organização para a Cooperação Econômica e Desenvolvimento) para o chamado "crime de computador" é qualquer comportamento ilegal, anti-ético ou não autorizado envolvendo processamento automático de dados e/ou transmissão de dados.

Ivette Senise FERREIRA entende como crime de informática toda ação típica, anti-jurídica e culpável contra ou pela utilização de processamento automático de dados ou pela sua transmissão[7].

Ângela Bittencourt BRASIL não vê diferença entre crime comum e crime de informática; salienta, todavia, que a fronteira que os separa é a utilização do computador para alcançar e manipular o seu sistema em proveito próprio ou para lesionar outrem.

O departamento de investigação da "Universidad de México", assinala como delitos informáticos como "todos aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, que hacen uso indebido de cualquier medio Informático".

Adotaremos a definição de Ivette Senise FERREIRA que nos parece caracterizar amplamente os elementos necessários para a criminalização das condutas puníveis.

---

[7] FERREIRA, Ivette Senise. **Os Crimes de Informática**. In: BARRA, Rubens Prestes, ANDREUCCI, Ricardo Antunes. **Estudos Jurídicos em Homenagem a Manoel Pedro Pimentel**. São Paulo : RT, 1992. p.141.

É crime de informática "puro" toda e qualquer conduta ilícita que tenha por objetivo exclusivo o sistema de computador, seja pelo atentado físico ou técnico do equipamento e seus componentes, inclusive dados e sistemas[8]. São exemplos o acesso não autorizado a banco de dados, alterações de informações em banco de dados, invasões de sites e a criação, inserção e disseminação de "vírus".

O legislador não criou óbices para tipificação de uma prática realizada pelo mundo virtual. Estes são os chamados crimes virtuais "impuros". Nestes casos, bastaria aplicar a legislação penal atual.

Crime de informática impuro (ou comum) são todas aquelas condutas em que o agente se utiliza do sistema de informática como mera ferramenta a 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.

Crime de informática misto são todas aquelas ações em que o agente visa a um bem juridicamente protegido diverso da informática, porém, o sistema de informática é ferramenta imprescindível a sua consumação.

No final do século XIX um cidadão alemão foi preso acusado de furto de energia elétrica. Os advogados do acusado, entretanto, observaram que não existia na legislação penal alemã para tal delito, pois a energia elétrica não tinha *"status"* de coisa, e somente coisa poderia ser passível de furto. O tribunal absolveu o réu ao entender que a lei penal não permite interpretação analógica. Com isso, o legislador alemão providenciou logo um dispositivo legal que

---

[8] COSTA, Marco Aurélio Rodrigues. **Crimes de Informática**. In http://www.jus.com.br/doutrina/crinfo1.htm. Acessado em 23/03/2002.

tipificasse como crime o furto de energia elétrica, pois sem a mesma, aqueles que viessem a desviar a energia elétrica ficariam impunes[9].

No final do século XX surgiram lacunas na lei decorrentes de atos e fatos que acontecem mediante o uso dos computadores na Internet, porém a repreensão aos novos crimes virtuais que afloram em nosso meio deverá cumprir o princípio da reserva legal, disposta no artigo 1º do Código Penal Brasileiro e consagrado pelo artigo 5º, XXXIX da Constituição Federal de 1988: "Não há crime sem lei anterior que o defina. Não há pena sem prévia cominação legal".

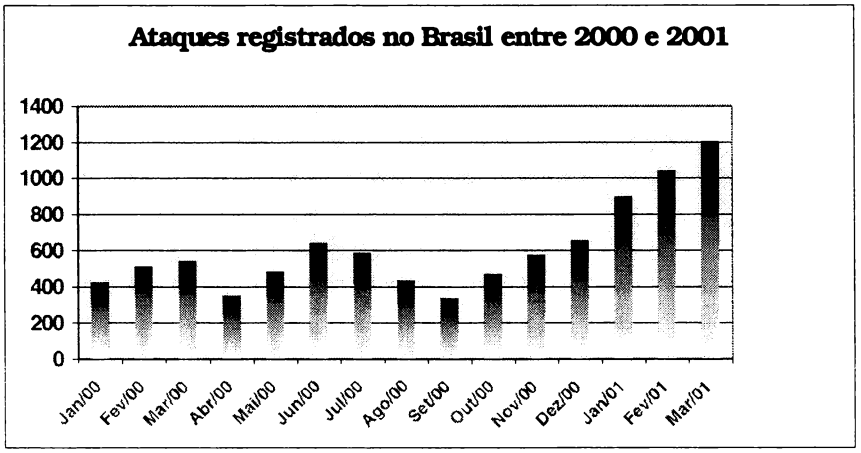
O brocardo latino *"nulla poena nullo crimen sine legge"* exprime essa situação, pois não pode haver conduta punível se não existe lei que proiba, e portanto, a reserva legal é premissa inafastável para a capitulação dos atos lesivos ou prejudiciais aos cidadãos. Um agente só pratica um crime se estiver escrito na lei que a sua conduta é criminosa, pois caso contrário trata-se de uma conduta atípica.

O Direito Penal, tutelador dos bens jurídicos mais relevantes, quais sejam, vida e a liberdade, deve ser regido pelas normas penais vigentes. A sociedade não pode submeter-se a falta de interpretação destas ou ficar a mercê do Direito costumeiro e da analogia para definir a sua aplicação.

Infelizmente o Brasil tornou-se especialista nas sabotagens de sites na Internet, por causa desses piratas da "net" chegou a ser proibido acessar o site da NASA a partir do Brasil. Apenas o grupo que se apresenta como "*Prime Suspectz*" era há dois anos, o segundo colocado no "*rancking*" de crimes virtuais.

---

[9] PINHEIRO, Reginaldo Cesar. **Os Crimes Virtuais na Esfera Jurídica Brasileira.** Boletim IBCCRIM. São Paulo-SP. abril/2001. Nº. 101, ano 8.



Fonte: NIC Br.Security Office (NBSO)/RNT

Vale destacar que grande parte dos ataques não é divulgada porque as empresas não querem perder a confiabilidade dos clientes[10].

Especialistas são unânimes ao afirmar que a incidência de crimes virtuais aumentará consideravelmente pela carência de profissionais de segurança no mercado. Outro fator é a proliferação de máquinas "zumbis", configuradas para ataques[11].

Há alguns anos atrás apenas uma pequena quantidade de pessoas tinha acesso à Internet, eram na quase totalidade estudantes e profissionais da área de Informática. Hoje está muito mais popularizado o seu uso e qualquer pessoa pode adquirir alguns conhecimentos de informática e cometer um delito, note-se que não é necessário conhecimento aprofundado para disseminar um vírus, por exemplo.

Quanto à investigação da criminalidade informática há carência de policiais preparados tecnicamente e os recursos materiais para tal são escassos ou inexistem.

---

[10] Fonte: RNT-Revista Nacional de Telecomunicações. Nº. 261 Maio/2001. p. 45.
[11] Fonte: Notícia, ZDNet. Em 18/12/2000.

Dentre as inúmeras condutas delituosas, a literatura especializada tem ressaltado as seguintes infrações por intermédio do computador[12]:

a)Acesso indevido aos sistemas de computador: penetrar indiscriminadamente, sem autorização ou permissão aos sistemas ou serviços de computador.

b)Acesso indevido com o intuito de cometer crime mais grave: penetrar indiscriminadamente, sem autorização ou permissão aos sistemas ou serviços de computador desejando cometer crime mais grave, como vantagem econômica ou dano, por exemplo.

c)Causar dano, obter vantagem, alterar programas, devassar o sigilo das informações contidas no sistema: Crime mais grave pode incluir fraude eleitoral, crime de calúnia, injúria e difamação, entre outros;

d)Violação de sistema de processamento de dados através de senha de outrem: penetrar em sistema informático através de senha obtida ilicitamente de outra pessoa, ou sem sua autorização.

e)Fraude através do uso de computador: Fraudar é agir com má fé, enganar, lograr. As fraudes de maior freqüência na Internet são leilões, compra e venda de mercadorias, uso de senhas alheias na conexão com provedores de acesso, pirâmides, trabalhos em casa com promessa de altos ganhos e utilização de senhas falsas na utilização de serviços "on-line" pagos.

f)Furto de informações contidas no computador: Obter informações sigilosas ilicitamente invadindo ou não sistemas informáticos.

---

[12] Antônio José M. Feu Rosa. **Dos Crimes Virtuais**. Revista Consulex Maio/2001. No.105, ano V, p. 46.

g)Falsificação de documentos: utilizar da tecnologia do computador para falsificar documentos. Os "softwares" e periféricos do computador têm resultados cada vez melhores que às vezes a cópia se torna idêntica a original.

h)Sabotagem informática: impedir ou prevenir o funcionamento de um computador, temporária ou permanentemente, interferindo no sistema de forma a causar distúrbios no mesmo, tanto por uma operação de programa como uma avaria elétrica;

i)Danos ao computador e às informações contidas nele: Danificar "software" ou "hardware" do computador e seus periféricos, ou as informações contidas neles.

j)Aquisição ilícita de segredos industriais e comerciais: Obter para si ou para outrem segredos industriais e comerciais para auferir vantagem econômica.

k)Uso não autorizado de computador: furto de tempo de sistema: Utilizar o computador alheio desautorizadamente.

l)Cópia/uso ilícito de programas de computador: é a pirataria de programas de computador, a cópia indiscriminada de programas com licença para apenas um computador.

m)Cópia/uso ilícito de um "chip": Copiar a estrutura interna de um "*chip*" significa burlar a lei de patentes.

n)Violação de direito autoral: Pode-se dizer que se trata de uma modalidade específica entre os crimes de pirataria. Enquadram-se nesses crimes a difusão de obras literárias, jornalísticas, musicais, entre outras

o)Criação, inserção e distribuição de "vírus": Criação, inserção e distribuição de pequenos programas hostis que têm a finalidade de danificar outros programas dentro do computador e seus periféricos.

p)Espionagem: Pode ser a espionagem para roubar segredo industrial ou para roubar segredo militar.

q)Racismo: O racismo é a divulgação da aversão a determinados grupos de pessoas, muitas vezes incitando à violência, seja pela etnia, pela religião, pela nacionalidade, através de "homepages", correio eletrônico, "chat" ou outro meio digital.

r)Interceptação indevida de telecomunicações: Interceptar significa Interromper no seu curso; deter ou impedir na passagem, cortar, interromper, porém entende-se que apenas acessar ilicitamente comunicação privada sem autorização, durante a transmissão ou não, mudando ou não seu conteúdo, já constitui crime.

s)Violação de dados pessoais: Acessar indiscriminadamente dados pessoais sem autorização.

t)Tráfico de drogas: Utilizar os sistemas de informação para venda e compra de drogas.

u)Pedofilia/pornografia infantil: O uso da rede de computadores para colocar à disposição dos usuários cenas de sexo explícito envolvendo menores.

v)Crimes contra a honra: Consistem nos atos que denigrem a integridade moral das pessoas através da injúria, da calúnia ou da difamação, utilizando a Internet como maneira de difusão de ofensas, seja por imagens, seja por palavras.

