UNIVERSIDADE FEDERAL DE CAMPINA GRANDE
CENTRO DE CIÊNCIAS JURÍDICAS E SOCIAIS
UNIDADE ACADÊMICA DE DIREITO
CURSO DE CIÊNCIAS JURÍDICAS E SOCIAIS

EDNELTON HELEJONE BENTO PEREIRA

DOS CRIMES DE INFORMÁTICA E SUA NECESSÁRIA TIPIFICAÇÃO EM CONCORDÂNCIA AO PRINCÍPIO DA RESERVA LEGAL

SOUSA - PB
2006

EDNELTON HELEJONE BENTO PEREIRA

DOS CRIMES DE INFORMÁTICA E SUA NECESSÁRIA TIPIFICAÇÃO EM CONCORDÂNCIA AO PRINCÍPIO DA RESERVA LEGAL

Monografia apresentada ao Curso de Ciências Jurídicas e Sociais do CCJS da Universidade Federal de Campina Grande, como requisito parcial para obtenção do título de Bacharel em Ciências Jurídicas e Sociais.

Orientador: Professor Esp. Admilson Leite de Almeida Júnior.

SOUSA - PB
2006

EDNELTON HELEJONE BENTO PEREIRA

DOS CRIMES DE INFORMÁTICA E SUA NECESSÁRIA TIPIFICAÇÃO EM CONCORDÂNCIA AO PRINCÍPIO DA RESERVA LEGAL

BANCA EXAMINADORA

Prof. Admilson Leite de Almeida Júnior

Prof. .....

Prof. .....

Dedico este trabalho a todas as pessoas que me acompanham em meu dia a dia. aos meus mestres, colegas, aos meus pais e meus irmãos, a minha namorada e por fim a meus amigos, pelo auxílio que a mim foi oferecido pelos mesmos.

Agradeço a todos que de maneira direta ou indireta contribuíram para elaboração deste trabalho. Agradeço a meus colegas de sala pelas dicas ofertadas, a minha namorada Hérika pela força e paciência nas horas que me encontrava desenvolvendo esse trabalho. Aos meus familiares pelo esforço e silêncio necessários para conclusão desse trabalho, e em especial aos meus professores pelo conhecimento necessário para compreensão do tema escolhido.

"Eterno é tudo aquilo que dura uma fração de segundos, mas com tamanha intensidade que se petrifica e nenhuma força consegue destruir."

Carlos Drummond de Andrade.

SUMÁRIO

RESUMO

Para uma efetiva garantia do princípio da reserva legal para o direito, a constituição federal em seu artigo 5º, inciso XXXIX, e o código penal brasileiro, em seu artigo 1°, vincula a necessidade de uma lei especifica para que determinada circunstância seja considerada delitiva. Os crimes de informática são crimes que vieram a acompanhar o avanço tecnológico e o advento da era digital em todo o mundo, fazendo com que surja por meio dos países uma adequação legal e uma tipificação dos delitos para que referidas condutas passem a ser consideradas como delitivas. Os métodos utilizados na abordagem do assunto foram o dedutivo e o histórico, onde se buscou por meio de uma abordagem histórica informar todo o surgimento da tecnologia no referente a informatização e o surgimento com isso das ilicitudes digitais, informando o perfil dos criminosos, a motivação para cometimento dos delitos e a necessidade de legalização da prática desses atos para uma garantia de tranqüilidade societária. Foi realizada uma extensa pesquisa científica em revistas de informática, em doutrinas, legislações e principalmente em artigos na internet. O trabalho foi abordado sob uma ótica jurídica, mas com grande enfoque sociológico, tendo em vista que tanto a ciência jurídica como a da informática, são hoje inseparáveis, uma dependendo diretamente da outra. O resultado do trabalho foi compilado, breve, adequado, minimizado e efetivo no intuito de demonstrar a necessária tipificação dos delitos de informática para que se haja uma garantia do princípio da reserva legal.

Palavras-chave: Avanço tecnológico, princípio da reserva legal, crimes de informática, criminosos digitais, crimes virtuais, tipificação.

SUMMARY

For an effective guarantee of the principle of the legal reserve for the right, the federal constitution in its article 5º, interpolated proposition XXXIX, and the Brazilian criminal code, in its article 1°, ties the necessity of a law specifies so that definitive circumstance is considered criminal. The computer science crimes are crimes that had come to follow the technological advance and the advent of the digital age in the whole world, making with that it appears by means of the countries a legal adequacy and a criminal type of the delicts so that related behaviors they pass to be considered as criminal. The methods used in the boarding of the subject had been deductive and the description, where if it searched by means of a historical boarding to all inform the sprouting of the technology in the referring a computerization and the sprouting with this of the digital illegalities, informing the profile of the criminals, the motivation for cometiment of the delicts and the necessity of legalization of the practical one of these acts for a guarantee of societary tranquillity. An extensive scientific research in computer science magazines was carried through, in doctrines, legislações and mainly in articles in the Internet. The work was boarded under a legal optics, but with great sociological approach, in view of that as much the legal science as of computer science, is today non-separable, one depending directly on the other. The result of the work was compiled, soon, adjusted, minimized and effective in intention to demonstrate the necessary criminal type of the computer science delicts so that if it has a guarantee of the principle of the legal reserve.

Word-key: Technological advance, principle of the legal reserve, digital crimes of computer science, criminals, virtual crimes, criminal type.

1.0 INTRODUÇÃO

As inúmeras mudanças acontecidas na estrutura tecnológica atual fizeram com que a sociedade procurasse novos meios de se amoldar a esse forte avanço da tecnologia mundial. Todos os ramos das ciências sofreram alterações, e dentre esses ramos não poderia ficar de fora o ramo da ciência jurídica. O Direito se apresentou mediante tais fatos de forma quase inerte no tocante a esse assunto, e, de forma direta pode-se observar que princípios constitucionais presentes no direito estão sendo gritantemente violados, como o caso do princípio da reserva legal.

O avanço da tecnologia foi algo que surgiu de forma rápida e inesperada, talvez não gerando as condições necessárias para que a sociedade conseguisse se adequar a essas alterações, criando uma confusão generalizada no que tange a legislação para efetiva punição aos delitos relacionados à informática.

O presente trabalho tentará de forma sucinta e objetiva demonstrar a necessidade de adequação, em caráter de urgência, dessas novas tendências mundiais, ao âmbito jurídico, fazendo com que o principio da reserva legal em destaque seja respeitado, não gerando assim uma violação ao Direito societário.

A justificativa central desse trabalho, em última análise, é de demonstrar a toda a sociedade, a necessária criação de novas leis, que formem tendência de adequação legal dos crimes de informática em concordância ao principio da reserva legal, existente no artigo 5º, XXXIX, da constituição federal e também presente no artigo 1º do código penal brasileiro.

Para atingir este objetivo se realizou amplas pesquisas, de âmbito referencial, para que pudesse encontrar o aludido tema em literaturas científicas, com o grande apoio de pesquisas realizadas na internet, revistas jurídicas, revistas comuns, leis e doutrina específica, a qual é bastante limitada.

Para o desenvolvimento da estrutura da pesquisa cientifica, dentro de uma linha de raciocínio lógico, foi utilizado o método dedutivo, partindo da idéia de que a sociedade não pode ficar a mercê de uma ausência de estrutura legal que possa penalizar os criminosos digitais, ferindo assim princípios e normas constitucionais e especificas.

Os resultados de tal pesquisa foram reunidos, analisados, seqüenciados, adequados e resumidos, de forma que se conseguisse transmitir a noção de que, da maneira que se encontra

o sistema jurídico em relação a tal assunto, não se pode continuar, pois a necessidade de leis especifica ao tema é cada vez mais notória.

Para isso buscou-se demonstrar no primeiro capítulo o histórico da informatização, com o surgimento das primeiras máquinas de computar e as mudanças tragas a sociedade e ao pensamento societário com isso, sendo abordada em conjunto a evolução dessas máquinas, o surgimento dos computadores, o que gerou de forma espontânea o inicio da era digital, onde referido avanço tecnológico ocasionou um avanço da criminalidade.

O segundo capitulo trouxe o conceito de crimes de informática, o surgimento dos tais crimes digitais, o caminhar rápido com que aconteceu o advento de tais ilicitudes, a possibilidade de tentativa nos crimes digitais, além dos criminosos em si, suas classificações em grau hierárquico e alguns famosos criminosos mundialmente, condenados pela prática de tais criminalidades.

O terceiro capítulo aborda a necessária atuação do Estado quanto aos crimes de informática, de forma direta, apresentando o Estado como meio maior de proteção da sociedade, e os serviços com que a tecnologia poderia prover para auxiliar essa sociedade, trata também do difícil controle dos crimes digitais e da ampla oportunidade para o cometimento de tais ilícitos, traz o relacionamento da lei em face desse problema e dois importantíssimos projetos de lei, que tramitam a muito tempo no congresso nacional, que poderiam gerar um certo conforto e diminuição na criminalidade se obtivessem sua efetivação.

O quarto capítulo trata a respeito dos princípios do direito como num todo. Os meios de interpretação de tais condutas, desde a hermenêutica jurídica quanto a analogia jurídica, traz o princípio da legalidade para o direito penal e retira desse princípio o que diz respeito a parte da anterioridade, restando assim o princípio mor para a resolução de referido trabalho, sendo este denominado princípio da reserva legal, com sua adequação aos delitos virtuais e a necessária forma de se tipificar os delitos para que os mesmos não sejam fatos atípicos, em concordância ao próprio principio findo abordado.

O quinto capítulo trata a respeito das novas tendências no Brasil e no mundo a respeito da criminalidade de informática, a questão da territorialidade e extraterritorialidade da lei, traz o desrespeito com que os crimes digitais ocasionam as soberanias dos países, além do direito internacional em relação ao assunto e a utilização do direito comparado, além de algumas

novas tendências brasileiras sobre os fatos com a citação de jurisprudências advindas de tribunais brasileiros.

Essa nova função de delitos gerou uma necessária tipificação de suas condutas em leis, de caráter especifico objetivando uma garantia da efetivação do princípio constitucional da reserva legal.

2.0 CAPÍTULO I

2.1 O surgimento da era digital e dos crimes de informática

2.1.1 O surgimento das máquinas de computar

O computador é uma invenção sem criador próprio, isso contrariando a lógica e outras invenções que possuem nome, sobrenome, patente e atestado de criação de obra por parte do autor que a desenvolveu, isso parte do suposto que o computador é um aperfeiçoamento constante de idéias anteriores.

A primeira máquina de computar que se possui relato surgiu há aproximadamente 5.500 anos atrás, e se chamava ábaco[1], uma maquina de calcular onde sua grande desvantagem era que o operador da mesma não podia se distrair nem interromper o processo de computação, caso isso viesse a acontecer, teria de reiniciar todo o processo de computação, pois o ábaco não possui memória.

O primeiro instrumento moderno de calcular, construído pelo físico, matemático e filosofo francês Blaise Pascal, foi uma somadora, em 1642. Essa máquina possuía seis rodas dentadas, cada delas contendo algarismos de 0 a 9, permitindo somar até três parcelas por vez, até o resultado final de 999.999. Pascal morreu em 1662 com trinta e nove anos de idade, porém, antes de sua morte, Pascal deixou outras invenções em varias áreas da ciência, dentre outros inventos de Pascal podemos destacar um que se utiliza até os dias de hoje, a caixa registradora.

A somadora de Pascal foi sendo aperfeiçoada por vários outros inventores, e teve uma vida útil de quase duzentos anos, funcionando cada vez melhor mas possuindo sempre um limite, a entrada de dados dependia sempre da eficiência da pessoa que estivesse batendo os números em sua tecla, então dependia-se rapidamente de uma solução para o aumento da velocidade de alimentação de dados, e quem conseguiu esse feito, foi outro francês, Joseph-Marie Jacquard, filho de tecelões e ele também aprendiz têxtil, sentia-se incomodado com a monótona tarefa de alimentar os teares com novelos de linhas coloridas para formar os

---

[1] O ábaco é um antigo instrumento de cálculo, formado por uma moldura com bastões ou arames paralelos, dispostos no sentido vertical. Teve origem provavelmente na Mesopotâmia, há mais de 5.500 anos. O ábaco pode ser considerado como uma extensão do ato natural de se contar nos dedos.

desenhos nos panos que estavam a serem fiados, como a tarefa era manual, seu serviço era a cada segundo trocar o novelo, seguindo as determinações de contraste, então, passado-se vinte anos matutando, Jacquard percebeu que as mudanças eram sempre seqüenciais, inventando assim um processo de cartões perfurados, onde o contramestre registrava ponto a ponto a receita para confecção de um tecido, construindo assim um tear automático que, lia os cartões e executava as operações nas seqüências programadas. Dez anos após sua primeira demonstração, já havia mais de 10 mil teares de cartões em uso na França.