Há crimes em que há impossibilidade prática de serem cometidos pela internet, o homicídio por exemplo. Porém é possível vislumbrar que daqui a alguns anos esses crimes serão executáveis via rede. Considerando que a rede vai se tornar cada vez mais rápida, muito mais atividades poderão ser realizadas. Na medicina, por exemplo, a interceptação de uma informação digital que instruiria

a aplicação de determinado medicamento que em doses errôneas levaria o paciente a óbito.

Já há a possibilidade, também, de serem executadas cirurgias a distância. Com a utilização da *realidade virtual*, um cirurgião no Brasil pode operar uma pessoa nos EUA.

3. PERSPECTIVAS PROCESSUAIS

3.1 INVESTIGAÇÃO

A investigação é atividade estatal da *"persecutio criminis"*, destinada a preparar a ação penal, isto é, fornece subsídios para que o titular da ação penal, possa ingressar em juízo. A investigação preparatória como primeiro momento da persecução penal é também momento pré-processual.

Como ensina Carla Rodrigues Araújo de CASTRO dois são os objetivos da investigação: verificar a materialidade e identificar a autoria. Esclarecer se o crime aconteceu de fato, se afirmativo, quais foram as circunstâncias e esclarecer quem foi o autor ou autores, isto é, aqueles agentes que cometeram o crime[13].

Nos crimes de informática a investigação deve respeitar os princípios gerais que norteiam esta atividade da polícia judiciária, consideradas as peculiaridades que lhe são características.

Os princípios aplicáveis na investigação preparatória são[14]:

a) Princípio da inocência[15]: Cita a Declaração dos Direitos do Homem e do Cidadão *"Toda pessoa acusada de um ato delituoso tem o direito de ser presumida inocente, até que sua culpa tenha sido provada de acordo com a lei, em julgamento público no qual tenham sido asseguradas todas as garantias necessárias à sua defesa"*;

b) Princípio do menor sacrifício: Os feitos apuratórios devem se desenvolver com o menor desgaste possível para aquele que é alvo de investigação;

---

[13] CASTRO, Carla Rodrigues Araújo de. **Crimes de Informática – e Seus Aspectos Processuais**. 1º ed. Rio de Janeiro: Lumen Júris, 2001, p.95.

[14] TASSE, Adel El. **Investigação Preparatória**. 2ª edição. Curitiba: Juruá, 2001.

[15] Brasil, Constituição. **Constituição da República Federativa do Brasil**. Brasília-DF: Gráfica do Senado Federal, 1988, art. 5º, LVII.

c) Princípio da integridade física e moral: É vedada a utilização de qualquer tortura, seja física ou psicológica, coagindo o indivíduo a manifestar-se ou comportar-se de modo diverso a sua convicção;

d) Princípio da idoneidade dos meios[16]: Quanto às provas, os recursos de obtenção devem ser lícitos, quer quanto ao seu conteúdo quer quanto à forma de obtenção.

A investigação deve ser desenvolvida de forma idônea, de modo a não ocorrer nenhum abuso das autoridades e dessa maneira não gerar descrédito da sociedade, o que resulta sempre num prejuízo para todo o sistema.

A justa causa é condição autêntica da ação penal, é fundamental que haja um mínimo de convicção sobre a materialidade e autoria. Para mover o aparato punitivo há que se ter consciência da responsabilidade de ocasionar marcas prejudiciais seríssimas no indivíduo alvo da investigação, inclusive das pessoas que o cercam, portanto não pode jamais ser um ato de prepotência.

Como referência para as diligências a serem providenciadas o art. 6° do CPP enumera-as de maneira não taxativa, deixando campo para ponderação do delegado de polícia desenvolver as diligências que forem necessárias para cada caso.

As dificuldades são outras nos crimes através da rede mundial, já que a técnica intelectual fala muito mais alto e o anonimato permitido pela Internet atrapalha na identificação da autoria.

Nos crime praticados através da rede mundial de computadores podem ocorrer várias situações. Nos crimes via "E-

---

[16] Brasil, Constituição. **Constituição da República Federativa do Brasil**. Brasília-DF: Gráfica do Senado Federal, 1988, art. 5°, III.

mail" o investigador deverá intimar o provedor de acesso à rede do usuário para determinar quem foi o autor da mensagem enviada.

Nas infrações exercidas através de "sites", o investigador deverá determinar quem é o responsável pela página na Internet. Para tanto é necessário acessar www.registro.br e mediante o endereço eletrônico do site se pode descobrir quem registrou, seu CPF ou CGC e seu endereço[17].

O investigador poderá chegar no autor da infração em outras hipóteses com auxílio técnico e de posse de algumas informações como a data e o horário exato da lesão, qual equipamento foi utilizado etc.

Há alguns anos atrás, no Centro de Treinamento das Polícias Federais nos Estados Unidos - FLETC - na Geórgia, o Agente Federal Manson, provocou risos ao dizer que logo os policiais seriam chamados de "Cybercops" e ao invés de arma usariam um "notebook" para combater os crimes de informática.

Os "Cybercops" não são mais objeto de ficção científica, há alguns anos o FBI já treina policiais aptos para combater crimes de alta tecnologia transnacionais: eis o desafio da polícia global do século XXI.

No Brasil, infelizmente, existe um grande despreparo por falta de treinamento, pessoal tecnicamente experiente e uma estrutura adequada. Para se realizar um trabalho eficiente nessa espécie de investigação o primordial é antecipar.

O delegado titular da Delegacia de Repressão ao Crime Informático e às Fraudes Eletrônicas do Estado de Minas Gerais (Dercife/MG), Willian Leroy, revela que muitas vezes não sabia como começar uma investigação. "Todos os dias são investidos milhões em

---

[17] CASTRO, Carla Rodrigues Araújo de. **Crimes de Informática – e Seus Aspectos Processuais**. 1º ed. Rio de Janeiro: Lumen Júris, 2001, p.96.

novos programas de computadores. O que hoje é novidade, amanhã pode ser ultrapassado. Ninguém pode dizer que conhece profundamente o mundo virtual", comenta Leroy[18].

A Internet não é virtual, é extremamente real e os crimes praticados são rápidos e dinâmicos, tornando-se mais sofisticados com o emprego de comunicações móveis e telefonia anônima pré-paga, exigindo da polícia uma resposta célere e eficiente.

A maioria das empresas já sentiu a ameaça de perderem milhões com a criminalidade na rede e já estão investindo cada vez mais em recursos privados de segurança.

Os governos estadual e federal montam centros de investigação e preparam policiais para combater crimes por meio da rede. Existem cinco desses centros: três da polícia civil - em São Paulo, Rio de Janeiro e Minas Gerais - e dois da federal, um em Brasília e o outro no Rio.

Responsável pelo Setor de Crimes pela Internet (Detel) da Polícia Civil de São Paulo, Mauro Marcelo de Lima e Silva, formado pela Academia Nacional do F.B.I. (turma 173), graduado em Justiça Criminal pela UVA - Universidade de Virgínia-EUA, colabora com a "Web-Police", uma instituição que congrega policiais de todo o mundo no combate a crimes do ambiente virtual.

O grupo de trabalho da "Web Police" tem como Diretor Executivo Renée Kloss e Gregory Chernobrov, que contam com mais de três mil funcionários em escritórios localizados em 132 países.

No mês de abril de 2002 tiveram 48.360 (quarenta e oito mil, trezentos e sessenta) casos relatados, 1.612 (um mil, seiscentos e doze) por dia (houve um incremento de 21% no mesmo mês do ano passado).

---

[18] Fonte: **www.cg.org.br/clipping** Em 05/09/2002

Segundo a "Web Police" os três crimes mais freqüentes de 71 categorias de crimes, relatados ao nível internacional, são: [19]

a) Fraude: 31% do total relatados
b) Pedofilia/pornografia infantil: 18% do total relatados
c) Perseguição/perturbação/injúria: 11% do total relatados

A Web Police está constantemente expandindo e adquirindo novos recursos para ajudar na luta contra o crime na Internet.

Segundo a experiência do delegado Mauro Marcelo Lima e Silva, "cerca de 80% dos inquéritos são por crime contra a honra", são números da Detel de São Paulo.

Os crimes contra instituições financeiras são reduzidos, porém como já foi mencionado em outro lugar, muitas empresas não delatam à polícia com receio de perderem a credibilidade, cita o delegado Lima e Silva "a síndrome da má reputação leva as empresas a assumirem prejuízos, encobrindo os delitos".

A Polícia Federal trabalha na apuração de crimes cometidos contra a União e nos casos de pedofilia, a pornografia envolvendo crianças e adolescentes. Chegam em torno de 50 denúncias por mês no Setor de Crimes por Computador da Polícia Federal. "Das denúncias, 10% se transformam em inquéritos", afirma Caricati. Por enquanto existem no Brasil poucos inquéritos envolvendo crimes de informática contra instituições financeiras. "Algumas empresas escondem as fraudes com receio de criar insegurança entre os clientes", diz Caricati.

A polícia também esbarra em outra artimanha utilizada pelos criminosos. "Às vezes, como nos casos de difamação ou racismo, descobrimos o autor mas não podemos prendê-lo ou tirar o site do ar,

---

[19] Fonte: Web Police in: **http://www.Web-Police.org**. Em 15/07/2002

porque foi feito em provedor de um país onde isso não é crime, caso dos Estados Unidos, onde é totalmente livre qualquer tipo de manifestação de opinião", explica o delegado Lima e Silva.

Por falta de legislação específica as eventuais condenações por crimes de informática são feitas com base no Código Penal, que foi reformado em 1984 - antes, portanto, da existência da Internet. Há quem considere necessário que alguns aspectos sejam incluídos numa lei própria: "Os provedores deveriam ser obrigados a guardar informações por um determinado período", diz o perito André Caricati, do Setor de Crimes por Computador da Polícia Federal.

Hoje, o Comitê Gestor da Internet (CGI) no Brasil recomenda aos provedores nacionais que guardem por até três anos as identificações das mensagens - os chamados Protocolo de Internet (IP), a "carteira de identidade do computador" - para que os investigadores possam chegar aos criminosos[20].

Os dois investigadores, porém, concordam que mesmo com as empresas encobrindo as fraudes, o número de crimes envolvendo recursos financeiros ainda pode ser considerado pequeno no Brasil. "Os programas têm falhas, mas é possível ter sistemas de segurança que dificultem o acesso dos "hackers" com eficiência", diz Caricati.

A maioria dos indivíduos que praticam crimes na Internet têm uma sensação de anonimato, ledo engano, o crime no ambiente virtual sempre deixa rastros, o que facilita bastante a vida dos investigadores.

Ninguém entra na Internet sem um provedor de acesso que, preservado, oferece as principais pistas à polícia sobre os piratas virtuais. Sejam eles "hackers" com altos conhecimentos de informática para entrar em sistemas de empresas apenas por

---

[20] Fonte: **www.cg.org.br/clipping** . Em 05/09/2002.

diversão ou criminosos empenhados em roubar ou simplesmente sujar a imagem de alguém.

No cerco aos bandidos cibernéticos, as polícias começam a se especializar. Há seis meses foi inaugurado no Rio de Janeiro o Núcleo de Prevenção e Repressão a Crimes Cometidos via Internet (Nunet), o primeiro da Polícia Federal fora de Brasília. O núcleo, que funciona na Delegacia de Ordem Pública e Oficial (Deops), tem mais de 2.500 (dois mil e quinhentos) casos em seu banco de dados, a maioria com informações de crimes contra crianças e adolescentes. Os números chegaram ao Nunet por meio de denúncias feitas a Associação Brasileira Multiprofissional de Proteção a Infância e ao Adolescente (Abrapia).