Os mesmos cartões perfurados de Jacquard obtiveram uma decisiva influência no ramo da computação e deram um passo crucial para originar os computadores, pois eram maneiras eficientes de alimentar a maquina com milhares de dados em poucos minutos, eliminando a lentidão humana. Em 1834 um Inglês de nome Charles Babbage conseguiu equacionar os cartões perfurados de Jacquard, através de um projeto chamado de aparelho analítico, que anteviu os passos que até hoje são a base de funcionamento de um computador, pois o aparelho conseguia:

1°. Alimentar dados, através de cartões perfurados;
2°. Possuir unidade de memória, onde os números podiam ser armazenados e reutilizados;
3°. Programar seqüencial as operações por um procedimento hoje em dia conhecido como sistema operacional.

A maquina de Babbage, porém nem chegou a ser construída, pois o mesmo apenas era Professor e não dispunha de recursos suficientes para sua construção, deixando assim de legado seus escritos, que passaram a ser então leitura obrigatória para todos os inventores que dali em diante se aventurassem no mesmo caminho, espalhando seus conceitos teóricos pelo mundo, até os cartões perfurados de ganharem sua primeira aplicação lógica na computação de dados através de Hollerith.

O conceito de Hollerith possuía duas etapas: primeiro transferir dados numéricos para um cartão duro, perfurando-o em campos predeterminados, depois transformar os furos em impulsos, através da energia elétrica que passava por eles, ativando dessa forma os contadores mecânicos dentro de uma maquina. Hollerith conseguiu assim unir os cartões perfurados de Jacquard e o conceito de impulsos elétricos para transmissão de dados, usando um principio

desenvolvido por Samuel Morse[2] em 1844, quando do invento do telégrafo transformando letras e números em sinais elétricos.

Em 1887, durante estudos estatísticos sobre mortalidade, utilizou-se pela primeira vez os cartões perfurados de Hollerith, mas apenas 13 anos depois em 1890, durante o recenseamento dos Estados Unidos, foi que o sistema passou a ser conhecido mundialmente, o recenseamento foi rápido em relação ao que seria e gerou aos Estados Unidos economia em tempo e em dinheiro, graças ao sistema desenvolvido por Hollerith, sendo esse um grande avanço para a geração de máquinas de computar que viria logo em seguida, os avós do computador, que esperavam apenas de uma pequena ajuda para então se iniciar o processo de desenvolvimento da computação.

Apesar de ser um dos maiores contra–sensos da humanidade, o que ainda estava faltando para o computador "computar", talvez fossem guerras. Elas tem sido uma espécie de Dínamo tecnológico, uma inovação mundial que antecipou ainda mais o desenvolvimento tecnológico. Foi durante a II Guerra Mundial (1938/1945), que a ciência da computação deu seu salto definitivo, com a criação de uma maquina pelos nazistas, chamada de Enigma.

Durante os primeiros anos de guerra, os serviços de contra–espionagem dos países aliados conseguiram interceptar as mensagens dos alemães, mas era incapaz decifra–las, quando finalmente conseguiam, pouco adiantava, pois, a mensagem seguinte vinha num código diferente. Isso porque a Enigma gerava novos códigos a cada mensagem, a partir daí decifrar como esses códigos eram reprogramados tornou-se prioridade absoluta, e os ingleses resolveram que isto não era trabalho para Heróis autoritários com bazucas e sim cientistas capazes. Um deles foi Alan Turing, que já havia publicado trabalhos teóricos sobre computação de dados antes da guerra, por isso foi recrutado pelas forças armadas. Se suas teorias estivessem corretas, elas levariam à construção de um equipamento capaz de imitar o cérebro humano, para isso bastaria, "alimenta–la" com qualquer mensagem alemã, que em seguida devolvia à mensagem de forma compreensível. Então, Thomas Flowers construiu uma nova maquina, logo após o aprendizado com a Enigma, mais sofisticada e elaborada, e a chamaram de Colossus, demoraram um ano para construí–la, mas logo após viram sua eficiência, uma vez plugada, programada e "alimentada", resolvia qualquer questão de

---

[2] **Samuel Finley Breese Morse**, nasceu em Charlestown aos 27 dias do mês de abril de 1791 e morreu em Nova Iorque em 2 de abril de 1872. Foi inventor e pintor de cenas históricas estadunidense. Ficou conhecido mundialmente devido as invenções do código morse e do telégrafo.

criptografia em poucos minutos, mesmo assim, o Colossus ainda não era um modelo bem acabado de computador, só executava uma única e específica tarefa, mas mostrou que a computação poderia resolver rapidamente qualquer problema que pudesse ser transformado em instruções numéricas.

Um dos criadores do primeiro computador mecânico, perfeitamente operacional, controlado por um programa binário, foi o alemão Konrad Zuse. Infelizmente a máquina de Zuse, chamada Z1, foi reduzida às cinzas logo após um bombardeio dos aliados sobre Berlim, restaram apenas às anotações do próprio Zuse (as plantas de construção, e os princípios do Z1) que mostraram incrivelmente semelhantes a tudo o que viria depois.

Uma campanha promocional, muito bem feita, talvez explique o motivo por que se acredita que o primeiro computador tenha sido uma máquina americana chamada ENIAC.

O ENIAC era uma geringonça que funcionava usando 17.480 válvulas de rádio, pesava 4 toneladas, media incríveis 30 metros de comprimento por 3 de altura, ocupava uma área de 180 m², e era capaz de fazer 5 mil somas por segundo, foi ligado na tomada em 1946. Foi construído por dois cientistas da Universidade da Pennsylvania, no EUA, e seu nome vem das iniciais de *Eletronic Numerical Integrator And Computer* (Integrador e Computador Numérico Eletrônico). Funcionava de forma bem diferente dos atuais computadores, hoje em dia ao clicar o mouse, ou ao teclar ESC, um usuário não tem a mínima idéia de como as coisas acontecem lá dentro, simplesmente o comando é obedecido, no ENIAC era completamente diferente, as coisas ocorriam do lado de fora da máquina. Primeiro cientistas desenvolviam equações matemáticas na seqüência exata em que elas tinham que ser codificadas pelo sistema. A seguir seis especialistas programavam o computador para executá-las, girando botões e plugando centenas de fios nos locais corretos, então o que se é chamado hoje de sistema operacional, naquela época era uma operação totalmente manual.

Na decada de 30, muitos inventores simultaneamente desenvolviam projetos de somadoras e calculadoras de alta velocidade, sendo que em 1939 foi desenvolvida pelo doutor John Atasanoff, auxiliado pelo estudante Clifford Berry, um aparelho que foi denominado ABC (Atasanoff Berry Computer), que foi demonstrado para dezenas de outros inventores. Afirma-se que o projeto do ABC experimental, deu inicio ao ENIAC, gerando assim a primeira lide no processo computacional, por parte de Atasanoff que assegura ser seu o projeto copiado e gerador do ENIAC.

A IBM também participa dessa história, reivindicando ser de sua propriedade a autoria do primeiro computador moderno, o Havard Mark I, tinha o nome técnico do calculador automático seqüencial e foi construído entre 1939 e 1944 pelo inventor Howard Aiken e financiado pela IBM.

Em 1950, surgiu no mercado um circuito integrado que veio para revolucionar os formatos das grandiosas maquinas. Chamado de transistor, o mesmo veio para substituir as antigas válvulas, essas por serem enormes, ocupavam grande espaço dentro das maquinas, e em 1960 já se via relatos de programas que conseguiam fazer bolinhas pular na tela, ou fazer tijolos sendo empilhados, esses são os avôs dos softwares modernos.

Em 1962, três sujeitos com média de 25 anos de idade cada, desenvolveram nos Estados Unidos o *SpaceWar,* o primeiro vídeo-game da humanidade. O Spacewar demonstrava que era possível ao operador escapar da ditadura dos programas quadrados e decidir o que iria acontecer na tela no momento seguinte.

Em 1970, a *Xérox Corporation*[3], contratou cientistas renomados para que os mesmos desenvolvesem projetos baseando seus experimentos para o avanço da tecnologia. O primeiro experimento foi uma maquininha chamada de Alto, que consistia apenas em uma tela vetical de televisão acoplada a um teclado semelhante a de uma máquina de escrever, ambos conectados em uma caixa um pouco maior que um nobreak[4] atual, dentro do qual programas com instruções faziam a engenhoca funcionar. Esse conceito era altamente revolucionário para a época, em que computadores eram enormes, pesados e caros. Sendo então da Xérox o conceito de que fora produzido o primeiro micro computador a funcionar na prática conforme a teoria.

A partir do conceito do ALTO, os cientistas da Xérox conseguiram desenvolver um projeto onde vários micro computadores ficassem interligados entre si por meio de uma rede, permitindo assim aos usuários que compartilhassem informações entre si, fazendo assim o que nem os grandes computadores da época conseguiam fazer. Essa rede foi batizada de **ETHERNET.**

---

[3] Xerox Corporation é uma empresa estado-unidense baseada em Stamford (Connecticut). O logo da Xerox é a letra X maiúscula vermelha (Xerox).A Xerox é conhecida mundialmente como a inventora da fotocopiadora, mas ela fabrica também impressoras.

[4] Aparelho que contem baterias, para em eventual queda de energia elétrica continue o funcionamento do equipamento utilizado, sem dano para o operador. O tempo de uso do equipamento depende da capacidade de armazenamento do mesmo.

Apesar do grande avanço trago com o Alto, o mesmo não foi colocado a venda, ficando essa missão para 1975, por parte de uma empresa denominada MITS[5], que colocou a venda no mercado um kit com peças que tinham que ser montadas pelo próprio usuário em sua casa, o que seria o surgimento do micro computador caseiro, que já possuía um elemento denominado de microprocessador, desenvolvido por dois jovens americanos de nomes: Paul Allen e Bill Gates, gerando assim o inicio da era Apple de fabricação de micro computadores de uso doméstico e comercial, ficando por muito tempo no mercado, vindo logo em seguida a criação dos sistemas operacionais para funcionamento dos micros, e o constante avanço de mudanças que não permitem o acompanhamento da sociedade por parte de atualização. Enquanto uma máquina chega ao mercado, dezenas de outros projetos já se encontram em estudo para um avanço da tecnologia, gerando um constante índice de rotatividade nas maquinas nos dias atuais. No Mundo as gerações de computadores vão se apresentando de forma rotineira, com um mesmo padrão em processo de desenvolvimento desde 1981, ocorrendo modificações constantes, que vão desde o surgimento de um co-processador matemático para auxilio do processador, como aconteceu no modelo 286 DX-2 até os processadores de 4 GHz[6] (Gigahertz) de Velocidade, como os atuais Pentium 4, existentes no mercado atual, propiciando assim aos consumidores uma maior facilidade de acesso a era dos computadores.

2.1.2 O surgimento da internet

A Internet nasceu praticamente sem querer. Foi desenvolvida nos tempos remotos da Guerra Fria sendo primeiramente denominada de Arphanet, tendo função de manter a comunicação entre as bases militares Americanas, mesmo que o Pentágono fosse destruído de qualquer forma.

Quando do final da guerra fria, a Arphanet ficou sem função alguma, gerando assim nos militares um pensamento só, de que a mesma já não possuía mais importância alguma para poder ser mantida sob sua proteção. Sendo assim repassado o acesso aos cientistas que, logo em seguida a cederam para as universidades americanas, as quais sucessivamente, a passaram para universidades de outros países, consentindo que pesquisadores domésticos

---

[5] Abreviatura para Micro Instumetation and telemetry Systems
[6] GHz é a freqüência que corresponde a potencia de 10 elevado a 9 vezes 1Hz (um Hertz)

obtivessem acesso a mesma, até que mais de 5 milhões de pessoas já estavam conectadas com a rede e, para cada nascimento, mais 4 se conectavam com a enorme teia da comunicação mundial.

Com o surgimento da WWW - World Wide Web, esse meio foi locupletado. O conteúdo da rede ficou mais atraente e vasto, com possibilidades de se incorporar a mesma, imagens e sons. Um novo sistema de localização de arquivos criou um ambiente em que cada informação pudesse obter um endereço único, sendo encontrada por qualquer usuário da rede, surgindo assim os http – Hyper Text Transfer Protocol, ou protocolos de transferências de hiper textos.

Resumindo, a Internet é um conjunto de redes de computadores interligadas que possuem em comum um anexo de protocolos e serviços, de maneira que os usuários conectados usufruam de serviços de informação e comunicação de alcance mundial.

2.1.3 O advento da internet no Brasil

A história da Internet no Brasil começou só em 1991 com a Rede Nacional de Pesquisa, em uma operação acadêmica subordinada ao Ministério de Ciência e Tecnologia.

Em 1994, no dia 20 de dezembro é que a EMBRATEL lança o serviço experimental a fim de conhecer melhor a Internet.

Somente em 1995 é que foi possível, pela iniciativa do Ministério das Telecomunicações e Ministério da Ciência e Tecnologia, a abertura ao setor privado da Internet para exploração comercial da população brasileira.

A Rede Nacional de Pesquisa é a responsável pela infra-estrutura básica de interconexão e informação em nível nacional, tendo todo o controle sobre a mesma no Brasil.

2.2 O início dos crimes digitais

Com o firme avanço da tecnologia, foram surgindo novas modalidades de sociedade, dentre elas aquela que aprendeu a se habituar a constante atualização do processo de informatização do mundo, surgindo assim pessoas capazes de cometer ilícitos, estes denominados nessa esfera tanto como crimes de informática, crimes de computador, crimes

eletrônicos, crimes telemáticos, crimes informacionais, cyberdelitos, cybercrimes, etc. Não existindo um consenso para o sentido etiológico da palavra em si.

Dentre tais denominações, as mais utilizadas são as de crimes informáticos ou crimes de informática, sendo que as expressões crimes telemáticos ou cybercrimes são mais adequadas para identificar violações das redes de computadores ou a própria Internets.

Os crimes de Informática surgiram no final do século XX, devido ao avanço tecnológico, vindo assim a mostrar a fragilidade do sistema, que não foi prevista por seus criadores, sejam da rede, da internet ou do micro computador em si.

Para a OECD[7], o crime de informática é "qualquer comportamento ilegal, aético ou não autorizado envolvendo processamento automático de dados ou transmissão de dados", que envolvem várias categorias. A OECD vem desde 1983, ou seja, desde bem antes da difusão dos crimes de computador para a massa da sociedade, tentando uma maneira de controlar os referidos ilícitos.

No Brasil, esses ilícitos podem ser classificados como próprios ou impróprios. Serão próprios, aqueles praticados por computador e se totalizem em um ambiente digital, tendo como objeto jurídico a segurança dos sistemas e a titularidade de inviolabilidade desses referidos sistemas. Já os crimes denominados impróprios, são os que o agente utiliza de computador para produzir resultado externo a este, gerando afrontes ao espaço real da sociedade, gerando lesões diversas a outros bens diversos dos de informática.

O Advento da Informática e o avanço das tecnologias geraram impactos fortes nas ideologias societárias, inclusive no que tange para o norteador no Direito mundial. O surgimento dos crimes digitais era apenas uma relevante conseqüência do que esse avanço tecnológico poderia vir a oferecer, surgindo assim e sendo denominados inúmeros tipos de crimes de informática.

---

[7] Organization for Economic Cooperation and Development

3.0 CAPÍTULO II

3.1 O advento da ilicitude digital

3.1.1 Conceito de informática jurídica

Informática Jurídica é uma ciência que estuda o auxilio com que máquinas e elementos digitais propiciam ao desenvolvimento e rapidez nas questões jurídicas, constituindo de ajuda e fonte ao Direito propriamente dito, tendo como objeto principal o computador. Porém esse conceito é mais amplo, constituindo o conjunto de normas, aplicações, processos e relações jurídicas surgidas como efeito da aplicação e desenvolvimento da informática. È uma ciência geral, integrada por ciências especificas que derivam de ramos autônomos do próprio direito, como: Direito civil, direito penal, direito processual, direito trabalhista, direito empresarial, etc.

3.1.2 Conceito e definição de crimes de informática

Vive-se em uma época onde tudo se baseia na informação e para isso utiliza-se bastante sistemas digitais de alta tecnologia, ficando totalmente dependente a sociedade por parte desses mecanismos, ficando inevitável que sejam praticados atos ilícitos, pois os computadores hoje são verdadeiras máquinas de uso popular, onde os sistemas de segurança não conseguiram de forma alguma acompanhar o desenvolvimento tecnológico, mostrando assim a fragilidade que esse sistema possui. Esses ilícitos são os Crimes de Informática, frutos do avanço tecnológico e do uso popular do computador e da Internet.

Os crimes de Informática, por não estarem tipificados, não possuem conceituação legal, restando assim à conceituação doutrinaria. Carla Rodrigues Araújo de Castro, traz como sendo crime de Informática:

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

Esse conceito não é uniforme, para Guilherme Guimarães Feliciano o conceito de crimes digitais é que os mesmos são:

> "Ilícitos penais (delitos, crimes e contravenções) que têm por objeto material ou meio de execução o objeto tecnológico informático (hardware , software , redes etc.)".

Outro conceito que podemos destacar é o de Gustavo Testa Correa, para ele crimes digitais seriam:

> "Todos aqueles relacionados às informações arquivadas ou em trânsito por computadores, sendo esses dados, acessados ilicitamente, usados para ameaçar ou fraudar; para tal prática é indispensável à utilização de um meio eletrônico".

Os crimes de informática são configurados quando o agente pratica uma ação típica, antijurídica e culpável, contra ou por meios de utilização de processamentos automáticos, eletrônicos, digitais, de dados ou sua transferência, tendo como bem jurídico a ser protegido o sistema informático num todo, sendo o computador objeto ou instrumento dos crimes digitais.

3.1.3 Crimes digitais mais comuns

Os crimes digitais são aqueles de difícil elucidação, os mesmos podem afetar simultaneamente e instantaneamente milhares de pessoas em vários locais do mundo ao mesmo tempo sem que o criminoso sequer saia de sua residência. Existe uma grande variedade de crimes de informática, onde os mais comuns são: O estelionato em todas as suas formas, Violações à lei do Software, propagação de Vírus de computador em rede, Violações à propriedade intelectual ou industrial, Lesões a direitos humanos (terrorismo, racismo, etc.), pornografia infantil, Invasão de privacidade, lavagem de dinheiro, crime de "salami slicing"[8], pirataria em geral, trafico de armas e drogas, crimes de Hackers em todas as suas modalidades (Hackers, Crackers, Phrackers, Sniffers, Slammers,

[8] Tradução para o Inglês de fatiamento de salame, crime em que o ladrão faz regularmente transferências eletrônicas de pequenas quantias de milhares de contas para a sua própria, muitas vezes camuflada por campanhas de arrecadação de donativos de modo a não despertar suspeitas.

Spamers, etc.), jogos ilegais, crime de furto, destruição de informações, espionagem, sabotagem, dano, dentre outros.

3.1.4 Os crimes digitais no Brasil

Por serem crimes de difícil elucidação em diversos segmentos abordados, os crimes digitais requerem investigação policial especializada e efetiva, sendo que no Brasil existem preciosos policias que se adequam a essas características. Os poucos que existem estão designados para ocupar funções em seções onde se necessita de conhecimento em diversas áreas, estes adquiridos por própria iniciativa dos policias que não podem ficar esperando o descaso do Estado para com investimentos nesse setor.

A administração estatal apenas investe em qualificações ao como: preparação de agentes ao manuseio de dados eletrônicos e transmissão de dados, coleta de informações em banco de dados, operação de sistemas de computador, restringindo assim a atuação na área digital tão somente as necessidades internas de compilação e consulta instantânea, qualificando também os servidores para atuarem na elaboração de laudos policiais específicos característicos da área criminalística, visando obter evidencias fáticas em caos de apreensões de material digital.

As iniciativas de investimento na área publica nacional limita-se a treinamento de servidores para atuarem como digitadores, usuários de sistemas de dados, arquivistas, ou aptos a realizarem "autópsias eletrônicas", inexistindo assim um investimento claro para a proteção e segurança da sociedade quanto aos crimes digitais, não se percebendo alterações estruturais e específicas dos crimes desta área, mostrando dessa maneira a falta de visão, planejamento, treinamento e preparo no policiamento brasileiro.

3.1.5 O crime digital tentado

Para o direito penal brasileiro, crime tentado é o crime que iniciada a execução, não se consuma por vontade alheia a do agente, e se encontra tipificado no código penal brasileiro[9], em seu artigo 14, inciso II. Entendendo em um conceito mais técnico como o de Wessels, crime tentando é:

---

[9] Decreto-Lei de N°. 2.848 de 07 de dezembro de 1940.

> "A manifestação da resolução para o cometimento de um fato punível através de ações que se põem em relação direta com a realização do tipo legal, mas que não tenham conduzido a sua consumação" (*Direito Penal*: Parte geral, trad. Juarez Tavares, Porto Alegre, Sérgio A. Fabris, editor, 1976, p.133).

A modalidade de tentativa nos crimes digitais é aceitável, bastando que para isso, o agente possua interesse na pratica do ilícito e que o mesmo não se consume por vontade alheia deste. Pode-se tomar como exemplo o crime de "invasão", onde determinado individuo resolva vasculhar o computador de outrem afim de que possa com isso verificar sua pasta "meus documentos" e, depois de invadido, por vontade externa a do agente, este não consiga acesso à referida pasta, restando assim a tentativa do referido crime.

3.1.6 Os criminosos digitais

Os crimes digitais cometidos via internet são apegos à oportunidades, os criminosos em geral são ligados ocupacionalmente a área da informática. O perfil dos mesmos, baseados em pesquisas sem caráter científico, indica como sendo pessoas jovens, inteligentes, entre 15 e 32 anos de idade, do sexo masculino, educados, audazes, arrojados, desafiados pela amplitude do saber, além do anonimato que os privilegia, bloqueando assim os parâmetros de juízo para avaliar sua conduta como ilegal, alegando sempre não conhecimento do fato como ilícito e resultado de simples "brincadeira". Esse perfil mostra a dificuldade para a aplicação do flagrante e o colhimento de provas contra tal individuo.

3.1.6.1 Hackers

3.1.6.1.1 Conceito

No mundo digital como num todo, a denominação hacker é um termo respeitado, onde tal termo nasce do inglês "to hack", que significa fuçar. Esse termo foi iniciado pelos estudantes do Instituto de Tecnologia de Massachusetts, que utilizavam o termo "rato de laboratório" para designar aqueles que "fuçavam" os computadores da Universidade, alem do limite de uso. O hacker é um individuo muito sábio e devido a esse alto nível de saber é que o

mesmo possui condições de cometer ações de difícil execução. O hacker quer aprender cada vez mais, acabando normalmente a perder horas de suas noites para isso.

O hacker naturalmente é um "xereta" e adora invadir sistemas alheios para simplesmente satisfazer seu ego, as vezes corrompendo arquivos, subtraindo programas e roubando informações, colocando vírus em computadores, descobrindo senhas, sendo que estes denominados de Crackers, normalmente perigosos e que muitas vezes acabam por se auto destruir.

3.1.6.1.2 A origem dos hackers

Os hackers existem desde o final de década de 50, aparecendo apenas à terminologia como conotação negativa em 1988 por meio de uma reportagem da rede de TV CBS. A partir de então, tal terminologia ganhou cada vez mais conotação mundial como sendo os hackers criminosos digitais. Chamados por alguns de "piratas de computador", os hackers são temidos por uns e admirados por outros, devido aos estragos e a inteligência que só alguns deles possuem quando da invasão de um sistema computacional.

3.1.6.2 Hierarquias – grupos e subgrupos

3.1.6.2.1 Hacker

É aquele que possui grande facilidade de análise, assimilação, compreensão e capacidade de conseguir fazer o que achar melhor com um computador. Ele sabe muito bem que nenhum sistema é completamente livre de falhas, sabendo procurar por elas com o auxilio de técnicas das mais variadas. O hacker é uma pessoa que cada vez mais quer saber, conhece muito de computador e não fica tentando desconectar usuários da net. Ao invés disso o hacker utiliza sua capacidade para desenvolver novos programas. O termo hacker foi banalizado perante a rede como sendo sempre um criminoso da área da tecnologia, onde nem sempre isso acontece, sendo o hacker um verdadeiro conhecedor da informática e as vezes podendo utiliza-la de forma que contribua diretamente para o avanço da tecnologia perante o meio social.

3.1.6.2.2 Lamers

Utilizam programas disponíveis na internet e saem por aí tentando libertinar com os outros, geralmente sendo contra-atacados por hackers, que fazem o papel de inocentes, atacando assim o lamer que lhe ameaçara.