Os chamados crimes de informática *impuros* ou *impróprios* são delitos passíveis de tipificação pela atual legislação. Porém é indispensável que haja uma reforma na legislação criminal, nos âmbitos nacional e internacional, além dos órgãos de investigação que precisam ser reestruturados de modo que exista uma cooperação que ultrapasse fronteiras, no sentido de coibir estes crimes transnacionais.

3.2 PROVA

A prova é a demonstração da verdade de um fato. A prova penal é objeto de duas operações: constitui o procedimento investigatório da *"informatio delicti"* num momento pré-procesual e após na ação penal no momento da instrução do processo. A prova obtida no momento pré-processual é a mais efetiva, considerando que a materialidade do crime é recente e que o tempo é inimigo da autoridade investigadora.

Cabe a Criminalística a função de ceder elementos para uma investigação segura na reconstrução do fato delituoso. O levantamento de provas importantes depende diretamente de uma investigação eficiente.

É crucial o aparelhamento técnico e material na atividade investigatória para a colheita de evidências e elucidação do evento delituoso.

No processo penal brasileiro, vigora o princípio da verdade real conforme o art. 155 do Código de Processo Penal. É imprescindível que fique elucidado o "*thema probandum*" para que se ache a exata solução ao pedido que se contém na acusação[21].

Não há, em tese, limitações ao meio de prova, é livre a produção de qualquer prova podendo indicar as enumeradas pelo CPP ou quaisquer outras, como exibição de fitas de vídeo, fotografias, inclusive os "E-mails". Contudo, o princípio da liberdade probatória não é absoluto. Exclui-se a possibilidade de apreciação das provas ilegítimas ou ilícitas, tanto no seu conteúdo como na forma de obtenção, conforme o art. 5º da Constituição, "*in verbis*":

> *"LVI – são inadmissíveis, no processo, as provas obtidas por meios ilícitos;"*

Nesse campo a interceptação de correspondência eletrônica é altamente polêmica principalmente quando esta poderia servir como prova e meio de instrumento de investigação de outros crimes.

O artigo 5º, XII, da Constituição Federal, foi regulamentado há algum tempo, através da Lei 9.296, de 24 de julho de 1996 que, em seu artigo 1º, preconiza, "*verbis*" :

> *"Art. 1º. A interceptação de qualquer comunicação telefônica, de qualquer natureza, para prova em investigação criminal e em instrução*

---

[21] MARQUES, José Frederico. **Elementos de Direito Processual Penal**. 1ª ed. Campinas: Bookseller, 1997. Vol. II, p. 259.

processual penal, observará o disposto nesta Lei e dependerá de ordem do juiz competente da ação principal, sob segredo de justiça.
Parágrafo Único - O disposto nesta Lei aplica-se à interceptação do fluxo de comunicações em sistema de informática e telemática."

Há quem sustente a inconstitucionalidade desse dispositivo, contrastando-o com o artigo 5º da atual Carta, "*in verbis*":

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

A afirmativa parte da premissa de que a inconstitucionalidade residiria no fato de que a Constituição só cuida da interceptação das **comunicações telefônicas**, e **não** do **fluxo das comunicações com o emprego da telemática** que, notadamente na atualidade, onde há possibilidade de transmissão de dados independente da utilização de linha telefônica.

Cumpre ver entretanto que, em outro ponto, o inciso X do mesmo artigo 5º preconiza, "*verbis*":

"X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação;"

José Henrique Barbosa Moreira LIMA NETO, advogado de São Paulo, argumenta ser em parte inconstitucional a Lei 9.296/96, por entender que somente pode haver quebra de sigilo telefônico, jamais das comunicações em sistemas de informática ou telemática, conforme pretende a Lei supra referida.

Tecnicamente é possível acessar arquivos existentes em computadores, desde que sejam interligados em redes, ou acompanhar as comunicações havidas por este meio, acontecidos através da internet ou "intranet". Porém a interceptação desses

dados, para a posterior utilização como prova judicial, deve obedecer aos preceitos legais da imprescindibilidade da urgência da medida.

É interessante o exemplo de Luís Carlos Cancellier de OLIVO, na hipótese de um usuário que envia um "e-mail" ameaçador e logo depois deleta de seu micro tem a falsa sensação de que está eliminando qualquer prova da autoria do crime.

A mensagem fica armazenada em muitos locais, no próprio computador do autor, na lixeira, na pasta de arquivos temporários, no provedor do autor, no provedor da vítima, nos computadores de "*back up*" dos dois provedores, no computador da vítima, enfim são muitos os rastros[22]. Como já foi mencionado, o Comitê Gestor da Internet (CGI) recomenda aos provedores a guarda por até três anos as identificações das mensagens[23].

Através do endereço IP ("*internet protocol*") se consegue determinar a autoria de um crime pela rede mundial, funciona como a *identidade* do computador. Todo endereço eletrônico está vinculado a um número que é seu endereço IP, trata-se de quatro seqüências de números separadas por pontos, por exemplo, 123.45.6.78.

Este número individualiza cada máquina na internet. Na verdade por trás de cada site na internet existe um computador ligado 24 horas gerando a página que lá encontramos, que pode ser criada por uma empresa, uma instituição, um órgão do governo ou um indivíduo qualquer.

Quando alguém digita um endereço eletrônico, por exemplo, www.senado.gov.br o programa navegador irá buscar na rede uma

---

[22] OLIVO, Luís Carlos Cancellier de. **Direito e Internet: a Regulamentação do Ciberespaço**. Florianópolis: Ed. Da UFSC, CIASC, 1998. p.62.

[23] Fonte: **www.cg.org.br/clipping**. Em 05/09/2002.

lista com os nomes de domínios brasileiros (sufixo br), em seguida selecionará aqueles do ramo governamental (sufixo gov) para então traduzir o nome de domínio para seu endereço IP que poderia ser algo como 123.45.6.78. Finalmente com o endereço IP na memória, o computador da pessoa irá conectar-se ao computador do senado[24].

O estudo do endereço IP é fundamental para a resolução de provas para crimes praticados pela internet.

No campo técnico, produzir provas é um grande desafio. Imagine-se um álibi ou prova de crime que dependa da máquina. Podemos programar um computador para cumprir uma determinada tarefa em um determinado dia, sem que seja necessária a presença da pessoa.

Os rastros eventualmente deixados só informam as máquinas que estavam ligadas uma as outras, e esse contato pode ter sido feito automaticamente, de outra cidade, estado ou país. Uma pessoa pode usar o computador de outra, ou uma máquina pública. As evidências digitais podem, ainda, serem modificadas. Como poderemos ter certeza de que as informações obtidas não foram falsificadas? O "e-mail" ,por exemplo, não é uma mensagem assinada, apesar de existirem projetos para criação de assinatura eletrônica ou criptografia, este avanço ainda não está difundido.

Caberá a parte interessada demonstrar a autenticidade. Mediante todos esses obstáculos, o "e-mail" pode ser considerado prova como qualquer outra, dependendo apenas do convencimento do juiz (art.157 do CPP).

---

[24] VIANNA, Túlio Lima. **Dos Crimes por Computador**. Monografia realizada para graduação na UFMG. Belo Horizonte, 1999.

O procedimento investigatório não se apresenta trajado de provas irrefutáveis e contundentes do crime cometido. Isto acaba por ser um sintoma decorrente da falta de preparo dos agentes de investigação e da estrutura disponível.

Em solidariedade às dificuldades anteriores, os documentos eletrônicos (arquivos de computador) são provas facilmente modificáveis, permitindo adulterações comprometedoras a seu conteúdo probatório. Portanto, há grandes dificuldades na comprovação da veracidade desses documentos, que geralmente são as únicas provas do crime.

Vale ressaltar que não é complicado identificar a máquina utilizada para o crime, mas sim a identificação da pessoa que a manuseou em determinado momento. Cada vez é mais fácil localizar a máquina emitente das informações, o problema é saber quem estava no seu comando.

A prova pericial é necessária quando a infração deixa vestígios, será indispensável o exame de corpo de delito (art. 158 CPP). Portanto, nos crimes de informática é mister que se apreenda o computador para realização da perícia conforme art. 240 do CPP.

A busca será determinada de ofício pela autoridade ou mediante requerimento das partes (art. 242 CPP). O mandado de busca deverá atender às exigências do art. 243 do CPP. Realizada a busca, o material deverá passar pelo crivo de dois peritos (art. 159 CPP).

Segundo sugere Carla Rodrigues Araújo de CASTRO, podemos ter os seguintes quesitos nestas três categorias de crimes[25]:

---

[25] CASTRO, Carla Rodrigues Araújo de. **Crimes de informática – e Seus Aspectos Processuais**. 1º ed. Rio de Janeiro: Lumen Júris, 2001. p104.

"Quesitos para o crime de pedofilia

a) Qual a natureza e quais as características do material encaminhado ao exame?

*b) No computador apreendido há arquivos contendo imagens (extensões: *.jpg; *.bmp; *.pcx; *.gif; *.cif etc.)?*

c) Em caso positivo, dentre tais arquivos, existe alguma imagem que contenha crianças, adolescentes ou jovens retratados em poses pornográficas, inclusive nuas ou seminuas?

d) Quais Programas de correio foram utilizados pelo usuário do computador periciado?

e) Neste programa de correio eletrônico constam "logs" na caixa de saída, na lixeira, ou em qualquer outro local possível (arquivos temporários na Internet), contendo alguma imagem de cunho pornográfico relacionado a criança ou adolescente, anexado às mensagens enviadas?

f) Em caso positivo, esclarecer quais seriam as imagens, indicar dia e hora em que foram enviados, imprimindo as mesmas.

g) O usuário do computador periciado utiliza algum programa de "news"?

h) Em caso positivo, há mensagens contendo arquivos de imagens?

i) Neste programa de "news" consta, nos "logs", na caixa de saída, na lixeira ou em qualquer outro local (arquivos temporários na Internet), alguma imagem de cunho pornográfico relacionado a crianças ou adolescentes anexadas às mensagens postadas?

j) Em caso positivo, que o Sr. perito imprima tais imagens e forneça dia e hora que as mesmas foram postadas, anexando ao laudo.

k) O usuário de computador periciado utiliza algum programa IRC (Internet Relay Chat), como mIRC e todas as suas variantes?

l) Em caso positivo, houve alguma conversa que o usuário enviou mensagem com imagem de cunho pornográfico relacionado a crianças ou adolescentes nos logs do IRC?

m) Em caso positivo, esclareça o Sr. perito o dia e hora e imprima as imagens, anexando ao laudo.

n) Outras considerações a critério dos senhores peritos."

"Quesitos para crime de pirataria:

a) Qual a descrição e quais as características do material encaminhado a exame?

b) Na máquina apreendida estão instalados sistema operacional ou qualquer outros aplicativos com os códigos que os identifiquem e data da instalação?

c) Em sendo negativa a resposta do quesito acima, se os senhores peritos podem afirmar terem sido instalados sistema operacional ou quaisquer outros aplicativos na máquina apresentada, fornecendo os códigos que os identifiquem e data da respectiva instalação.

d) Se ainda for negativa a resposta aos quesitos anteriores, podem os Srs., peritos afirmar, com base em fragmentos encontrados, terem sido instalados quaisquer programas na máquina apresentada, nomes dos mesmos, códigos que os identifiquem e datas da instalação?

e) Outras considerações pertinentes e esclarecedoras a critério dos Srs. Peritos."