3.1.6.2.3 Cracker

Possuem tanto conhecimento quanto os hackers, não bastando para eles adentrar aos sistemas, quebrar senhas e descobrir falhas. Os crackers geralmente costumar deixar nos locais invadidos recados maldosos para informar que ali esteve, algumas vezes destruindo parte do sistema e até aniquilando com tudo o que vêem pela frente. São atribuídos aos crackers, programas que retiram travas de sistema, bem como os que alteram suas características, adicionando ou modificando opções , muitas vezes relacionadas à pirataria.

3.1.6.2.4 Phreacker

O phreacker é especializado em telefonia. Faz parte de suas principais atividades as ligações gratuitas tanto locais como em centrais de escutas colocadas em seu próprio telefone, tendo assim acesso as conversas de outros indivíduos. O conhecimento de um phreacker é essencial para se buscar informações que nas mãos de pessoas mal intencionadas seriam muito úteis. Permitem que possível ataques a um sistema tenha como ponto de partida provedores de acessos em outros países. Com o avanço da tecnologia, a atividade phreacker se atualizou, possuindo na atualidade como vitimas maiores os usuários de telefonia celular.

3.1.6.2.5 Cyberpunk

O movimento cyberpunk se propõe a explorar as possibilidades de um futuro não muito distante, onde o extremo desenvolvimento da ciência da informática possibilitará ao homem viajar pelo universo digital com a mesma facilidade como que caminha em uma

calçada. Tal movimento ainda é pouco conhecido no Brasil, apesar do substancial aumento do número de computadores vendidos por aqui.

3.1.6.3 Hackers famosos

3.1.6.3.1 Kevin Poulsen

O Hacker mais famoso do mundo é dos Estados Unidos. Atualmente se encontra preso, condenado por fraudes no sistema de telefonia, roubo de informações e invasão de sistemas. Os danos materiais são incalculáveis.

3.1.6.3.2 Kevin David Mitnick

É considerado o hacker mais famoso de todos os tempos, e assim como *Kevin Poulsen* também é americano. Invadiu muitas empresas, foi julgado duas vezes, consegui escapar do presídio e, desde 1995 está na casa de detenção de Los Angeles, onde aguarda pelo julgamento de seus crimes. Considerado o rei dos hackers, muitos sonham em conseguir a realização de seus feitos.

3.1.6.3.3 Mark Abene

Americano, inspirou toda uma geração a vasculhar os sistemas públicos de comunicação e telefonia. Sua popularidade chegou a tal ponto de ser considerado uma das 100 pessoas mais espertas de Nova York. Atualmente trabalha como consultor em segurança de sistemas.

3.1.6.3.4 John Draper

Praticamente um ídolo dos demais hackers, *Draper* também era Americano e foi o introdutor do conceito de phreacker, ao conseguir realizar ligações gratuitas, utilizando um apito de plástico que vinha de brinde em uma caixa de cereais. Obrigou todo os Estados Unidos a trocar a sinalização de controle nos seus sistemas de telefonia.

3.1.6.3.5 Johan Helsinglus

Finlandês, foi responsável por um dos maiores servidores de e-mail anônimo. Foi preso após se recusar a fornecer dados de um acesso que publicou documentos secretos de uma entidade de cientologia[10] na Internet. Conseguiu esse feito com um computador 486 com HD de 200Mb, nunca precisando usar seu próprio servidor.

3.1.6.3.6 Vladimir Levin

De naturalidade Russa, preso pela Interpol[11] após meses de investigação, nos quais conseguiu transferir 10 milhões de dólares de contas bancárias do Citibank[12] para sua própria conta.

3.1.6.3.7 Robert Morris

Outro Americano, espalhou acidentalmente um Worm[13] que infectou milhões de computadores fazendo boa parte da Internet parar em 1988, desenvolvendo assim um novo formato que se tornou constante na rede.

---

[10] A Cientologia é um sistema de crenças fundado em 1952 pelo autor de ficção cientifica L. Ron Hubbard (1911-1986 b. Tilden, Nebraska). A Cientologia foi oficializada em 1954. Esta religião baseia-se nos livros de Hubbard Dianética: A Moderna Ciencia da Saude Mental (1950), Dianética: A Evolução da Ciência e Ciência da Sobrevivência. Hubbard considerava a Dianética como uma subdisciplina da Cientologia. Até morrer, em 1986, Hubbard publicou centenas de livros sobre cientologia e apenas alguns sobre Dianética.

[11] Trata-se de uma central de informações para que as polícias de todo o mundo possam trabalhar integradas no combate ao crime internacional, o tráfico de drogas e os contrabandos.

[12] O Citibank é um banco Norte americano com sede em Nova Iorque que faz parte do Citigroup Inc é um dos maiores bancos do mundo. No Brasil tem sua sede em São Paulo na Av Paulista. Durante os anos 80 foi o maior credor privado da divida externa brasileira.

[13] Um Worm em computação é um programa auto-replicante, semelhante a um vírus. O vírus infecta um programa e necessita deste programa hospedeiro para se propagar, o worm é um programa completo e não precisa de outro programa para se propagar

4.0 CAPITULO III

4.1 A necessária influência estatal no combate aos crimes digitais

4.1.1 O Estado como meio de proteção da sociedade.

Paralelamente ao aumento da rede de informatização, se constata cada mais vez um crescente número de usuários fazendo mau uso deste novo meio de comunicação, fazendo com que a rede se torne um objeto muitas vezes perigosas. O número de invasões, acessos não-autorizados e destruição de dados de sistemas são alarmantes. A sociedade cada vez mais fica perplexa com tais acontecimentos.

Diante de tal situação, não poderia o Estado permanecer inerte, diversas empresas, particulares e órgãos públicos estão sendo lesionados moralmente e economicamente e, na grande maioria das vezes, o culpado não é responsabilizado pelo dano que causou, saindo totalmente impune e ileso das atrocidades cometidas. Não se pode deixar que um moderno e eficaz meio de comunicação, como o computador, seja mal utilizado, tornando-se um veículo de rápida desagregação da sociedade.

4.1.2 Garantia da tecnologia a serviço da cidadania

O Estado visa obter meios para que a tecnologia seja um meio usual de serviços que se relacione com a cidadania, vindo somente a servir a sociedade como num todo. Esses meios se formularão em torno da certeza de que a nova técnica procurada permitirá abolir distâncias, fronteiras e problemas de serviços de comunicação e para aqueles em que o acesso à comunicação é limitada, a mesma neutraliza e reforça as desigualdades, a exclusão e paralisa a limitação. Isso é o que dará consistência aos direitos do cidadão, deliberação e decisão, devendo ser questionado a saber, o lugar desse individuo dentro de tal conjunto institucional e procedimental denominado de cidadania, do qual o cidadão obtém sentido e consistência, figurando como ser maior.

A tecnologia transformada em espaço de cidadania, não será apenas elemento para formação de um fórum de discussão, essa certeza será apenas uma das fases com que esse

procedimento garanta a ciência como arte de benefícios, gerando lucros nos vários âmbitos imagináveis, em favor da própria sociedade.

4.1.3 Ampla oportunidade para realização dos crimes digitais

O avanço da tecnologia a e a facilidade de acesso a computadores por parte da sociedade, são fatores que auxiliam o contato direto de determinados indivíduos com a ampla oportunidade para realização de delitos na esfera digital. Os mesmo encontram-se acobertados pelo anonimato, o que lhes garante uma vantagem para cometimento de tais ilícitos.

O uso da internet é outro fator que evidencia essa referida oportunidade, pois o ambiente de cometimento do ilícito se torna incerto, causando assim mais dificuldade quanto da elucidação do mesmo.

Nota-se que o uso da internet e o volume do comércio eletrônico estão crescendo muito rapidamente, e esse crescimento tem sido desigual entre os países, onde os mais industrializados se dão ao luxo de dominarem previamente o uso do avanço da tecnologia. No Brasil estima-se que exista cerca de um quinto da população com acesso a internet e um terço com acesso a computadores. Esse grande volume de acesso à tecnologia gera não só um aumento dentre os usuários como também um aumento de vitimas e criminosos digitais.

4.1.4 Desafio quanto ao controle dos crimes digitais

Existe uma necessidade de se controlar vários fatores que idealizam o cometimento dos crimes de informática, dentre esses fatores podemos destacar a motivação dos criminosos, a oportunidade dos mesmos, a ausência de vigilância eficiente contra estes, a ausência de uma plataforma legal, a necessidade de barreiras extraterritoriais, etc.

4.1.4.1 Controlando fatores de motivação

Dentre os fatores de motivação dos criminosos digitais, podemos destacar a ganância, o desejo, a vingança e a curiosidade. Um dos leques necessários para o controle de tais crimes é justamente o controle de tais motivações. Alguns desses fatores são tão antigos quanto à sociedade humana, ficando assim o desafio intelectual de se controlar um sistema complexo.

Tanto do lado individual como no todo, sabe-se que é muito difícil se obter esse controle, carecendo que se obtenha investidas estrategicamente vantajosas que se preocupem com a redução de tais fatores. Tal controle exige que o Estado faça um melhor acompanhamento social dos indivíduos, por meio de uma política pública voltada a referido tema, com acompanhamento psicológico e divulgação em mídia para uma melhor conscientização da sociedade sobre os prejuízos que podem ser gerados quanto ao assunto focalizado.

4.1.4.2 Quanto ao controle da oportunidade

A quantidade e variedade de crimes digitais aumentam enquanto as motivações tendem a não se alterar. O crescimento na computação cria oportunidades para potenciais criminosos e paralelamente o surgimento de vitimas.

O modo mais eficiente para eliminar tal oportunidade é se arrancar o soquete do computador da parede, isto sendo muito improvável. O desafio das nações quanto ao uso das tecnologias é minimizar a revés que a mesma está ocasionando, restando assim soluções menos prováveis, mas aparentemente eficazes. Um comerciante por exemplo, pode analisar detalhadamente cada transação realizada em seu estabelecimento envolvendo cartões de crédito, reduzindo assim drasticamente os riscos de fraude, sacrificando de certa forma uma clientela honesta.

Existem atualmente tecnologias que reduzem as oportunidades de cometimento de crimes digitais, considerando que grande parte desses crimes depende de acesso não autorizado a sistema de informações. Assim, as tecnologias de controle de acesso e autenticação se tornaram essenciais, elaborando-se dispositivos sofisticados e produtos para prevenção desses referidos crimes como é o caso do Denning[14], elaborado pela empresa *segurança de computadores*, que é uma das industrias mundiais com maior crescimento nessa área. Além do Denning, outras tecnologias estão sendo desenvolvidas nesse setor. Já podemos contar com detectores de vírus que podem identificar e bloquear códigos maliciosos de computadores, programas de bloqueamento e filtragem que podem procurar e bloquear acesso a conteúdos indesejáveis e uma rica variedade de *softwares* comerciais que já operam com esta capacidade.

[14] Programa desenvolvido em 1999 que possui uma oferta de inventario completo das tecnologias para se reduzir as oportunidades dos crimes digitais.

4.1.4.3 O Controle da vigilância computacional

Outro fator básico que está diretamente relacionado à oportunidade de atuação dos criminosos digitais é a ausência de vigilância eficiente, que tem evoluído ao longo da historia da humanidade desde a época do feudalismo até a aparição do Estado e da proliferação das instituições estatais de controle social, até a época pós-moderna. A vigilância contra o crime convencional envolve esforços preventivos no campo das vitimas potenciais, contribuições da sociedade, do comércio em geral e das agencias de acossamento criminal.

A tecnologia pode induzir diretamente ao aumento da vigilância, o avanço dos alarmes permitem que os mesmos indiquem quando sucessivas tentativas de efetuar login[15] falham, devido a inserção de senhas incorretas ou quando essas tentativas são realizadas fora do horário normal de trabalho. Outros dispositivos podem detectar anormalidades que irão identificar padrões de uso dos sistemas, incluindo a destinação atípica e as durações das ligações telefônicas, ou ainda, padrões de consumo incomuns no uso dos cartões de crédito.

Com o surgimento dessas novas tecnologias, o policiamento do espaço territorial digital é agora empreitada, gerando responsabilidade pelo controle da criminalidade digital que será similarmente dividida entre os agentes do Estado, os especialistas em segurança de informação e o usuário individual desse sistema. A primeira linha de defesa será a autodefesa, onde basicamente cada um cuida do que é seu.

4.1.4.4 A ausência de uma plataforma legal

O espaço digital se caracteriza cada vez mais como meio dominante para o comércio, tornando-se imprescindivelmente relevante que exista uma plataforma legal segura para o comércio eletrônico, necessitando assim de uma base legal básica para que a jurisdição possa se proteger quanto aos crimes digitais. Tal base legal básica envolve leis criminais, direito de busca e apreensão e o direito das provas, sendo necessário uma uniformização tanto quanto possível das nações quanto a esse assunto, devido a natureza global do espaço digital. Isso é

[15] Efetuar Login é a ação necessária para acessar um sistema computacional restrito inserindo uma identificação, podendo esta ser ou não única para cada usuário, e a senha relacionada a ela. Uma vez logado, o usuário passa a ser identificado no sistema, sendo restringido ou permitido a acessar recursos do sistema.

necessário porque as leis de algumas nações são vagas e capazes de alcançar novas circunstancias sem necessitarem de emendas e outras muito rígidas, requerendo mudanças para novas formas de crimes. Isso implica que a lei criminal deverá conter:

- Acesso não autorizado aos computadores ou sistemas computacionais;
- Interferência com o uso ilícito de um computador ou sistemas computacionais;
- Destruição ou alteração de informação num sistema computacional;
- Furto de propriedade intangível;
- Obtenção de valores por fraude com a inclusão de sistemas eletrônicos.

4.1.5 A necessidade de barreiras extraterritoriais

A natureza global do ciberespaço aumenta significantemente a habilidade dos indivíduos em cometerem um crime em um determinado país que afetará diretamente indivíduos de outra nação, configurando grande desafio para detecção, investigação e persecução dos transgressores.

Dois problemas surgem nesse aspecto inter-jurisdicional: Primeiro a determinação do local onde ocorreu o crime, decidindo assim qual lei será aplicada. O segundo é a obtenção de provas e garantia de que o criminoso poderá ser localizado e levado a julgamento. Ambos levam problema de conflito de jurisdição e extradição.

Os crimes digitais de execução extraterritorial trazem consigo além de tempo para elucidação, gastos altos e incerteza para obtenção do culpado, e se bem executados os artifícios de extradição podem ser tão altos que excluem a atenção para todas as outras infrações, requerendo a conjunção de valores e prioridades que raramente ocorrem.

Alguns países estão declarando sua jurisdição para fora das fronteiras. Na Austrália, a lei de crimes digitais[16] depreca jurisdição nos casos em que a conduta constitui transgressão que ocorra parcialmente na Austrália ou a bordo de um navio ou aeronave australiana, onde o resultado dessa conduta constitua transgressão que ocorra parcialmente na Austrália ou a bordo de um navio ou aeronave australiana e quando a pessoa que cometa a transgressão é cidadã australiana ou uma empresa da Austrália.

---

[16] *Cybercrime Act* de 2001

Para efetivação desse sistema dentre todas as nações, temos de esperar um homogênismo do sistema mundial dos Estados soberanos, mesmo onde o poder de Estado existe com força total, mas a corrupção de alguns regimes pode impedir a colaboração internacional. Já a nível nacional deverão ser tomadas medidas que incluam a adoção de atitudes para criminalizar o acesso ilegal aos sistemas de computadores, a interceptação ilegal ou interferência em dados, a produção, venda ou aquisição de ferramentas de hackeamento, atividades relacionadas à pornografia infantil e contravenções relacionadas a violação de direitos autorais.

4.1.6 O relacionamento da lei em face dos crimes digitais

A lei é, e sempre será fundamental para a precaução e repreensão aos crimes, sejam estes em qualquer ambiente que se encontrem, material ou virtual. O filósofo Hans Kelsen afirma que:

> "(...) o direito é uma ordem normativa de conduta humana, ou seja, um sistema de normas que regulam o comportamento humano. Com o termo "norma" se quer significar que algo deve ser ou acontecer, especialmente que um homem se deve conduzir de determinada maneira. É este o sentido que possuem determinados atos humanos que intencionalmente se dirigem a conduta de outrem"[17]

A lei visa adequar à conduta humana, dentro de alguns princípios, possibilitando dessa forma a pacificação social. Por meio dela que o errado, imoral e as atividades destruidoras podem ser prevenidas e eliminadas, gerando um Estado onde os integrantes dessa sociedade possam conviver melhores. Se não houvesse a imposição desses limites, ficaria difícil assegurar que alguém não invadisse o espaço de outrem.

Nessa nova era, denominada aqui de "era digital" e com a conseqüente onde de surgimento de crimes, ora chamados de "crimes digitais", a garantia dos limites de cada um são importantíssimas.

O avanço da tecnologia cresce em uma rapidez tamanha, que se torna difícil, elementos jurídicos que venham combater de forma concisa as implicações advindas de tal crescimento. Esse avanço tecnológico demanda leis mais especificas quanto ao tema. A

[17] Hans Kelsen, *Teoria pura do direito*, p. 4

existência de leis já existentes pode auxiliar a esse combate, como no caso de se furtar um periférico computacional, então o indivíduo responderá pelo crime de furto, tipificado no Código Penal Brasileiro[18], art. 155. Outro meio seria a aplicação das leis já existentes sem alteração alguma, adicionando apenas novas normas, que abrangeria elementos da "era digital", atingindo assim de maneira mais eficaz seu objetivo.

Existem sim leis no Brasil e em outros paises que tentam coibir os crimes praticados pelo meio digital, porém surgirão crimes cada vez crimes menos óbvios, e as leis existentes não preencherão tais lacunas que eventualmente também virão a surgir.

De forma alguma isso seria suficiente para assegurar a sociedade uma existência de limites e garantia de direitos e deveres. A efetivação de leis mais especifica para o combate aos males que são oriundos do avanço tecnológico, o anonimato oferecido pela rede e a minimização da incidência de provas, se torna como algo inevitável, tendo que ser observados vários parâmetros para que não surjam leis vagas e esparsas.

4.1.7 A criação de Projetos de Lei que tende a regulamentar os crimes digitais no Brasil

Projetos de lei de muita importância para o Brasil tentam de varias formas regulamentar os crimes digitais. Dentre os quais, dois que apresentaram grande valor quanto ao assunto foram: O projeto de lei nº. 84/99, de autoria do deputado Luiz Piauhylino Monteiro, do estado de Pernambuco, e o projeto de lei nº. 1.713/96, de autoria do Deputado Cássio Cunha Lima, do estado da Paraíba, considerado o mais completo de todos.

O projeto de lei 84/99, encontra-se atualmente em proposição sujeita a apreciação do plenário no Congresso Nacional. O mesmo dispõe sobre os crimes cometidos na área de informática, suas penalidades e dá outras providências. Caracterizando como crime informático ou virtual os ataques praticados por hackers e crackers, em especial as alterações de home pages[19] e a utilização indevida de senhas.

O projeto de lei 1.713/96 também se encontra em proposição sujeita a apreciação do plenário, correndo conjuntamente entre a câmara dos deputados e o senado federal. Tal projeto dispõe sobre o acesso, a responsabilidade e os crimes cometidos nas redes integradas

---

[18] Decreto - lei nº. 2.848/40

[19] Home Page é a página inicial de um site (também chamado sítio). Compreende uma apresentação do site e de todo seu conteúdo.

de computadores e dá outras providências. Estabelecendo que somente por ordem judicial possa haver cruzamento de informações automatizadas com vistas à obtenção de dados sigilosos.

Tais projetos necessitam urgentemente de sua apreciação e efetiva aprovação para que a moralização quanto aos crimes de informática comecem a ser iniciadas no Brasil.

5.0 CAPÍTULO IV

5.1 Princípios do direito penal brasileiro em relação aos crimes de informática

5.1.1 A Hermenêutica Jurídica

A palavra hermenêutica provém do grego, *Hermeneúein, interpretar,* e deriva de *Hermes,* deus da mitologia grega, filho de Zeus e de Maia, considerado o intérprete da vontade divina. A Hermenêutica é teórica e estabelece princípios, critérios e métodos, orientação geral, já a interpretação é de caráter prático, aplicando os ensinamentos da hermenêutica. Tais conceitos não se confundem. Segundo a enciclopédia virtual Wikipédia[20], temos como sendo hermenêutica:

> "Hermenêutica é a ciência filosófica voltada para o meio de interpretação de um objeto. No caso do Direito, trata-se de técnica específica que visa compreender a aplicabilidade de um texto legal.Em palavras mais simples: quando uma lei entra em vigor, assim como toda e qualquer literatura, requer uma compreensão de seu conteúdo. Se não houvessem regras específicas para tal interpretação (e é disso que trata a hermenêutica jurídica), cada qual poderia (quer juízes, quer advogados) entender a lei da maneira que melhor lhe conviesse. Logo, a Hermenêutica traz para o mundo jurídico uma maior segurança no que diz respeito à aplicação da lei, e, ao mesmo tempo, assegura ao legislador uma antevisão de como será aplicado o texto legal, antes mesmo que entre em vigor."

No mesmo ditame e em conformidade ao autor Marcelo M. Ramalho Bittencourt, em seu artigo intitulado *a arte da interpretação jurídica*, interpretação seria:

> "Interpretação advém do latim Interpress, que em Roma, representava a figura do intérprete ou adivinho que lia o futuro das pessoas pelas entranhas da vítima (...). (...) De amplo alcance, a interpretação não se limita à Dogmática Jurídica: interpretar é o ato de explicar o sentido de alguma coisa, é revelar o significado de uma expressão verbal, artística ou constituída por um objeto, atitude ou gesto, em busca do verdadeiro sentido das coisas. Por isso o espírito humano lança mãos de diversos recursos, analisa os elementos, utiliza-se de conhecimentos de lógica, de psicologia e, muitas vezes, de conceitos técnicos, a fim de penetrar no âmago das coisas para identificar as mensagens contidas. Todo objeto cultural, sendo obra humana, está impregnado de significados, que impõem interpretação."

---

[20] Vide home page na internet, www.wikipedia.com

De tal maneira a hermenêutica jurídica é a forma mais objetiva de interpretação nas questões que envolvem o direito, não podendo deixar de fora o tem ora abordado, onde a necessidade de utilização de hermenêutica é de grande relevância aos ditames referenciais.

5.1.2 O Princípio da analogia para o Direito.

A analogia é um termo que desde logo, caracteriza a idéia de proporção, de semelhança e de correspondência. Para se aplicar uma norma especial a um caso especial, diferente daquela a que se foi aplicada, fundamenta-se no principio de que para haver identidade de razões, deve haver a mesma disposição.

No campo do Direito, a analogia pode ser definida como um processo lógico pelo qual o aplicador de uma referida lei a adapta a um caso concreto não previsto pelo legislador a uma norma jurídica que tenha o mesmo fundamento. Além disso, a analogia pode ser conceituada como sendo uma operação que consiste em aplicar a um caso não previsto, norma jurídica referente a um fato previsto, conquanto que entre os mesmo exista semelhança e a mesma razão jurídica para defini-los de igual maneira.

Para o povo romano, *"onde houver o mesmo fundamento haverá o mesmo direito"*[21] ou *"onde impera a mesma razão deve prevalecer a mesma decisão"*[22]. Estas expressões foram de grande valia para o surgir da analogia.

Em outros termos, a analogia jurídica consiste em aplicar, a um caso não previsto pelo legislador, a norma que rege o caso análogo, semelhante, por exemplo, a aplicação de dispositivo referente a empresa jornalística, uma firma consagrada quanto à edição de livros e revistas. A analogia não diz respeito a interpretação jurídica propriamente dita, mas a conexão da lei, pois, seu fim maior é suprir as lacunas existentes deixadas pela regra.

A analogia é uma técnica de integração do direito, preenchendo as lacunas da lei, e é necessária quando, o juiz, ao decidir uma lide não encontra a norma adequada à mesma. Se não havendo lacuna ou omissão da lei, o processo analógico é desnecessário e violador do direito. Aplicar a analogia quando existe norma especifica, é deixar de aplicar a lei. O Propósito da mesma é guardar a vitalidade do direito escrito, impedindo que as relações

---

[21] Expressão vinda do Latim *"Ubi eadem ratio ibi idem jus"*
[22] Também do Latim *"Ubi eadem legis ratio ibi eadem dispositio"*

sociais fiquem desamparadas pela lei. Por outro lado, a remissão feita por um artigo a outro que trará de dispositivos iguais ao primeiro não admite analogia.

A analogia, não deve ser confundida com os princípios gerais do direito, pois, ao se recorrer a mesma, existe norma expressa para um caso semelhante para o não previsto, ao passo que, para se recorrer aos princípios do direito é necessária a inexistência de norma expressa análoga. Encerrado o processo analógico, inexistindo norma do direito a ser aplicada, resta ao juiz apenas recorrer aos princípios gerais do direito.