"Quesitos para o crime de ameaça e crimes contra a honra:

a) Qual a descrição e características do material encaminhado a exame?

*b) No computador apreendido há arquivos contendo textos (extensões: *.doc; *.txt)?*

c) Em caso positivo, existe algum contendo texto ou mensagem ameaçador (ou injurioso)?

d) Quais programas de correio eletrônico foram utilizados pelo usuário do computador periciado?

e) Neste programa de correio eletrônico constam "logs" na caixa de saída, na lixeira ou em qualquer outro local possível (arquivos temporários na internet), contendo algum texto de cunho ameaçador (ou injurioso)?

f) Em caso positivo, esclarecer quais seriam os textos, indicar dia e hora em que foram enviados, imprimindo os mesmos.

g) Outras considerações pertinentes e esclarecedoras a critério dos Srs. peritos."

De outro lado, o avanço tecnológico oferece novas técnicas na apuração dos fatos delituosos.

Uma possibilidade de utilização das técnicas de realidade virtual é, por exemplo em tribunais, na reconstrução dos fatos a partir de provas. Contudo, esta aplicação é bastante controversa pois é discutível se poderá haver manipulação de imagens por forma a adulterar a realidade, (pode-se por meio de computador, reproduzir, p. ex., a trajetória de um projétil num homicídio).

Outra novidade seria o interrogatório "on line", que parece antipático a alguns, mas que traz celeridade ao processo. Experiência levada a efeito em São Paulo, por iniciativa do magistrado Luíz Flavio Gomes, o novo interrogatório, que seria realizado por computador, estando de um lado, no Fórum, o magistrado e de outro lado da linha, no presídio, o acusado, sem contudo um contato entre ambos, para o idealizador, é maneira de agilizar, desburocratizar, trazendo economia para a Justiça. Muitas vezes, devido a alta periculosidade do criminoso e sua hierarquia no mundo do crime, há que se mobilizar dezenas de policiais para garantir que tudo ocorra bem.

Vozes de todos os cantos do país levantam-se contra essa experiência, argumentando pois sob o manto da modernidade e da economia, revela-se perversa e desumana, afastando o acusado da única oportunidade que tem ele de falar ao seu julgador, trazendo frieza e impessoalidade ao ato.

Na verdade não podemos evitar a adequação aos novos tempos, precisamos sim, favorecer-nos dessas facilidades que a Ciência nos fornece, sob pena de o aparato estatal não conseguir acompanhar a evolução da sociedade.

3.3 PERFIL DOS DELINQÜENTES

Segundo o conceito formal, crime é a violação culpável da lei penal do Estado, criada para garantir a segurança dos cidadãos. É, segundo o conceito substancial, a ofensa de um bem jurídico tutelado pela lei penal. É, também, segundo o conceito analítico, fato típico, antijurídico e culpável.

Lógico que esta violação há de ser cometida por alguém. Este "alguém" é o criminoso. O agente da ação anti-social que comete o crime. Não há como se falar em criminoso, sem falar em Cesare Lombroso (Verona,1835 - Turim, 1909) e das suas teorias no campo da caracterologia. Lombroso relacionou certas características físicas à psicopatologia criminal, ou à tendência inata de indivíduos sociopatas e com comportamento criminal.

Esta abordagem de Lombroso descende da frenologia, criada pelo físico alemão *Franz Joseph Gall* e relacionada com a caracterologia e fisionomia (estudo das propriedades mentais a partir da fisionomia do indivíduo). A teoria de Lombroso foi desacreditada cientificamente, mas chamou a atenção para a importância de estudos científicos da mente criminosa, estudo este que passou a ser chamado de antropologia criminal.

É verdade, os estudos realizados por Lombroso estão há muito superados pelo espírito crítico da moderna criminologia, porém deve-se confessar que a partir de sua teoria muito se aproveitou no desenvolvimento de novas teorias que evoluíram a criminologia em um caminho mais sociológico.

A Criminologia é o estudo dos elementos naturalísticos (psico-físicos) do crime. É estudo causal-explicativo do crime[26].

O estudo do perfil do criminoso é matéria da Criminologia. É indispensável distinguir o perfil dos criminosos que atuam na internet, como agem, que ferramentas são essenciais no cometimento do crime, importante para a sua caracterização e finalmente a elucidação da autoria do fato delituoso.

Contudo, infelizmente, a disciplina de Criminologia está desaparecendo das faculdades, como se não merecesse uma reflexão mais acurada nesse campo pelo operador do Direito.

Nos crimes de informática temos as distinções do perfil dos criminosos que atuam na rede mundial de computadores por categorias, em que pode ser útil seu reconhecimento inicialmente pela faixa etária.

Como ensina o prof. Antonio Aurélio Abi Ramia Duarte[27]:

> *"encontramos a primeira categoria de pessoas (dos 13 aos 17 anos de idade – portanto, inimputáveis), nesta classe se encontram adolescentes "hackers" que praticam desde ilícitos de pouca expressão (como por exemplo: montam páginas na Internet, pegam na própria rede fotos de pornografia infantil, etc.), até ilícitos de maiores conseqüências (como: receitas de bombas, crimes raciais, etc.)."*
> *"Na Segunda categoria de delinqüentes, encontramos pessoas com um conhecimento mais profundo em computação (dos 17 anos aos 25 anos de idade), que geralmente tentam obter pequenas vantagens com arrimo nos ilícitos cometidos (como por exemplo: compra de CDs com números de cartões de créditos falsos)."*
> *"Já a terceira categoria destas pessoas, usam a rede para nocivamente difundir ideais fascistas, nazistas, praticam crimes financeiros – esta é a categoria mais hostil."*

Há maior expressão na primeira categoria, principalmente, pelo motivo de que a Internet passa uma falsa impressão de

---

[26] Soibelman, Leib. **Enciclopédia do Advogado**. 5ª edição. Rio de Janeiro: Thex Ed.: Biblioteca Universidade Estácio de Sá, 1994, p.103.

[27] DUARTE, Antônio Aurélio Abi Ramia. **Crime na Internet: a Falsa Noção de Impunidade** – Artigo em http//www.jus.com.br, acessado em 21/09/2001.

anonimato, ledo engano, há mais pistas na internet para se alcançar o criminoso do que os leigos imaginam.

A ampliação do comércio eletrônico preocupa o delegado Mauro Marcelo de Lima e Silva, segundo o qual o número de golpes virtuais deve aumentar muito. Ele explica que a gravidade das ações ilegais na Internet aumenta com a idade dos envolvidos: adolescentes, entre 12 e 17 anos, em geral são movidos pela curiosidade e pelo desafio e podem causar algum prejuízo, da mesma forma que quebrar vidraças ou pichar muros. Já entre os 17 e 22 anos, eles costumam praticar pequenas contravenções, "como pedir pizza pela Internet". Mas os que persistem, acima dessa faixa, usam os conhecimentos que adquiriram para a prática de crimes mais sérios, esses são os que oferecem maior periculosidade.

O agente criminoso da informática revela-se muitas vezes diferente dos demais pela utilização plena do intelecto e dos conhecimentos técnicos. Nessa seleção estão os criminosos que usam do conhecimento de programação avançada para realização do evento delituoso Não há emprego de armas tradicionais e quase sempre inexiste contato com a vítima, pois todos os procedimentos acontecem à distância. Existe nesse meio uma nomenclatura específica para distingui-los e que vale citar:

a) ***"hackers"***- dominam o conhecimento da informática e apenas buscam ampliar sua sabedoria a respeito, praticam geralmente invasões a "sites" de expressão para demonstrar o nível do conhecimento de que são detentores e assim tornarem-se famosos e possivelmente conquistarem um bom emprego, seu objetivo verdadeiro é o sucesso profissional.

O grupo chamado "*Prime Suspectz*" é um exemplo desta espécie de criminosos. Através do vasto conhecimento de informática

eles invadem sites especializados como o **Attrition.org** e **Alldas.com**[28] e deixam uma mensagem na tela com o nome do grupo assumindo a invasão. Apesar de o grupo "Prime Suspecz" ter assumido a invasão do Tribunal de Contas do Paraná, não foi divulgado oficialmente pelo órgão a invasão do dia 28 de outubro de 2000[29];

b) ***"crackers"*** – são especializados em quebrar senhas, tencionam obter vantagem financeira com o conhecimento das falhas nos sistemas. Têm um perfil hostil e se favorecem dos conhecimentos técnicos para subtraírem o que puderem;

c) ***"lammers"*** – fazem o uso anti-social da rede, apenas para perturbar, não possuem conhecimento desenvolvido em informática;

d) ***"phreakers"***- utilizam-se de meios de comunicação através de fraudes, sem pagar pelos serviços. Possuem altos conhecimentos de telefonia para ampliar mais ainda suas formas de invasão. Suas técnicas são uma constante preocupação para as companhias telefônicas[30].

A utilização de computadores é essencial para o cometimento dos crimes de informática. Para manusea-los é necessário possuir um mínimo de conhecimento de microinformática. Há certos crimes que exigem um conhecimento elevado sobre as linguagens de computadores que só poderiam ser cometidas por um profissional desenvolvedor na área de software, ou um estudante de engenharia

---

[28] *Attrition.org* e *Alldas.com* são páginas da Internet.

[29] Fonte: **http://www.infoguerra.com.br/infonews/talk/973573200,64125,.shtml** em 20/08/2002

[30] M@RCIO. **A Internet e os Hackers: Ataques e Defesas**. São Paulo-SP: Chantal editora, pg32.

da computação. Esses crimes são, por exemplo, a criação de um vírus, o roubo de senhas de cartão de crédito, para posterior utilização, invasões de sites e etc. De outro lado, há crimes que podem ser praticados por qualquer pessoa mal intencionada que possua um computador e um conhecimento básico de informática. A disseminação de vírus, a pedofilia, a ameaça e a injúria via "E-mail", são exemplos.

Portanto, nem todos os autores de crimes de informática são perpetrados por gênios do "software" e do "hardware". Com a evolução tecnológica os programas de computador ficaram mais descomplicados, mais intuitivos. Quanto ao valor para se obter um equipamento está mais acessível. Com a difusão do uso do computador, que é fundamental para o desenvolvimento, mais pessoas com conhecimentos rudimentares de computação vão ser potencialmente capazes de cometer delitos via computador.

Na década de 70, nos EUA, muitos delinqüentes de informática, após serem condenados a penas leves, eram contratados como especialistas em segurança e consultores de informática.

Hoje, através das inumeráveis compilações que circulam pelo mundo da informática, são os crimes dessa espécie cometidos à égide da *"special opportunuty crimes"*, qual sejam, os crimes afeitos à oportunidade, perpetrados por agentes que têm a sua ocupação profissional ao manuseio de computadores e sistemas, em várias atividades humanas, e em razão dessa ocupação cometem delitos, invariavelmente, contra seus empregadores.

Essas compilações ainda trazem o perfil do delinqüente de informática, que são pessoas inteligentes, gentis, educados, principalmente, nos EUA e na Alemanha, com idade entre 24 e 33 anos.

São todos, em regra, do sexo masculino, operadores competentes de computadores e sistemas, educados, brancos, dedicados, com "QI" acima da média. Devido a essa inteligência, geralmente privilegiada, são aventureiros, audaciosos e mantém com o computador e os sistemas um desafio constante de superação e de conhecimento. Para muitos é sua principal razão para trabalharem.

Têm, nesse desafio, sempre, a disputa, tanto com a máquina e seus elementos, como com os amigos que faz nesse meio, basta ver que os *crimes de informática* são perpetrados em co-autoria.

Entendem, exclusivamente ao seu juízo, não estarem cometendo qualquer delito, pois o espírito de aventura, audácia e de disputa bloqueiam seus parâmetros para avaliarem o legal do ilegal.

Suas condutas delituosas passam por estágios de objetivos. No início trata-se apenas de vencer a máquina. Após percebem que podem ganhar dinheiro extra. E , por fim, em razão desse dinheiro extra, passam a fazê-lo para sustentarem os seus altos gastos que são, em regra, com aparência pessoal e equipamentos de ponta na área de informática.

A esse perfil agrega-se o de serem pessoas avessas à violência e jamais se incomodam de prorrogarem seus horários, inclusive, até gratuitamente.

Esse, em suma é o delinqüente de informática, que em qualquer parte do mundo mantém esse perfil, que dificulta ao máximo que seja surpreendido em ação delituosa, ou que se suspeite dele.

3.4 JURISDIÇÃO

Como ensina Júlio Fabbrini MIRABETE "a jurisdição é o poder das autoridades judiciárias regularmente investidas no cargo de dizer

o direito no caso concreto, ou seja, de pronunciar concretamente a aplicação do direito objetivo"[31].

A soberania dos Estados impõe a aplicação de sua lei penal no seu respectivo território[32].

A idéia de que impera a anarquia na internet é falsa, não é uma zona sem lei, como muitos pensam, e o desconhecimento das normas não absolverá ninguém.

No que concerne à aplicação da lei no espaço, temos os seguintes princípios:

a) Princípio da territorialidade: aplicar-se-á a lei do Estado em razão de fatos ocorridos nos limites de seu território nacional;

b) Princípio da defesa: a lei do Estado aplicar-se-á em razão do bem jurídico tutelado;

c) Princípio da nacionalidade: aplicar-se-á a lei do Estado em razão da nacionalidade do indivíduo, onde quer que este esteja.

d) Princípio da justiça penal universal: aplicar-se-á a lei do Estado em razão de qualquer crime, sem qualquer restrição;

e) Princípio da representação: aplicar-se-á a lei do Estado em razão de serem praticados delitos em aeronaves e embarcações privadas, quando praticado fora dos limites territoriais.

O art. 5º do nosso Código Penal exprime a opção pelo princípio da territorialidade no nosso ordenamento como regra, e como exceções, o princípio da defesa, ou real (art. 7º, I, a, b ,c e §

---

[31] MIRABETE, Julio Fabbrini. **Código de Processo Penal Anotado**.4ºed. São Paulo: Atlas, 1996, p.128.

[32] MICHAELIS: moderno dicionário da língua portuguesa / São Paulo: Companhia Melhoramentos, 1998- **Conceito de território**: Área certa de superfície de terra que contem a nação, dentro de cujas fronteiras o Estado exerce sua soberania, e que compreende o solo, rios, lagos, mares interiores, águas adjacentes, golfos, baías e portos.

3º), da justiça universal (art. 7º,II, a), da nacionalidade (art. 7º II, b) e da representação (art. 7º, II, c)[33].

Adotou também o Código Penal Brasileiro no art. 6º a teoria da ubiqüidade, que nas palavras de Damásio de Jesus adota como local do crime "aquele em que se realizou qualquer dos momentos do "*iter*", seja da prática dos atos executórios, seja da consumação". O crime tem que ter tocado o território brasileiro para que nossa legislação deva ser aplicada.

Lugar do crime

*"**Código Penal - 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."*

Considerada competente a justiça brasileira, cabe aplicar-se a teoria do resultado, a competência será determinada pelo lugar em que se consumar a infração tal como referida no artigos 69 e 70 do Código de Processo Penal. Decidido o "lugar da infração" como aquele onde o crime se consumou, portanto, onde estava o computador utilizado para a conduta delituosa.

Com o avanço tecnológico torna as comunicações mais dinâmicas, com o uso de "notebooks", os crimes podem ser praticados de qualquer lugar que exista uma linha telefônica, podem ainda ser praticados de vários locais, um após o outro. Com a tecnologia da internet móvel, mediante telefonia celular, isso se tornará mais comum.

Para estes casos, em que se torna difícil saber o local exato que ocorreu o crime, subsidiariamente se fixa a competência pela residência do réu (art. 72 do CPP). No caso de o réu possuir mais de uma residência, fixa-se então pela prevenção (art.72 §1º do CPP). Se não tiver residência certa ou for ignorado seu paradeiro, será

---

[33] CASTRO, Carla Rodrigues Araújo de. **Crimes de Informática – e seus Aspectos**

competente o juiz que primeiro tomar conhecimento do fato (art. 72 §2º do CPP).

Nos crimes de menor potencial ofensivo definidos pelo art. 61 da Lei nº 9.099/95, estarão sujeitos ao seu procedimento, prestigia-se a teoria da atividade; importará, portanto, o local onde foi praticada a ação.

Sandra GOUVÊA lembra que em 1996, a Lei nº 9.307 regulamenta a matéria de arbitragem internacional. É instituto limitado, porém, aos direitos patrimoniais disponíveis. Ressalta-se a desvantagem deste instituto pela impossibilidade de obrigar um terceiro, envolvido no conflito, a se subordinar a esta decisão. O instituto poderá, sem dúvida ser utilizado nas relações de natureza civil, mas não poderá ser aplicada em matéria penal[34].

Raciocinando agora numa extensão global, a questão do direito penal no espaço é um sério complicador quando se trata de crimes de informática, mais especificamente aqueles cometidos pela internet, por conta de seu caráter internacional, onde as fronteiras desfazem-se, ou melhor, são pouco notadas. O usuário pode interagir em qualquer lugar do planeta (quem sabe até fora dele[35]) onde houver um outro computador, ou equipamento similar, conectado também na rede mundial.

Processuais. 1º ed. Rio de Janeiro: Lumen Júris, 2001. 196 p.7.

[34] GOUVÊA, Sandra. **O Direito na Era Digital – os Crimes Praticados por Meio da Informática**. RJ: Mauad, 1997, p. 97.

[35] Notícia -fonte: **http://istoedigital.terra.com.br/noticia2.asp?CodigoNoticia=444** em 16/09/2002 "Um dos pioneiros da Internet se aliou ao governo americano para mandar a Internet para Marte - literalmente. Vinton Cerf foi quem em 1969 criou o protocolo de comunicação IP, responsável pelo gerenciamento do tráfego de dados na grande rede. 32 anos depois, ele se tornou o todo-poderoso estrategista-chefe para Internet da MCI Worldcom, segunda maior operadora mundial de telefonia de longa distância e dona da nossa Embratel. O sonho de Cerf é colocar em órbita de Marte uma rede de satélites de comunicação que possa transmitir ininterruptamente dados em alta velocidade para a Terra e vice-versa. Cerf dedica dois dias de trabalho do seu atribulado mês ao planejamento da Internet InterPlaNetária (IPN)."

A nossa capacidade de absorver toda essa inovação tecnológica tão avançada nos leva a ter a Internet, ainda, como tema de ficção científica, porém seus efeitos tem resultado prejuízos milionários às empresas.

A internet não possui um centro ou um núcleo, ela é a rede que está distribuída por todo planeta através dos meios telefônicos de transmissão. Não pertence a nenhum Estado ou empresa. Se ocorre um crime na internet, a questão é: qual o local do crime? De suma importância para definir qual legislação a ser aplicada ao delito. A jurisdição e o ciberespaço são, pois, temas desafiadores da perspicácia dos juristas.

Consideremos então o seguinte exemplo para melhor meditar sobre o assunto: O indivíduo X, residente na Bélgica contrata um provedor mexicano para abrigar sua "homepage" contendo injúrias contra o indivíduo Y, residente na Alemanha, colocando em seu "site", matérias que viriam a macular a honra de Y, quem teria jurisdição para julgar tal situação? O juiz belgo, de onde a conduta foi praticada; o juiz mexicano, de onde o material injurioso estava hospedado; ou o juiz alemão, de onde a injúria foi consumada, ou seja, o indivíduo Y tomou conhecimento.

Se por um lado consideramos a legislação pátria do delinqüente, pode ser que esta não considere a conduta criminosa e o autor do crime não seja punido e continue praticando o ato tido como ilícito em outros Estados.

Se por outro lado, considera-se a legislação pátria da vítima, como decidir considerando que muitas vezes os crimes são plurisubjetivos em relação ao ofendido.

Pode haver mais de uma vítima para apenas um crime cometido através da grande rede, em vários territórios, todos com leis distintas. Na hipótese de um site que abrigue conteúdo racista ou

preconceituoso, por exemplo, não há nem como se medir a extensão do dano moral que possa ter causado com tal conduta.

Poderia supor que fosse considerado como competente o juízo do local em que os arquivos estejam fisicamente armazenados, e portanto de onde eles seriam distribuídos para o mundo todo, isto é, o local do provedor que abriga a "homepage" (México). Neste caso não há conveniência alguma de se julgar o crime neste local.

Acreditamos ser conveniente a adoção da teoria do resultado nos crimes realizados pela internet, que envolvam mais de um país, e que sejam de menor potencial ofensivo, levando-se em conta a maior facilidade na investigação e aplicação da lei segundo os valores da cultura do indivíduo infrator.

A questão da territorialidade da internet precisa ser resolvida, mesmo porque existe uma série de outros delitos, que podem ser cometidos através da rede, e que se não houver uma regulamentação acerca desta matéria pode fazer com que um delito possa ser julgado em toda e qualquer parte do mundo.

Há também aqueles crimes não tipificados em outros Estados, como os crimes contra a honra, p. ex., que podem tocar territórios que repulsam tal conduta.

É um problema intrigante visto que ainda não há tratado internacional que regulamente detalhes sobre essa espécie de criminalidade. O problema da delimitação espacial do âmbito da eficácia da legislação penal há de perpassar, necessariamente, as soluções propostas pelo Direito Internacional Penal. Essas decisões devem ser discutidas e estabelecidas numa comissão, formada por especialistas no assunto, de todos os Estados, cada um cedendo uma parcela igual de sua soberania, sem excessos nas regulamentações, sob pena de não haver adesão.

É relevante também acrescentar sobre a intenção do usuário de estar sob o jugo de normas que não conhece. Não é livremente manifesto o desejo de se relacionar com outras localidades e, consequentemente, de se subordinar às normas que naquelas estejam em vigor.

Quem ingressa no ciberespaço de uma dada nação (seja com intenção de comerciar ou meramente "navegar"), muitas vezes não tem consciência de que pode se sujeitar às normas alienígenas.

3.5 PRISÃO EM FLAGRANTE

Como demonstra o artigo 301 do Código de Processo Penal, a prisão em flagrante é uma medida cautelar de natureza processual que dispensa ordem escrita e é prevista expressamente na Constituição (art. 5º, LXI). O princípio da presunção de inocência consagrado no art. 5º LVII, da Magna Carta, não suprime a prisão em flagrante.