Fato importante é que a analogia não se aplica no direito penal, a não ser a analogia *In bonam partem*[23], jamais agravando a pena. Segundo a lei penal a mesma não oferece lacunas, por não há crime sem lei anterior que o defina, sendo que toda conduta humana, para ser considerada criminosa, há de estar tipificada na lei penal, podendo haver interpretação ostensiva no direito penal, jamais analogia.

5.1.3 O princípio da legalidade

O princípio da legalidade é o que se encontra transcrito no inciso XXXIX, do artigo 5º da constituição federal e também se encontra no artigo 1º do código penal brasileiro. Tal princípio descreve: "não há crime sem lei anterior que o defina. Não há pena sem prévia cominação legal."[24], tal expressão é obtida do latim *Nullum crimen, nulla poena sine praevia lege* . O princípio da legalidade é sem duvida o mais importante para o direito penal, pois a partir do mesmo podemos tomar que, não se fala na existência de crime se não houver uma lei definindo-o como tal. A lei é a única fonte do Direito Penal quando se quer proibir ou impor condutas sob a iminência de sanção. Para o direito penal, tudo o que não for expressamente proibido, é licito.

Tomando o princípio da legalidade como aspecto político, observa-se que o mesmo apresenta sentido de garantia constitucional dos direitos do homem. Institui basicamente a liberdade civil, que ao contrario da penal, consiste em não fazer tudo o que ser quer, mas apenas aquilo que é permitido por lei.

Além do aspecto político, possui o princípio um aspecto jurídico, pois o mesmo fixa o conteúdo de normas incriminadoras, não permitindo que o ilícito penal seja estabelecido de

---

[23] Em favor do réu

[24] Redação do artigo 1° do decreto-lei 2.848, de 7 de dezembro de 1940. (código penal brasileiro)

forma genérica sem definição prévia da conduta punível e deliberações da *sanctio júris*[25] aplicável.

Com o advento da *teoria da tipicidade*, o princípio da legalidade ganhou muito de técnica. Típico é o fato que se amolda à conduta criminosa descrita pelo legislador, sendo necessário que o conjunto de elementos descritivos do crime contido na lei penal, aqui denominado de tipo, tenha sido definido antes da prática do delito. Diante de o exposto falar-se em anterioridade da lei penal incriminadora. De tal forma entende-se que, para que haja crime é preciso que o fato que o constitui seja cometido após a entrada em vigor da lei incriminadora que o define. Destarte, o mesmo estaria devidamente tipificado.

5.1.4 O principio da reserva legal e a anterioridade da lei

Uma grande parte dos doutrinadores considera como sendo sinônimo: princípio da legalidade e princípio da reserva legal. Heleno Cláudio Fragoso, nesse sentido, afirma em sua obra *Lições de direito penal; parte geral, 4. ed.., Rio de Janeiro, Forense, 1987, p.89*, o seguinte:

> "Essa regra básica denomina-se princípio da legalidade dos delitos e das penas ou princípio da reserva legal, e representa importante conquista da índole política, inscrita nas Constituições de todos os regimes democráticos e liberais."

A doutrina em sentido amplo orienta-se como não acontecendo diferença entre legalidade e reserva legal. Diferente desse ponto, Fernando Capez, em sua obra *Curso de direito penal; parte geral, 5. ed., São Paulo, Saraiva, 2003, p 38,* traz o referido:

> "(...) princípio da legalidade é gênero que compreende duas espécies: reserva legal e anterioridade da lei penal. Com efeito, o princípio da legalidade corresponde aos enunciados dos arts. 5º, XXXIX, da Constituição Federal e 1º do Código Penal ("não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal ") e contém, nele embutidos, dois princípios diferentes: o da reserva legal, reservando para o estrito campo da lei a existência do crime e sua correspondente pena (não há crime sem lei que o defina, nem pena sem cominação legal), e o da anterioridade, exigindo que a lei esteja em vigor no momento da prática da infração penal (lei *anterior e prévia* cominação)."

---

[25] Expressão em latim que significa sanção jurídica.

Em tal sentido, pode-se afirmar que a regra do artigo 1° do Código Penal, denominada outrora de Principio da legalidade, é apenas a fusão de dois outros princípios agora compreendidos: o da anterioridade e o da reserva legal.

Perante o princípio da reserva legal, somente a lei, em seu sentido mais estrito, pode deliberar crimes e atribuir penalidades, pois a matéria penal deve expressamente fazer obedecer a uma manifestação de vontade do poder estatal a que, por força da constituição, compete o poder de legislar.

O Princípio da anterioridade é uma garantia constitucional do direito individual do cidadão perante o poder punitivo do Estado. Ante tal princípio da lei penal, é necessário que a lei já esteja vigorando na data e que o fato for praticado, em observância ao princípio da reserva legal, a relação jurídica é determinada pela lei vigente à data do ocorrido. O princípio da anterioridade possui como um dos efeitos decorrentes a irretroatividade pela qual a lei penal é editada para o futuro e não para o passado.

A proibição da retroatividade não se restringe às penas, mas a qualquer sistema de natureza penal, mesmo que da parte geral do código penal. Toda e qualquer norma que venha a instituir, extinguir, aumentar ou diminuir a satisfação do direito de punir do Estado deve ser considerada de caráter penal. Nesse mesmo sentido, as normas de execução penal que tornem mais gravoso o cumprimento da pena, impeçam ou acrescentem elementos para a progressão de regime não podem retroagir gerando prejuízos ao condenado. A irretroatividade não atinge somente a pena, mas também as medidas de segurança.

Em resumo, o princípio da anterioridade estabelece que o delito e a pena respectiva serão considerados exclusivamente nos termos da lei vigente ao tempo da prática do crime. Para que uma ação ou omissão seja tida como crime, é preciso que a norma seja anterior ao fato. Por tal princípio, não há crime nem pena sem lei prévia.Tem como exceção as situações em que há favorecimento do réu: se lei posterior descaracterizar uma conduta criminosa como tal, ou cominar-lhe pena mais branda, esta será aplicada, e não a vigente ao tempo do fato.

5.1.5 A reserva legal como objeto de estudo no que se refere aos crimes de informática

Para uma melhor adequação dos crimes de informática as necessidades básicas enfrentadas pelo avanço da tecnologia, existe o imperativo de tal procedimento ter fundamentação legal perante o direito atual. Tal fundamentação terá obrigatoriamente que se basear em um dos princípios abarcados pelo direito penal.

A hermenêutica jurídica, não supre tal necessidade, pois obsta apenas de uma interpretação básica dos fatos, estabelecendo assim os princípios, conteúdos de critérios e metodologia a ser aplicada em tal interpretação.

Não princípio, mas meio de utilização para solução dos ditames na área jurídica é a questão da analogia, que muito menos que a hermenêutica, não de adequará de forma alguma ao caso supra mencionado. A analogia preenche as lacunas deixadas pela lei, adequando o caso não definido então como crime a algum semelhante. O direito penal não admite o fato de utilizar-se da analogia para o auxilio do mesmo, pois essa tese contrária o principio da legalidade, podendo apenas ser empregada em casos de beneficio de réu.

O principio a ser abordado em questão, será o da legalidade, contido no artigo 1° do código penal, afirmando que não há crime e nem pena sem lei prévia. Obstante a retirada do princípio da anterioridade (que afirma a necessidade de uma lei anterior para definir o crime e de uma prévia cominação legal para a aplicação da pena) contido em tal ditame, restará assim à reserva legal como meio de observação para solução prática dos delitos virtuais.

Tomando os princípios do direito penal atual como base, os condenados em tal circunstâncias não poderão ser apenados, pois, como o direito penal brasileiro não admite a analogia a não ser em favor do réu e toma como princípio de maior importância o da legalidade, em sua 1ª parte ora denominada de reserva legal, onde não existirá crime sem lei que o defina e muito menos pena sem sua imposição legal, torna-se como sendo lícitas as prática então delituosas no direito cibernético, conceituando-os como fatos atípicos para o direito penal.

A questão necessita então de uma legislação especifica para abordar o assunto, refletindo diretamente nas questões processuais a respeito do ditame. Tal legislação especifica é o que para o direito penal denomina-se tipificação ou tipicidade dos delitos.

5.1.6 Da tipicidade dos delitos

O tipo legal é um dos postulados básicos do princípio da reserva legal, à medida que a constituição federal e o direito penal brasileiro, por meio de seu código penal, adotam a questão de que não existe crime sem lei que o defina, nem pena sem sua cominação legal, fica concedida a lei a acentuada obrigação de descrever os crimes, definindo-os assim como tal. A lei penal não cabe a proibição dos delitos, senão descrevê-los de forma detalhada, demarcando precisamente o que o ordenamento jurídico entende por fato delituoso, o mencionando como crime. A tipicidade dos delitos tem uma função de garantia, impedindo que seja considerado crime o que não estiver descrito na lei. É também um indicío de antijuricidade[26], indicando que de início, a conduta descrita seja ilícita, salvo sua excludente que também está contida em lei.

5.1.7 A necessária adequação legal em concordância ao princípio da reserva legal

Na área do direito penal a necessidade de se adequar os delitos digitais em anuência ao princípio da reserva legal é enorme e exige rapidez acerca do assunto. Considerar determinada tarefa como delito é tarefa complicada e que requer alta responsabilidade.

O conceituado professor de Direito Penal, *Luiz Flávio Gomes*, proprietário do sitio de internet, *www.direitocriminal.com.br*, traz em seu site, um artigo que trata do seguinte:

> "Há muito reivindica-se no Brasil a criminalização específica dos crimes informáticos. Com o advento da Lei n. 9.983/00 (de 14.07.00), que entrou em vigor no dia 15.10.2000, surgiram no cenário jurídico-penal brasileiro algumas tipificações. (...) São tipificações, entretanto, muito específicas e que visam a

[26] Significa que o fato, para ser crime, além de típico, deve também ser ilícito, contrário ao Direito. Pode ser que exista uma causa que justifique o fato, embora típico, deixa de ser crime, por não ser antijurídico, como por exemplo, quando alguém pratica um fato típico, mas em estado de necessidade ou em legítima defesa. Dessa forma, a antijuridicidade é uma ação típica que não está justificada. Consiste na falta de autorização de mencionada ação típica.

> proteger primordialmente a previdência social e a administração pública. Não impede, portanto, a necessidade de uma lei penal mais geral."

Ainda no mesmo sentido, Luiz Flávio Gomes trata que:

> "A informática pode ser vista como um fator criminógeno na medida em que: a) abre novos horizontes ao delinqüente (que dela pode valer-se para cometer infindáveis delitos – é a instrumentalização da informática); b) permite não só o cometimento de novos delitos (p.ex.: utilização abusiva da informação armazenada em detrimento da privacidade, intimidade e imagem das vítimas) como a potencialização dos delitos tradicionais (estelionato, racismo, pedofilia, crimes contra a honra etc.); c) dá ensejo, de outro lado, não só aos delitos cometidos com o computador ("computer crime"), senão também os cometidos contra o computador (contra o "hardware", o "software" ou mesmo contra a própria informação); d) o crime informático pode ser cometido: (a) no momento da entrada dos dados ("input"); (b) na programação; (c) no processamento dos dados; (d) na saída dos dados ("output"); (e) na comunicação eletrônica; e) em todo o "iter criminis" pode ser utilizado o computador, é dizer, (a) no planejamento do crime; (b) na preparação do crime; (c) na sua execução; (d) e inclusive na fase posterior para seu encobrimento (destruição de provas); f) permite o desenvolvimento tanto de uma criminalidade privada (de particulares, pessoas físicas ou jurídicas) como pública (criminalidade estatal, que não só pode disseminar o uso da informática para controlar as pessoas, como também abusar das informações, tudo em flagrante violação aos direitos e garantias fundamentais típicas do Estado de Direito)."

Diante do fato expostos, vê-se que o delinqüente informático, cada vez mais se distancia do modelo padrão de Hacker, que geralmente é estudante, pertencente à classe média, especialista em informática, bom nível de inteligência, etc.

Atualmente tais delituosos são em geral, pessoas que trabalham no ramo da informática, não tão jovens nem inteligentes, vinculados a empresas, com característica central na pouca motivação em relação à norma e sua adequação para o crime, consiste na visão de lucro, perspectiva de promoção em seu emprego ou simplesmente para chamar a atenção. A vitima em geral conta com grande poder econômico e por isso mesmo quase nunca denuncia o delito contra ela cometido, tornando-se assim grande aliada do delinqüente. Para solução do foco abordado, é mister a adoção rápida e eficaz, legalmente falando, de novos tipos penais, para repressão a ações praticadas sob o aspecto informático e as novas realidades digitais,

para que as mesmas não se enquadrem em gêneros antijurídicos e atípicos, indo de contra ao principio da reserva legal.