Assevera o eminente jurista Julio Fabbrini MIRABETE que "cabe a prisão em flagrante delito não só em relação à prática do crime, em sentido estrito, como de contravenção , aplicando-se também a esta os preceitos do código de Processo Penal que se referem à prisão em flagrante delito quando da pratica de "infração penal" (art. 302, I, do CPP)[36].

Flagrante, em sentido jurídico, é uma qualidade do delito, que está acontecendo, ou acabou de acontecer. Por haver a evidência visual, a lei autoriza a prisão do autor sem mandado e o agente ativo da prisão pode, excepcionalmente, ser qualquer pessoa do povo,

---

[36] MIRABETE, Julio Fabbrini. **Código de Processo Penal Anotado**.4ºed. São Paulo: Atlas, 1996, p. 350.

inclusive permite a apreensão de coisas, objetos, relacionados com provas do crime.

Nos crimes de informática, flagrante pode se manifestar na circunstância em que o agente está praticando o ato ilícito, p. ex. no momento que o agente está destruindo os arquivos do computador alheio, ou está sabotando um computador para que entre em curto-circuito no momento que for ligado, ou ainda está roubando segredo industrial através de senha obtida ilicitamente de outrem etc.

Existem muitas hipóteses em que pode ocorrer a prisão em flagrante nos crimes de informática, desde que não sejam praticadas pela internet. Geralmente os crimes cometidos pela internet não são possíveis de serem surpreendidos no momento de sua execução, têm a característica de serem cometidos à distância e os resultados às vezes só serão percebidos algum tempo após a conduta delituosa.

Pedofilia, racismo, charlatanismo em "homepage", p. ex., não cessa a permanência enquanto estiverem acessíveis, entende-se o agente em flagrante delito, enquanto não cessar a permanência. O art. 303 do CPP trata de crime permanente, em que a conduta se prolonga no tempo.

Observa Carla Rodrigues Araújo de CASTRO que[37]:

> *"nos crime de competência dos Juizados Especiais Criminais não se imporá a prisão em flagrante, desde que o autor do fato se comprometa a comparecer no juizado (art. 69, parágrafo único, da Lei nº 9.099/95)".*

Há sempre necessidade, nos crimes pela internet, de uma investigação criteriosa para se chegar no autor do crime. Não se pode descartar a possibilidade de haver prisão em flagrante delito, mesmo que pela internet, no futuro, quando a polícia tiver seus

---

[37] CASTRO, Carla Rodrigues Araújo de. **Crimes de Informática – e seus Aspectos Processuais**. 1º ed. Rio de Janeiro: Lumen Júris, 2001, p.109.

grandes centros de investigação eletrônica, e puderem chegar no local da transmissão ou digitação da mensagem, no "calor do crime".

3.6 PENAS ALTERNATIVAS

As penas alternativas são relevantes para o nosso trabalho em face de que a maioria dos crimes de informática, mesmo aqueles praticados através da internet, são crimes de menor potencial ofensivo, como já mencionado em outra seção, os números da Detel de São Paulo revelam que cerca de 80% dos inquéritos dizem respeito a crimes contra a honra.

Penas alternativas são substitutivos penais (cuja pena mínima não exceda a um ano) processo e Rito especialíssimo, para tipos penais a que a lei constitucional denominou de infrações penais de menor potencial ofensivo que permitem às pessoas que cometem pequenos delitos como exemplo: Lesões corporais culposas delito de trânsito (art. 129); Periclitação da vida e da saúde (arts. 130 a 137); Crimes contra a honra (arts. 138 a 145); crimes contra a liberdade pessoal (arts. 146 a 149); Crimes contra inviolabilidade do domicílio (art.150 e seus parágrafos); Crimes contra inviolabilidade de correspondência (arts. 151 a 154); Do dano (art. 163 a 167); Da apropriação indébita (art.168 a 170); Estelionato (art. 171); e contravenções penais. Todos do Código Penal Brasileiro.

Quanto aos requisitos das penas, são os mesmos da suspensão de processo no caso do "SURSIS" e aceitação deve ser feita pelo arguido e pelo defensor. Havendo recusa de um deles segue o procedimento.

As chamadas penas alternativas e dentre elas, as restritivas de direitos foram incluídas no sistema legal brasileiro, quando da

reforma da parte geral do Código Penal, ocorrida em 1984, como a expressa intenção de funcionarem como substitutivos penais para as penas privativas de liberdade. Assim, no art.43, o Código Penal dispõe: As penas restritivas de direitos são:

I - prestação de serviços à comunidade;

II - interdição temporária de direitos;

III - limitação de fim de semana.

No nosso Código Penal, a pena de prestação de serviços à comunidade está prevista no art. 46:

Prestação de serviços à comunidade

> ***"Art. 46*** *- A prestação de serviços à comunidade ou a entidades públicas é aplicável às condenações superiores a seis meses de privação da liberdade.*
>
> ***§ 1º*** *- A prestação de serviços à comunidade ou a entidades públicas consiste na atribuição de tarefas gratuitas ao condenado.*
>
> ***§ 2º*** *- A prestação de serviço à comunidade dar-se-á em entidades assistenciais, hospitais, escolas, orfanatos e outros estabelecimentos congêneres, em programas comunitários ou estatais.*
>
> ***§ 3º*** *- As tarefas a que se refere o §1º serão atribuídas conforme as aptidões do condenado, devendo ser cumpridas à razão de uma hora de tarefa por dia de condenação, fixadas de modo a não prejudicar a jornada normal de trabalho.*
>
> ***§ 4º*** *- Se a pena substituída for superior a um ano, é facultado ao condenado cumprir a pena substitutiva em menor tempo (art. 55), nunca inferior à metade da pena privativa de liberdade fixada."*

Reunidas as condições previstas no art. 44 do Código Penal, pode-se substituir a pena de prisão pelas restritivas de direitos.

> ***"Art. 44****- As penas restritivas de direitos são autônomas e substituem as privativas de liberdade, quando:*

I - aplicada pena privativa de liberdade não superior a quatro anos e o crime não for cometido com violência ou grave ameaça à pessoa ou, qualquer que seja a pena aplicada, se o crime for culposo;

II - o réu não for reincidente em crime doloso;

III - a culpabilidade, os antecedentes, a conduta social e a personalidade do condenado, bem como os motivos e as circunstâncias indicarem que essa substituição seja suficiente.

§ 1º - (VETADO)

§ 2º - Na condenação igual ou inferior a um ano, a substituição pode ser feita por multa ou por uma pena restritiva de direitos; se superior a um ano, a pena privativa de liberdade pode ser substituída por uma pena restritiva de direitos e multa ou por duas restritivas de direito.

§ 3º - Se o condenado for reincidente, o juiz poderá aplicar a substituição, desde que, em face de condenação anterior, a medida seja socialmente recomendável e a reincidência não se tenha operado em virtude da prática do mesmo crime.

§ 4º - A pena restritiva de direitos converte-se em privativa de liberdade quando ocorrer o descumprimento injustificado da restrição imposta. No cálculo da pena privativa de liberdade a executar, será deduzido o tempo cumprido da pena restritiva de direitos, respeitando o saldo mínimo de trinta dias de detenção ou reclusão."

Diante do gravíssimo caso brasileiro, de insuficiência do sistema penitenciário e a experiência que a supressão da liberdade em alguns casos não é a melhor opção de pena para recuperar um delinqüente, por conta dessa apreciação, têm surgido normas do espírito criativo dos nossos legisladores que possibilitam flexibilizar essa situação.

Dentro da concepção de penas de prestação de serviços à comunidade, o que já tem sido posto em prática é a utilização do potencial dos condenados detentores de bons conhecimentos de informática em treinamento de pessoal, ou em digitação de trabalhos para órgãos públicos.

É desse espírito criativo que o sistema penitenciário precisa para vir a ser viável. Devemos ter em mente que o avanço tecnológico não nos oferece apenas mais um meio de se cometerem novas modalidades criminosas, mas pode nos proporcionar soluções

para realizar a execução da pena em face do condenado de maneira a não ferir o princípio fundamental da dignidade humana.

Um método já em uso na Austrália, Inglaterra, EUA e Canadá, monitora o condenado por meio eletrônico, são aparelhos de GPS *("Global Position System")* sistema de posicionamento global[38]. Idealizado em 1968 nos EUA, o sistema consiste em um pequeno dispositivo de rastreamento acoplado ao tornozelo do usuário que pode ser localizado 24 horas por dia.

Há um projeto de lei apresentado pelo deputado Marcus Vicente (PSDB-ES), para a criação das chamadas "prisão virtual" ou "cadeia virtual", para condenados por crimes de menor potencial ofensivo. A idéia é monitorar o condenado mediante rede GPS (via satélite). O equipamento fica instalado numa tornozeleira ligada ao indivíduo. Sua remoção ou violação são detectadas automaticamente pelo sistema e o condenado é recolhido.

Segundo dados do Ministério da Justiça, haviam em março de 2001 em torno de 226.551 (duzentos e vinte e seis mil e quinhentos e cinquenta e um) presos no país e um déficit de 69.900 (sessenta e nove mil e novecentas) vagas. "Desse total, cerca de 126.000 (cento e vinte e seis mil) presos podem ser monitorados eletronicamente", argumenta o Deputado, reduzindo em 1/3 (um terço) o custo da prisão.

O projeto modifica o artigo 43 do decreto-lei 2.848/40, que trata das penas alternativas. O monitoramento eletrônico será, de acordo com o projeto, facultativo ao condenado e se constitui na grande alavanca do sistema do "*probation officer*", tornando em realidade a fiscalização que é a essência do instituto.

---

[38] Fonte: **http://www.jusdicere.com.br/artigos/março-01/art11.htm** acessado em 14/05/2002.

4. CONCLUSÃO

Da reflexão que exercemos sobre esse tema tão atual e pertinente, pudemos apreender que é imprescindível que nos ocupemos em resolver algumas carências em face do Direito Penal e Processual Penal, das quais destacamos as seguintes:

a) Meditar, discutir e procurar soluções para as questões da criminalidade informática, não só ao nível dos organismos estatais, mas também num plano acadêmico;

b) Legislar em âmbito nacional onde há lacuna na norma penal, para que aquelas novas modalidades de crimes não fiquem impunes;

c) Discutir ao nível internacional a criação, pela ONU, de uma comissão composta de representantes de todos os países, para juntos elaborarem um tratado que uniformize o debate sobre os crimes enfocados pelo nosso trabalho;

d) Preparar os operadores do direito para que tenham discernimento adequado perante às novas modalidades criminosas, introduzindo uma disciplina sobre "direito e informática";

e) Criar uma aliança, uma espécie de vínculo entre a polícia e empresas de tecnologia de ponta para garantir que estes estejam sempre se adequando à realidade tecnológica-jurídica do momento. Portanto, de um lado, realizando a atualização da polícia face aos equipamentos de última geração, de outro lado, orientando as empresas das falhas técnicas de segurança que porventura ainda existam nos sistemas de informática, que sejam alvo da criminalidade;

f) Decorre da sugestão anterior equipar a nossa polícia com equipamentos e recursos materiais e humanos compatíveis com o processo evolutivo;

g) Interação entre a polícia e os provedores nacionais e internacionais para uma cooperação mútua;

h) Preparar policiais habilitados em investigar os crimes de informática e crimes de alta tecnologia, com a realização de seminários e congressos internacionais;

i) Fazer intercâmbios de conhecimento sobre o tema entre as diversas polícias do globo;

j) Enfim, utilizar os recursos tecnológicos disponíveis para a implementação dos organismos estatais em consonância com a atualidade.

Das sugestões propostas, já temos algo em execução, porém há que se levar adiante as propostas com a seriedade que merece.

Ainda há o problema de arcaísmo das leis vigentes, elaboradas em épocas em que não se imaginava o estágio em que a criminalidade poderia chegar. Portanto, as leis devem se adaptar à realidade e às necessidades que a modernidade impõem. Deve-se ter cuidado para não criar uma lei específica demais, já que novos delitos surgirão com o progresso tecnológico.

Todavia, precisamos nos cercar de cautelas para não incidir na chamada 'inflação legislativa', criar desordenadamente leis que se tornem ineficazes em curto espaço tempo.

Para se ter uma idéia do quanto é importante que exista a regulação penal da informática, na Suíça as seguradoras perdem anualmente cerca de 6 (seis) milhões de francos, somente através de crimes de informática. Em 1984, na França, 700 (setecentos) milhões de francos foram perdidos em delitos de informática, valor este superior aos prejuízos com assaltos bancários no mesmo ano.

Há um atraso significativo no Brasil diante da perspectiva para os crimes de informática. Defronta-se com uma realidade triste: um grande despreparo dos policiais, isto é, falta treinamento e pessoal habilitado tecnicamente; inexiste uma estrutura compatível, considerando que a tecnologia progride mais rápido que os recursos disponíveis nas delegacias. É conveniente que a sociedade atente para a carência na questão da segurança, que exija um investimento maior no controle dessa situação em que mal conseguimos solucionar os crimes do mundo real, quem dirá do "virtual"?

Espera-se que os tecnocrimes não avancem as fronteiras, sob pena de ficarem impunes; para isso devemos exercitar a prevenção.

É preciso que se resguarde o anonimato oferecido pela internet, mas há que se criar condições para que se possam identificar, quando necessário, de alguma maneira o indivíduo que acessou a internet, de modo que se utilizasse uma senha inviolável (leitor da íris, de impressão digital etc.) para que numa investigação de autoria de suposto crime informático, houvessem condições de se chegar até o responsável pelo ato ilícito. Esse acesso à identificação ficaria restrito a investigadores da polícia sem que o sistema perdesse seu caráter anônimo para o resto da rede.

O problema da jurisdição só poderá ser resolvido por uma cooperação entre os países, por meio de tratados internacionais que regularizem o uso da Internet. As leis de vigência interna em um país não serão suficientes a um mundo onde as barreiras da informação foram eliminadas.

Apoiando a lógica do Direito Penal mínimo, defende-se aqui a proporcionalidade na aplicação das leis e, sempre que possível, a substituição da pena privativa de liberdade pelas restritivas de direito.

Os aspectos internacionais que envolvem os crimes de informática apresentam uma situação mais complexa. O regulamento internacional da Internet vai exigir um esforço coletivo ao nível mundial, possivelmente através de um documento de dimensão multilateral, a ser providenciado pela ONU que deve criar um organismo para essa situação nos moldes da OMC.

GLOSSÁRIO

Arpanet: Rede de computadores criada em 69 pelo Departamento de Defesa norte-americano, interligando na altura instituições militares. Em meados dos anos 70 várias grandes universidades americanas aderiram à rede, que deu lugar à atual Internet.

Bios: É a memória básica da máquina. Contem instruções primárias para o funcionamento correto da maquina. BIOS que fica armazenada a informação de que em seu PC existe um teclado, por exemplo.

***Bug*:** Erro em algum programa ou arquivo.

BBS: "*Bulletin Board System*". Computador (um ou vários) que permitem que os usuários se liguem a ele através de uma linha telefônica e onde normalmente se trocam mensagens com outros usuários, se procuram arquivos e programas ou se participa em conferências (fóruns de discussão) divulgadas por varias BBS. Digamos que uma BBS está para a Internet assim como uma aldeia está para o Mundo

***Browser*:** navegador, pesquisador. Programa que permite a navegação na rede WWW

Cavalo de Tróia: É uma espécie de "vírus", enquanto o "vírus" apenas danifica um programa útil e deixa o computador fora de operação, o cavalo de tróia é um programa disfarçado que pode ser programado para realizar muitas outras tarefas, como roubar informações importantes, tal como a senha do usuário por exemplo.

CERN: Sigla de ¨*Centre Europeen de Recherche Nucleaire*¨. Centro Europeu de Investigação Nuclear. Um dos centros mais importantes da Internet (e, claro, da investigação física). Nele

trabalham centenas (ou mesmo milhares?) de investigadores e a sua "jóia da coroa" é um grande circulo de aceleração de partículas com 27 Km de diâmetro, que fica por baixo de Genebra, na Suíça, atualmente o maior acelerador de partículas existente no Mundo.

***Chip*:** pastilha, circuito integrado; pequeno pedaço de silício (material semicondutor) sobre o qual são gravados ou fabricados (por dopagem) um número de componentes tais como transístores, resistores e capacitores, que juntos executam uma função (tarefa).

***Chat*:** é o serviço de conversa *"on-line"* que permite a comunicação via teclado, em tempo real, com quem quer que esteja conectado na mesma hora.

Ciberespaço: Com a internet surge a expressão ciberespaço, criada pelo escritor americano William Gibson, em 1984. O ciberespaço é o espaço virtual e sem fronteiras onde circulam as milhares de informações veiculadas nas redes de informática , como a Internet.

Computador: máquina que recebe ou armazena ou processa dados muito rapidamente de acordo com um programa armazenado; ± ***"analog computer'* = computador analógico** = computador que processa dados na forma analógica (isto é, dados que são representados por um sinal que varia continuamente em oposição a dados digitais); ± ***"digital computer"* = computador digital** = computador que processa dados na forma digital (isto é, dados representados na forma discreta); **± *"mainframe computer"* = computador *"mainframe"* (de grande porte)** = sistema poderoso de computador com alta capacidade de memória, que pode suportar um grande número de periféricos, podendo normalmente rodar vários programas ao mesmo tempo e ter vários computadores menores conectados a ele; **± *"microcomputer"* or micro = microcomputador ou micro** = sistema de computador completo baseado em um chip

microprocessador com capacidade limitada de memória. Normalmente é usado por uma pessoa por vez; ± ***"minicomputer" or mini*** = **minicomputador ou míni** = computador que normalmente tem poder de processamento maior que o de um microcomputador e menor que o de um *"mainframe"*, suportando deste modo menos periféricos e menos usuários que um "mainframe"; ± ***"personal computer" (PC) or "home computer"*** = **computador pessoal ou computador caseiro** = computador de pequena capacidade que pode ser usado em casa, onde as várias partes (telas, teclado, unidades de disco, unidade de processamento, memória, etc.) estão em um ou dois gabinetes pequenos e compactos. OBS.: com o avanço tecnológico de hoje e o barateamento dos microcomputadores, é possível ter computadores pessoais tão poderosos quanto os usados em empresas

Correio eletrônico - Correio transmitido por meios eletrônicos, normalmente, redes informáticas. Uma carta eletrônica contem texto (como qualquer outra carta) e pode ter, eventualmente, anexo um ou mais arquivos.

CPU: Sigla de *"Central Processing Unit"* - Unidade central de processamento, grupo de circuitos que executam as funções básicas de um computador composto de três partes, a unidade de controle, a unidade lógica e aritmética e a unidade de entrada/saída

Criptografia: Torna algum programa ou mensagem secreta, ou seja, só poderá ler aquela mensagem ou executar aquele programa a pessoa que tiver a chave criptográfica (que serve como uma senha) para desencripta-los.

Cyberspace: Ver ciberespaço.

***Download*:** carregar; (i) carregar, transferir um programa ou uma seção de dados de um computador remoto via um meio qualquer, p. ex. um cabo, um feixe de luz infravermelho, uma linha telefônica.

Costuma-se dizer, em linguagem popular, "baixar" determinado programa.

Dado: coleção de fatos compostos de números, caracteres e símbolos armazenados em um computador de tal modo que possam ser processados e transmitidos pelo computador.

DNS: *Sigla de "Domain Name Server"*. Designa o conjunto de regras e/ou programas que constituem um Servidor de Nomes da Internet. Um servidor de nomes faz a tradução de um nome alfanumérico (p. ex. microbyte.com) para um numero IP (p. ex. 192.190.100.57). Por exemplo, no DNS brasileiro, gerem-se todos os nomes terminados em br. Qualquer outro nome será também traduzido pelo mesmo DNS, mas a partir de informação proveniente de outro DNS (isto se essa informação não tiver sido previamente obtida).

***E-commerce*:** comércio eletrônico, via internet.

***E-mail*:** correio eletrônico, via internet.

Endereço eletrônico: É um cadeia de caracteres, do tipo "nome_usuario@qqcoisa.empresax.br" (sem aspas) que identifica univocamente um determinado utilizador dentro da Internet e, em particular, a sua caixa de correio eletrônica. Qualquer envio de correio eletrônico para esse utilizador deve ser feito para o seu endereço eletrônico.

Firewall: Parede de Fogo. Medida de segurança que pode ser implementada para limitar o acesso de terceiros a um determinada rede ligada à Internet. Os mecanismos de implementação são variados, percorrendo variados tipos de controle por "*software*" ou *hardware*. Num caso limite, a única coisa que uma "*firewall*" poderia deixar passar de um lado (rede local) para o outro (resto da Internet) era o correio eletrônico (podendo mesmo filtrar correio de/para

determinado site). Um sistema de segurança de rede, cujo principal objetivo é filtrar o acesso a uma rede.

FTP: Sigla de "*File Transfer Protocol*", é um protocolo de comunicação para transferência de arquivos entre dois computadores. É o método mais comum de transferência de arquivos entre dois locais na internet.

FTP *server:* Servidor de FTP. Computador que tem arquivos de "software" acessíveis através de programas que usem o protocolo de transferencia de arquivos, FTP.

***Hacking*:** É o ato de penetrar em sistemas computadores para obter mais conhecimentos e entender como funciona. "Hacker" é um curioso da Informática.

Hardware: são os componentes físicos do computador e seus acessórios. São a placa mãe, placa de "fax-modem", interfaces, etc.

Homepage: é a pagina de entrada de um site na "*web*", ou de outro sistema de hypertexto ou de hipermídia, que geralmente contém uma apresentação geral e um índice, com elos de hipertexto que remetem às principais seções do site, visando facilitar a navegação pelo sistema.

HTML: Sigla de "*Hypertext Markup Language*". É uma linguagem de descrição de paginas de informação, standard no WWW. Com essa linguagem (que, para alem do texto, tem comandos para introdução de imagens, formulários, alteração de fontes, etc.) podem-se definir paginas que contenham informação nos mais variados formatos: texto, som, imagens e animações.

HTTP: Sigla de "*Hyper Text Transport Protocol*": é o protocolo utilizado para a transferência de páginas de hypertexto ou outros documentos na internet. O servidor WWW fornece a informação, requerida e transferida para o cliente através do protocolo http.

Informação: são os fatos e dados fornecidos à máquina e integram o conhecimento.

Informática: Ciência que visa ao tratamento da informação através do uso de equipamentos e procedimentos da área de processamento de dados.