6.0 CAPITULO V

6.1 O direito de informática como nova tendência jurídica no Brasil e no mundo

6.1.1 O princípio da territorialidade

A lei penal só tem aplicabilidade no território do Estado a qual foi editada, pouco importando para isso a nacionalidade do sujeito ativo[27] ou passivo[28] do delito. O princípio adotado pela legislação brasileira é o da territorialidade temperada, onde o ordenamento penal brasileiro é aplicável aos crimes cometidos no território nacional, de forma que ninguém, nacional, estrangeiro ou apátrida, residente ou em circulação pelo Brasil, poderá subtrair-se à lei penal brasileira por fatos criminosos aqui praticados, salvo quando normas de direito internacional dispuserem em sentido contrário. Sob o aspecto material, compreende como sendo território nacional, o espaço delimitado por fronteiras geográficas. Sob o aspecto jurídico, o território nacional, abrange todo o espaço em que o Estado exerce sua cidadania. Tal aspecto encontra-se na redação dada ao artigo 5° do código penal brasileiro, onde estabelece:

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

---

[27] Para o direito penal, sujeito ativo é o que pratica a conduta tipificada como crime, isolada ou conjuntamente com outros sujeitos.

[28] Passivo para o direito penal, é o sujeito ao qual é vitimado pela conduta tipificada como criminosa, isolada ou em conjunto com outros sujeitos.

6.1.2 O princípio da Extraterritorialidade

Consiste na aplicação da lei brasileira aos crimes cometidos fora do País. A jurisdição é territorial, na medida em que não pode ser exercida no território de outro Estado, a não ser por meio de regra permissiva, advinda do direito internacional costumeiro ou convencional. Respeitando o princípio da soberania[29], um país não pode impor regras jurisdicionais a outro, mas nada impede de um Estado exercer em seu próprio território, sua jurisdição, na hipótese de crime cometido no estrangeiro, salvo os casos em que exista preceito proibitivo explicito. O direito internacional concede ampla liberdade aos Estados para julgar, obedecendo a seus limites territoriais, qualquer crime, não importando o lugar onde tenha sido praticado, isso sempre que necessário, com o interesse de salvaguardar a ordem pública.

O princípio da extraterritorialidade, encontra-se elencado no código penal brasileiro em seu art. 7º, com a seguinte redação:

> "Art. 7º - Ficam sujeitos à lei brasileira, embora cometidos no estrangeiro:
> I - os crimes:
> a) contra a vida ou a liberdade do Presidente da República;
> b) contra o patrimônio ou a fé pública da União, do Distrito Federal, de Estado, de Território, de Município, de empresa pública, sociedade de economia mista, autarquia ou fundação instituída pelo Poder Público;
> c) contra a administração pública, por quem está a seu serviço;
> d) de genocídio, quando o agente for brasileiro ou domiciliado no Brasil;
> II - os crimes:
> a) que, por tratado ou convenção, o Brasil se obrigou a reprimir;
> b) praticados por brasileiro;
> c) praticados em aeronaves ou embarcações brasileiras, mercantes ou de propriedade privada, quando em território estrangeiro e aí não sejam julgados.
> § 1º - Nos casos do inciso I, o agente é punido segundo a lei brasileira, ainda que absolvido ou condenado no estrangeiro.
> § 2º - Nos casos do inciso II, a aplicação da lei brasileira depende do concurso das seguintes condições:
> a) entrar o agente no território nacional;
> b) ser o fato punível também no país em que foi praticado;
> c) estar o crime incluído entre aqueles pelos quais a lei brasileira autoriza a extradição;

---

[29] Entende-se por soberania a qualidade máxima de poder social através da qual as normas e decisões elaboradas pelo Estado prevalecem sobre as normas e decisões emanadas de grupos sociais intermediários. A soberania sobre uma nação é geralmente atributo de um governo ou de outra agência de controle política e se manifesta, principalmente, através da constituição de um sistema de normas jurídicas capaz de estabelecer as pautas fundamentais do comportamento humano.

> d) não ter sido o agente absolvido no estrangeiro ou não ter aí cumprido a pena;
> e) não ter sido o agente perdoado no estrangeiro ou, por outro motivo, não estar extinta a punibilidade, segundo a lei mais favorável.
> § 3° - A lei brasileira aplica-se também ao crime cometido por estrangeiro contra brasileiro fora do Brasil, se, reunidas as condições previstas no parágrafo anterior:
> a) não foi pedida ou foi negada a extradição;
> b) houve requisição do Ministro da Justiça."

6.1.3 Os princípios da territorialidade e da extraterritorialidade e os crimes digitais

Seguindo a lei penal propriamente dita, a mesma é elaborada para atuar limitada ao Estado que exerce sua soberania, surgindo assim a problemática de delimitação espacial do âmbito da eficácia da legislação penal, matéria do direito penal internacional.

No Brasil foi adotado pelo código penal o princípio da territorialidade, a partir de então fica a se pensar em como punir crimes cometidos em território brasileiro por meio digital como a internet. Esse é um grande ditame acerca da falta de legislação especifica para delitos que já estão sendo praticados e os que ainda virão a surgir pelo meio da informática.

Problemas como o lugar da infração e a lei a ser aplicada são questões que dificultam o ordenamento jurídico mundial, pois, ainda não existe nenhum tratado internacional que preveja a ocorrência dos delitos virtuais de extrapolação de limites fronteiriços de paises. Para se efetivar a aplicação do princípio da territorialidade nos crimes denominados a distancia, é necessário a exatidão do local onde foi cometida a infração.

O nosso direito penal adotou que a competência para julgar uma infração, será determinada pelo lugar onde foi consumada a infração, e nos casos de tentativa, no local onde fora praticado o ultimo ato executório.

Quando um brasileiro comete a pratica de crime através de provedor estrangeiro, onde a infração cometida será apreciada sem qualquer controle no Brasil, seria necessário a adequação dessa infração ao principio da extraterritorialidade para que tal sujeito seja julgado em concordância as leis brasileiras.

6.1.4 Crimes virtuais e o desrespeito à soberania dos países

Muitos paises, dentre eles o Brasil, perderam o controle e a repressão sobre crimes que ainda não se encontram tipificados em sua legislação, fazendo com que a informatização não

respeite qualquer fronteiras, não venerando assim a soberania dos países, que por vez, não conseguem aplicar suas leis em seu próprio território por conta de uma "imunidade virtual" que invade vários sistemas, expondo a muitas pessoas, sem limitação alguma, tudo o que sempre foi considerado como prática criminosa. Esse desrespeito fere e de forma acentuada a soberania dos países, tornando-os vulneráveis e objeto de brinquedo dos delituosos dessa área, fazendo com que a necessidade de aplicação da jurisdição se torne algo que exige rápida resolução.

6.1.5 Os níveis de jurisdição para os delitos virtuais

A doutrina acerca do assunto é pequena, mas clara, fazendo existir três níveis de jurisdição acerca do assunto.

O primeiro nível é o do espaço físico, onde as várias pessoas efetivamente residem e convivem, sempre governados por um único Estado-Nação. Dentro desse primeiro nível, as pessoas devem obedecer as leis do espaço onde elas estão fisicamente localizadas. Este seria um nível base de jurisdição para os delitos virtuais, que vincula a pessoa ao espaço físico que ocupa.

O segundo nível é o que se encontra os provedores de acesso, sendo este considerado o nível de jurisdição da internet. O provedor é o meio de conexão entre o mundo físico e o virtual, abrigando em seu centro um grande número de comunidades virtuais, tornando-se uma "nação virtual".

O terceiro nível é onde se encontra os domínios[30] e comunidades que excedem as fronteiras nacionais por meio dos provedores, e é nesse nível que se enquadra inúmeras comunidades virtuais que operam sem o mínimo de respeito pelas fronteiras internacionais ou de outros provedores.

Um outro nível pode se observado, sendo este denominado nível superior, pois é o nível onde se encontram as agências e outros órgãos de regulamentação acompanhados de organizações e indivíduos relacionados à internet, por onde quer que essas atividades se processem no espaço virtual. A jurisdição para esse nível está ligada diretamente as entidades que ela controla e não ao lugar físico em que se situam.

---

[30] Domínio é o endereço e a forma pela qual determinado sitio virtual se apresenta dentro da Rede, compondo de forma conceituada a Word Wide Web.

Este momento ao qual a dominação da informática se encontra em todo os âmbitos mundiais, é sem duvida um dos mais adequados para que novas normas internacionais ao assunto sejam adotadas, sejam leis ou tratados, contanto que tenham o sentido de prevenção da criminalidade. Tais normas viriam a impor limites ou ao menos meios de controle a essa criminalidade virtual, onde leis de âmbito internacional interferissem no abuso dos delitos e criassem meios de análise através de todo o sistema de informatização.

A criação de uma rede mundial interligada por computadores, em especial no que fere ao problema da territorialidade, ajudaria nas soluções ligadas ao tema, sem burlar dessa forma a soberania de qualquer dos países envolvidos, diante de que todos os países estariam diretamente submetidos às mesmas normas uniformemente, não reprimindo as nações menores aos interesses das mais poderosas.

6.1.6 Direito Internacional utilizado nos crimes digitais

A quebra de fronteiras territoriais é uma das características da era digital, por meio da internet. Na rede não existe um espaço geográfico delimitado, apenas o tempo da ação. Uma questão relevante sobre o assunto é o posicionamento do direito internacional público e privado frente às questões na internet. A partir do direito internacional, podem surgir fontes importantes para o esclarecimento dos crimes de informática, pois, ao Estado fica difícil o acompanhamento do ritmo das mudanças inerentes a informatização. Tais fontes servirão de instrumento hábil para manutenção da segurança jurídica, gerando assim um passo importante para a uniformização das relações mundiais essencial aos crimes digitais.

A tendência de uniformizar as questões internacionais existe e está ganhando espaço entre o meio jurídico. A União Européia já harmonizou a legislação de proteção à propriedade intelectual e telecomunicações. O Brasil já debate com a OEA – Organização dos Estados Americanos, a elaboração de um instrumento legal único de combate aos crimes eletrônicos.

6.1.7 O direito comparado na esfera de criminalidade virtual

O direito comparado é a área da ciência jurídica que estuda as diferenças e as semelhanças entre os ordenamentos jurídicos dos diferentes Estados do mundo, agrupando-os em família. Embora o direito comparado venha a auxiliar no estudo de diversos ramos do

direito, é no direito internacional privado que a disciplina do direito comparado exerce um papel fundamental: as instituições estrangeiras são estudadas por meio de comparação entre ordenamentos jurídicos.

O direito comparado, sem dúvida alguma, auxiliará nos trâmites e no desenrolar das lides envolvendo os crimes digitais, pois, em alguns países a tipificação desses crimes já se encontra totalmente definidas em lei e em outros essa tipificação vem acontecendo de forma parcial.

6.1.8 A jurisprudência brasileira quanto à matéria da criminalidade virtual

Atualmente no Brasil os tribunais apresentam decisões cada vez mais avançadas quando do surgimento de casos relativos a crimes virtuais. Orientando-se pela base legal que existe atualmente ao redor do mundo. Os magistrados, seja qual for sua área, não pode deixar de julgar, tendo que resolver a lide da maneira que melhor se adequar, não fugindo aos princípios do direito.

O direito penal possui uma função social de coibir as condutas lesivas, tendo como instrumento utilizado qualquer meio, mesmo que esse meio seja a informática. Enquanto não existe lei própria, aplica-se o direito filial, observando os respeitos aos ditames e princípios próprios estabelecidos na ciência jurídica criminal.

Abaixo segue alguns acórdãos a respeito do tema, podendo sendo denotado como bens jurídicos infringidos a concorrência desleal, a fraude e o estelionato e os crimes relacionados ao estatuto da criança e do adolescente.

> "PROCESSO PENAL – HABEAS CORPUS – PRISÃO PREVENTIVA – CONVENIÊNCIA DA INSTRUÇÃO CRIMINAL – GARANTIA DA ORDEM PÚBLICA – FRAUDES A INSTITUIÇÕES BANCÁRIAS E A SEUS CLIENTES – UTILIZAÇÃO DA REDE MUNDIAL DE COMPUTADORES – INTERNET – REQUISITOS DO ART. 312 – ATENDIDO – 1. Paciente em liberdade provisória. Ocorrência de novas fraudes contra instituições financeiras. Prisão Preventiva decretada. 2. Prisão Preventiva. Necessidade. Garantia da ordem pública. Conveniência da instrução criminal. 3. Ordem denegada. (TRF 1ª R. – HC 01000105586 – PA – 4ª T. – Rel. Des. Fed. Carlos Olavo – DJU 07.11.2002 – p. 90)."