Interface: (i) ponto no qual um sistema de computação termina e um outro começa; (ii) circuito ou dispositivo ou porta que permite que duas ou mais unidades incompatíveis sejam interligadas em um sistema padrão de comunicação, permitindo que se transfiram dados entre eles; (iii) parte de um programa que permite a transmissão de dados para um outro programa

Internauta: é o usuário da internet.

Intranets: São redes privadas que estão sendo desenvolvidas pelas empresas com o objetivo de facilitar a comunicação interna. Elas utilizam os mesmos recursos gráficos da Internet e, eventualmente, estão conectadas à grande rede.

IP: Sigla de "*Internet Protocol*" - é o protocolo utilizado para a comunicação na internet. As informações trafegam divididas em pacotes sincronizados pelo protocolo.

IRC: sigla que designa "*Internet Relay Chat*", é um sistema de conversação multi-usuário, em tempo real.

Link: É a ligação de um item em um documento a outros documentos. Este "link" pode transportar o acesso do usuário a um texto, uma imagem, som, vídeo, "*homepage*", outro documento ou mesmo outro protocolo, através do seu endereço na Rede.

Listserv: forma um enorme repositório de informação, é a área da Internet reservada aos grupos de discussão sobre assuntos específicos.

Login: Identificação de um utilizador perante um computador. Fazer o "login" é o ato de dar a sua identificação de usuário ao computador.

Logout: Ato de desconectar a sua ligação a um determinado sistema ou computador.

Mail Bomb: É a técnica de inundar um computador com mensagens eletrônicas.

Modem: Modulador/Demodulador. Pequena interface interna (conectada no interior do computador) ou externa (numa caixa de plástico conectada via cabo na CPU) que permite ligar um computador à linha telefônica, para assim estar apto a comunicar através de um protocolo. Muitos dos modems são também capazes de realizar funções de "fax".

Navegar: Na Internet significa passear, procurar informação, sobretudo no WWW.

Password: Palavra-chave usada para identificação do usuário, em conjunto com o "login".

Periférico: Unidade periférica = (i) item de "*hardware*" (como terminal, impressora, monitor, etc.) que é conectado a um sistema de computador; (ii) qualquer dispositivo que permite comunicação entre um sistema e si mesmo, mas não é operado diretamente pelo sistema.

Programa: conjunto completo de instruções que controla um computador para executar uma tarefa específica

Protocolo: Sinais, códigos e regras pré-combinadas para serem usadas na troca de dados entre sistemas; ± ***"protocol standards"*** **= padrões de protocolo =** padrões estabelecidos para permitir a troca de dados entre quaisquer sistemas de computador submetidos ao padrão.

Realidade virtual: É a simulação via computador de uma situação real, possível graças ao ciberespaço. No espaço cibernético, imaterial e sem fronteira, os computadores podem representar uma realidade em três dimensões, conhecida também como realidade virtual. Ela estabelece uma nova interatividade do usuário com o computador. Pode-se mexer objetos na tela do aparelho apenas com movimentos dos dedos, sem o uso do teclado ou do *mouse*. Óculos, luvas, capacetes, máscaras e sensores ligados ao corpo ajudam a criar sensações cada vez mais próximas da realidade. O usuário sente a textura de objetos, a iluminação e temperatura do ambiente. Novos *softwares* buscam incluir as sensações olfativas e gustativas.

***Script*:** roteiro; manuscrito; documento original; cópia.

Servidor (*Server*): Computador que oferece serviços.

Shareware: "*Software*" que é distribuído livremente, desde que seja mantido o seu formato original, sem modificações, e seja dado o devido credito ao seu autor. Normalmente, foi feito para ser testado durante um curto período de tempo (período de teste/avaliação) e, caso seja utilizado, o usuário tem a obrigação moral de enviar o pagamento ao seu autor (na ordem de algumas - poucas - dezenas de dólares). Quando é feito o registo, é normal receber um manual impresso do programa, assim como uma versão melhorada, possibilidade de assistência técnica e informações acerca de novas versões.

***Site*:** é o conjunto de documentos apresentados ou disponibilizados na "*Web*" por um indivíduo, instituição ou empresa, que pode ser fisicamente acessado por um computador e em endereço específico na rede.

SMTP: Sigla de "*Simple Mail Transport Protocol*". Protocolo utilizado entre os programas que transferem correio eletrônico de um computador para outro.

***Software*:** são os programas utilizados no computador.

***Spam*:** mensagens de correio eletrônico enviadas ao destinatário sem serem solicitadas, resultando em desperdício de espaço em disco e largura de banda nos meios de transmissão.

Telemática: é a ciência que cuida da manipulação e utilização da informação, com o uso do computador e meios de telecomunicação.

***Telnet*:** é um "*software*" que permite acessar remotamente outras máquinas.

User: O usuário dos serviços de um computador, normalmente registado através de um "login" e um "*password*".

Usuário: Ver "*user*".

***Vírus* de computador:** pequeno programa hostil criado para provocar danos em outros programas importantes como o sistema operacional, impedindo que o computador funcione normalmente. Podem agir de imediato ou só produzirem efeito em determinada data ou evento no computador.

Web: Em português, teia. Abreviatura para designar o *"World-Wide-Web"*.

***World Wide Web*:** ("ampla teia mundial") é um avançado sistema de navegação dentro da Internet. Com a "*web*" pode-se utilizar o recurso de hipertexto: você está escrevendo um texto sobre um assunto qualquer e com um simples comando no programa pode obter mais informações referentes ao assunto, sem ter que sair da tela onde está o seu texto. A WWW reúne todos os outros sistemas de comunicação pela Internet, como o "*Gopher*", o WAIS e a própria WWW.

BIBLIOGRAFIA

AMARAL, Sylvio do. **Falsidade Documental**. 3. ed. São Paulo : RT, 1989. 213p.

BASTOS, Cleverson Leite e KELLER, Vicente, **Aprendendo a Aprender – Introdução à Metodologia Científica**, 10º edição, Petrópolis, 1998, p.85.

BLOOMBECKER, Buck. **Crimes Espetaculares de Computação**. Rio de Janeiro : LTC, 1992, 228p.

CASTELLS, Manuel. **A Sociedade em Rede**. SP: Paz e Terra, 1999.

CASTRO, Carla Rodrigues Araújo de. **Crimes de Informática – e seus Aspectos Processuais**. 1º ed. Rio de Janeiro: Lumen Júris, 2001. 196 p.

CERQUEIRA, Tarcísio Queiroz. **O Direito do Ciberespaço**. Texto apostilado, 1995.

CERQUEIRA, Tarcísio Queiroz. **Software Direito Autoral e Contratos**. Rio de Janeiro : ADCOAS, 1993. 371p.

Brasil, Constituição. **Constituição da República Federativa do Brasil**. Brasília-DF: Gráfica do Senado Federal, 1988.

CORRÊA, Gustavo Testa. **Aspectos Jurídicos da Internet**. Saraiva, 1ª edição, 2000, 160p.

COSTA, Marco Aurélio Rodrigues. **Crimes de Informática**. In www.jus.com.br/doutrina/crinfo1.htm. Acessado em 23/03/2002.

DOTTI, René Ariel. **Controle de Informática**. In: Revista dos Tribunais. São Paulo, n. 518, p. 265-266, dez 1978.

Enciclopédia Digital Grolier. Versão 8.01 (inglês). The 1996 Grolier multimedia encyclopedia.

FARIA, Bento de. **Código Penal Brasileiro (Comentado).** Rio de Janeiro : Récord, 1959. v. III. 415p.

FERREIRA, Aurélio Buarque de Holanda. **Novo Dicionário da Língua Portuguesa**. 2. ed. Rio de Janeiro : Nova Fase, 1986. 1838p.

FERREIRA, Ivete Senise. **Os Crimes de Informática**. In: BARRA, Rubens Prestes, ANDREUCCI, Ricardo Antunes. **Estudos Jurídicos em Homenagem a Manoel Pedro Pimentel**. São Paulo : RT, 1992. 9. p.139-162.

GOUVÊA, Sandra. **O Direito na Era Digital – os Crimes Praticados por Meio da Informática**. RJ: Mauad, 1997.

JEHORAM, Hermann Cohen. **Proteção do "Chip".** In: Cadernos de Direito Econômico e Empresarial. Rio de Janeiro : RDP, jul/set 1991. p. 278-281

LICKS, Otto Banho: ARAÚJO JÚNIOR, João Marcelo. **Aspectos Penais dos Crimes de Informática no Brasil.** In: Revista do Ministério Público, São Paulo : Nova Fase, 1994. p. 82-103.

LUCCA, Newton De e Simão Filho, Adalberto (coordenadores) e outros. **Direito & Internet – Aspectos Jurídicos Relevantes**. Bauru, SP: EDIPRO, 2000.

M@RCIO. **A Internet e os Hackers: Ataques e Defesas**. São Paulo-SP. Chantal editora.

MARQUES, José Frederico. **Elementos de Direito Processual Penal**. 1ª ed. Campinas: Bookseller, 1997. Vol. I – IV.

MICHAELIS: **Moderno Dicionário da Língua Portuguesa** / São Paulo: Companhia Melhoramentos, 1998.

MIRABETE, Julio Fabbrini. **Código de Processo Penal Anotado**.4ºed. São Paulo: Atlas, 1996.

NEGROPONTE, Nicholas. **O Computador Liberta**. Veja, São Paulo, v. 28 n. 30, p. 7-10, jul 1993.

OLIVO, Luís Carlos Cancellier de. **Direito e Internet: a Regulamentação do Ciberespaço**. Florianópolis: Ed. Da UFSC, CIASC, 1998. 154p.

PALADINO, Enzo. **Novo dicionário Técnico de Informática**. São Paulo : Ciência Moderna, 1986. 458p.

PALAZZI, Pablo A. **Delitos Informáticos**. Buenos Aires: Ad Hoc, 2000.

PINHEIRO, Reginaldo Cesar. **Os Crimes Virtuais na Esfera Jurídica Brasileira**. Boletim IBCCRIM. São Paulo-SP. abril/2001. Nº. 101, ano 8.

RNT-Revista Nacional de Telecomunicações. Nº. 261 Maio/2001.

Rodrigo Pinto **Em defesa dos Sem-Terra do Ciberespaço**. Artigo in http:\\www.cg.com.br em 20/05/2002

SOIBELMAN, Leib. **Enciclopédia do Advogado**. 5ª edição. Rio de Janeiro: Thex Ed.: Biblioteca Universidade Estácio de Sá, 1994.

TASSE, Adel El. **Investigação Preparatória**. 2ª edição, Curitiba: Juruá, 2001.

TEODORO JUNIOR, Euclides. **Computador a Serviço do Crime**. In: BANAS. São Paulo, v. 25, n. 1192, p.30-32, dez 1978.

TOFFLER, Alvin. **A Terceira Onda**. 10ª ed. Rio de Janeiro: Editora Record. 1980. 494p.

UNIVERSIDADE FEDERAL DO PARANÁ. Sistema de Bibliotecas. **Teses, Dissertações, Monografias e Trabalhos Acadêmicos** / Universidade Federal do Paraná, Sistema de bibliotecas – Curitiba: Ed. da UFPR, 2000. 44p.

VIANNA, Túlio Lima. **Dos Crimes por Computador**. Monografia realizada para graduação na UFMG. Belo Horizonte, 1999.