"PROCESSUAL CIVIL – CIVIL – NOME DE DOMÍNIO NA INTERNET – REGISTRO – ATRIBUIÇÃO DA FAPESP – FUNDAÇÃO DE AMPARO À PESQUISA DO ESTADO DE SÃO PAULO, POR DELEGAÇÃO DO COMITÊ GESTOR INTERNET DO BRASIL – PRIMAZIA DO DIREITO DO PRIMEIRO REQUERENTE – INEXISTÊNCIA DE PRÁTICA DE CONCORRÊNCIA DESLEAL – SENTENÇA CONFIRMADA – I – O registro de nome de domínio ou concessão de endereço ip na rede internet é função atribuída à fapesp – Fundação de amparo à pesquisa do Estado de São Paulo, por delegação do comitê gestor internet do Brasil, órgão a quem incumbe coordenar e integrar todas as iniciativas de serviços internet no país, consoante os termos da portaria interministerial mct/mc nº 147/95. II – Dessa forma, diante da especificidade da matéria que encontra fundamento na Resolução nº 001, de 15.04.1998, do comitê gestor internet do Brasil, à Resolução da lide é indiferente as disposições da legislação que cuida da propriedade industrial e do registro público de empresas mercantis e atividades afins, respectivamente, Leis ns. 9.279/96 e 8.934/94. III – Assim, é de se conferir proteção judicial a quem primeiramente registrou o nome de domínio no referido órgão, que na hipótese foi a apelada. IV – Sem comprovação a alegação de prática de ilícito penal, qual seja, concorrência desleal, é de rigor a rejeição de tal pretensão. V – Recurso improvido. (TJDF – APC 20010110139208 – DF – 3ª T.Cív. – Rel. Des. Jeronymo de Souza – DJU 11.09.2002 – p. 52)"

"HABEAS CORPUS DELITOS PRATICADOS VIA INTERNET CARTÕES DE CRÉDITO CLONADOS – MATÉRIA DE PROVA IMPOSSÍVEL EXAME NOS ESTREITOS LIMITES DO WRIT – Se a verificação da ocorrência, ou não, do flagrante preparado, em face da prisão de agentes, a quem são imputados vários delitos, praticados pela internet, através de cartões de crédito clonados, depende do exame das provas colhidas na instrução criminal, isso não pode ser objeto de apreciação nos estreitos limites do Habeas Corpus. Ordem denegada. (TJRJ – HC 2542/2001 – 3ª C.Crim. – Rel. Des. Índio Brasileiro Rocha – J. 30.10.2001)"

"EMBARGOS DECLARATÓRIOS – APELAÇÃO CRIMINAL – PUBLICAÇÃO DA FICHA NA INTERNET – DIVERGÊNCIA COM O ACÓRDÃO PUBLICADO NO DJMT – ERRO MATERIAL – CORREÇÃO QUE PODE E JÁ FOI FEITA PELO PRÓPRIO SERVIDOR – CONTRADIÇÃO INEXISTENTE – RECURSO NÃO CONHECIDO – O resultado do julgamento, divulgado na Internet logo após a sessão, não é ato processual, e a divergência por acaso ocorrida com o que consta do acórdão publicado no DJMT, pode ser corrigida pelo próprio servidor que se equivocou, razão pela qual não devem ser conhecidos os embargos de declaração, propostos para esse fim, por ausência dos requisitos de admissibilidade. (TJMT – RED 3.746/00 – Paranatinga – 2ª C.Crim. – Rel. Des. Manoel Ornellas de Almeida – J. 10.10.2001)"

"CRIME DE COMPUTADOR – PUBLICAÇÃO DE CENA DE SEXO INFANTO-JUVENIL (E.C.A., ART. 241), MEDIANTE INSERÇÃO EM REDE BBS/INTERNET DE COMPUTADORES, ATRIBUÍDA A MENORES – TIPICIDADE – PROVA PERICIAL NECESSÁRIA À DEMONSTRAÇÃO DA AUTORIA – HC DEFERIDO EM PARTE – 1. O tipo cogitado – na modalidade de publicar cena de sexo explícito ou pornográfica envolvendo criança ou

> adolescente – ao contrário do que sucede por exemplo aos da Lei de Imprensa, no tocante ao processo da publicação incriminada é uma norma aberta: basta-lhe à realização do núcleo da ação punível a idoneidade técnica do veículo utilizado à difusão da imagem para número indeterminado de pessoas, que parece indiscutível na inserção de fotos obscenas em rede BBS/Internet de computador. 2. Não se trata no caso, pois, de colmatar lacuna da lei incriminadora por analogia: uma vez que se compreenda na decisão típica da conduta criminada, o meio técnico empregado para realizá-la pode até ser de invenção posterior à edição da lei penal: a invenção da pólvora não reclamou redefinição do homicídio para tornar explícito que nela se compreendia a morte dada a outrem mediante arma de fogo. 3. Se a solução da controvérsia de fato sobre a autoria da inserção incriminada pende de informações técnicas de telemática que ainda pairam acima do conhecimento do homem comum, impõe-se a realização de prova pericial. (STF – HC 76.689 – PB – 1ª T. – Rel. Min. Sepúlveda Pertence – DJU 06.11.1"

Tais jurisprudências se formam como meios elementares para o avanço do combate a criminalidade e a impunidade existente no Brasil no que tange aos crimes informáticos. Os tribunais cada vez mais estão buscando formas de combater tal criminalidade, e os magistrados buscando no direito alienígena[31] uma forma de "agilizar" o processo de especificidade dos delitos no Brasil.

[31] Forma de interpretação do direito de outros países sendo admitido como fonte do direito, em caso de não haver legislação especifica sobre um referido assunto.

7.0 CONSIDERAÇÕES FINAIS

Ao final de uma cuidadosa pesquisa, análise e compilação das informações e referências colhidas, em doutrinas, pesquisas na internet e revistas em âmbito geral, constatou-se a necessária adequação legal em concordância ao princípio da reserva legal por parte da criminalidade da informática.

Constatou-se uma mudança efetiva na adequação social relativo às novas tendências de tecnologia, o que essa referida tecnologia causou ao meio societário, a transformação do pensamento delitivo, e a necessidade legalização e tipificação dos delitos, que assim não acontecendo gerarão uma chaga nos princípios do direito.

O Estado por força de sua missão constitucional, fica obrigado a solução do ditame, tendo que demonstrar sua efetiva função de senhor absoluto, criando meios para que a sociedade fique de forma tranqüila, acabando com a inércia referente ao assunto de crimes de informática e fazendo com que os criminosos tomem por consciência de pensamento ante ao cometimento de qualquer dos delitos virtuais.

O ideal de conclusão e garantia de soberania nacional tem pelo Estado o dever de ser garantido, os criminosos não podem ficar impunes em referência aos crimes cometidos e também não se pode adequá-los a outros ilícitos em função da não-tipicidade e da não-legalidade dos delitos de informática, pois, isso acontecendo gerará omissão do Estado aos meios de condenação, suscitando meios para que prováveis recursos no tocante à matéria surjam, pois determinado individuo não pode ser condenado pela prática de evento que especificamente não é tido como uma conduta delitiva.

O Estado continua então com a árdua missão de se tipificar e legalizar tais delitos de forma rápida e prática, gerando assim certa estabilidade no tocante a matéria abordada. Uma necessária e urgente aprovação por meio do congresso de legislar quanto aos projetos de lei existente, será sem dúvida alguma um importante passo para solução dos delitos informáticos.

O Princípio da reserva legal, não pode continuar na mesmice de não ser observado, deixando assim uma enorme lacuna na lei e um amplo caminho para o aumento da ilicitude digital, onde cada vez mais criminosos estarão dispostos a criar novos tipos delitivos em conivência à impunidade gerada por meio da falta de leis especificas sobre o assunto.

Para um equilíbrio da fragilidade do sistema, não se pode deixar de continuar a sonhar com um futuro onde os delitos de informática possuirão legislação especifica de nivelação mundial e contará com punições aos criminosos dessa área, ficando garantida além da função

maior do principio da reserva legal pra o direito, as soberanias nacionais e a punição aos delinqüentes.

8.0 REFERÊNCIAS BIBLIOGRÁFICAS

CAPEZ, Fernando. **Direito Penal; Parte Geral, Vol. 1.** 5ª ed. São Paulo, Saraiva, 2003.

JESUS, Damásio E. de. **Direito Penal; Parte Geral, 1º Volume.** 26ª ed. São Paulo, Saraiva, 2003.

GRECO, Rogério. **Curso de Direito Penal; Parte Geral, Vol. 1.** 6ª ed. Rio de Janeiro, Impetus, 2006.

NADER, Paulo. **Introdução ao estudo do Direito.** 21ª ed. Rio de Janeiro, Forense, 2001.

SILVA, Flávio Ernesto Rodrigues; et al.; **Cadernos Adenauer IV, nº. 6 mundo virtual.** 1ª ed. Rio de Janeiro, Konrad Adenauer, 2004.

PAESANI, Liliana Minardi. **Direito de Informática: comercialização e desenvolvimento internacional do Software.** 4ª ed. São Paulo, Atlas, 2002.

COÊLHO, Fábio Ulhoa. **Curso de Direito Comercial, Vol. 3.** 6ª ed. São Paulo, Saraiva, 2000.

CORRÊA, Gustavo Testa. **Aspectos Jurídicos da Internet.** 2ª ed. São Paulo, Saraiva, 2001.

FÜHRER, Maximilianus Cláudio Américo; FÜHRER, Maximiliano Roberto Ernesto. **Resumo de Direito Penal , parte geral.** 20ª ed. São Paulo, Malheiros, 2002.

DOSSIÊ HACKER, PRIMEIRA PARTE. São Paulo, Escala, Ano um, nº. 1, 2000.

BRASIL, **Código Penal.** 10. ed., São Paulo, Rideel, 2004.

BRASIL, Constituição (1988). **Constituição da República Federativa do Brasil.** Brasília, Senado Federal, subsecretaria de edições técnicas, 2005.

ODISSÉIA DIGITAL - ESPECIAL. São Paulo, Abril, edição especial, 2001.

CASTRO, Carla Rodrigues Araújo de. **Crimes de informática e seus aspectos processuais.** Rio de Janeiro, Lumes Júris, 2001.

FELICIANO, Guilherme Guimarães. **Informática e Criminalidade**. Ribeirão Preto, Nacional de Direito, 2001.

FRAGOSO, Heleno Cláudio. **Lições de Direito Penal: Parte Geral.** 17ª ed. Rio de Janeiro, Forense, 2005.

MATA, Brenno Guimarães Alves da. Análise e tendências do cenário jurídico atual na Internet. **Jus Navigandi**, Teresina, ano 4, n. 46, out. 2000. Disponível em: <http://jus2.uol.com.br/doutrina/texto.asp?id=1771>. Acesso em: 12 set. 2006.

DJI, **Indice Fundamental de Direito – Analogia.** Disponível em: <http://www.dji.com.br/dicionario/analogia.htm>. Acesso em: 15 Out. 2006.

BITTENCOURT, Marcelo M. Ramalho. **A Interpretação no Direito.** Publicações UERJ, Faculdade de Direito, artigos, Jan. 2004. Rio de Janeiro. Disponível em: <http://www2.uerj.br/~direito/publicacoes/mais_artigos/a_interpretacao_tributario.html>. Acesso em: 22 Out. 2006.

WIKIPÉDIA, **Wikipédia a enciclopédia livre – História da computação.** Disponível em: <http://pt.wikipedia.org/wiki/Hist%C3%B3ria_da_computa%C3%A7%C3%A3o#Os_n.C3.BAmeros_e_o_.C3.A1baco>. Acesso em: 25 Out. 2006.

ARAS, Vladimir. **Crimes de informática. Uma nova criminalidade.** Jus Navigandi, Teresina, out. 2001. Disponível em: <http://jus2.uol.com.br/doutrina/texto.asp?id=2250> Acesso em: 01 nov. 2006.

PAIVA, Mário Antônio Lobato de. **Os institutos do direito informático.** Jus Navigandi, Teresina, Jul. 2002. Disponível em: <http://jus2.uol.com.br/doutrina/texto.asp?id=2571>. Acesso em: 06 nov. 2006.