UNIVERSIDADE PRESIDENTE ANTÔNIO CARLOS – UNIPAC FACULDADE DE CIÊNCIAS JURÍDICAS E SOCIAIS DE BARBACENA - FADI
CURSO DE GRADUAÇÃO EM DIREITO

PÂMELA ALINE ROCHA MOURA

CRIME CIBERNÉTICO E SEUS ASPECTOS NO UNIVERSO JURÍDICO

BARBACENA
2012

PÂMELA ALINE ROCHA MOURA

CRIME CIBERNÉTICO E SEUS ASPECTOS NO UNIVERSO JURÍDICO

Monografia apresentada ao Curso de Graduação em Direito da Universidade Presidente Antônio Carlos – UNIPAC, como requisito parcial para a obtenção de Bacharel em Direito.

Orientador: Prof. Esp. Colimar Dias Braga Júnior.

BARBACENA
2012

Pâmela Aline Rocha Moura

CRIME CIBERNÉTICO E SEUS ASPECTOS NO UNIVERSO JURÍDICO

Monografia apresentada ao Curso de Graduação em Direito da Universidade Presidente Antônio Carlos – UNIPAC, como requisito parcial para a obtenção de Bacharel em Direito.

Aprovada em ____/____/____

BANCA EXAMINADORA

Prof. Esp. Colimar Dias Braga Júnior
Universidade Presidente Antônio Carlos – UNIPAC

Profª. Esp. Maria José Gonzaga Goulart
Universidade Presidente Antônio Carlos – UNIPAC

Doutor Caio Lemos Rebouças
Advogado militante na área criminal – OAB/MG 128.896

Dedico aos meus pais e irmãos, pelas renúncias em nome da realização do meu sonho e por todo amor e carinho; ao Jonata, meu amor e melhor amigo; a todos meus amigos pelo apoio e pela paciência que tiveram comigo ao longo dessa caminhada.

AGRADECIMENTO

Agradeço, primeiramente, a Deus, por ter me concebido o dom da vida, sempre guiando meus passos e iluminando meu caminho, permitindo que eu chegasse até aqui.

Minha eterna gratidão à minha mãe, mulher de fibra, a mais bela dentre todas e amor da minha vida; sem ela não seria quem sou. Ao meu pai, homem responsável, que acreditou e lutou comigo para que pudesse, hoje, realizar meu sonho. Aos meus irmãos, Pablo e Rodrigo, pelo apoio incondicional. À minha avó Nadir, matriarca da Família Rocha e sinônimo de dedicação. Ao meu avô Manoel, meu poeta e maior exemplo de homem, de quem sentirei eterna saudade.

Àqueles que depositaram em mim sua confiança e me deram oportunidade de aprender, sobretudo ao Doutor Flávio Luiz Pinto de Vasconcellos, o primeiro mestre que tive na vida prática como operadora do Direito.

Aos meus amigos, que acompanharam de perto toda a trajetória; que vibraram com meus triunfos, me apoiaram e confiaram em mim, sem hesitar. Em especial ao Jonata, meu melhor amigo, confidente e parceiro; por toda sua paciência e dedicação, pelo carinho e amor, pela fidelidade e compreensão.

Aos docentes da Universidade Presidente Antônio Carlos, que muito me ensinaram, dentro e fora de sala de aula, deixando seu melhor em mim.

Agradeço ao professor Colimar Dias Braga Júnior, que prontamente aceitou o encargo de me orientar, também por sua dedicação e competência.

Ao Doutor Caio Lemos Rebouças, que em pouco tempo de amizade, tenho como exemplo; sua sede de conhecimento me inspira.

Em especial, à querida e grande mestre Maria José Gonzaga Goulart, por sua excelência, pelo profissionalismo e amor materno que tem comigo. Durante os três períodos em que ministrou suas excelentes aulas de Direito Processual Penal, fez com que eu me apaixonasse cada vez mais pelo Direito. Por ter sido mais que professora; foi conselheira, sempre de braços e coração abertos para me acolher, ensinar e ouvir. Para mim, a mestre é símbolo de humanidade! Sinto-me orgulhosa e honrada por ter sido sua aluna.

RESUMO

Modalidades delituosas evoluem celeremente em meio a coletividade. O progresso ocorre de forma tão rápida que o Direito não é capaz de acompanhar. Os crimes já existentes e compreendidos na esfera jurídica se aperfeiçoam, fazendo com que os usuários da rede mundial de computadores estejam expostos, com sua segurança comprometida. Toda a problemática social obriga a Ciência Jurídica ser ainda mais dinâmica, em resposta aos denominados crimes cibernéticos, através de meios preventivos e repressivos. Analisar inovações que as Lei 12.735/2012 e 12.737/2012 trouxeram para o ordenamento jurídico pátrio, bem como o panorama brasileiro e a escassez de normas específicas que tutelem o espaço digital são os principais objetivos deste trabalho. Contudo, antes de se aprofundar na matéria, breves explanações serão realizadas para que se obtenha uma melhor compreensão acerca do tema. Origem da internet e sua evolução, nomenclaturas, sujeitos ativo e passivo dos crimes, princípios da legalidade, anterioridade da lei e da territorialidade são alguns dos temas brevemente aclarados. A metodologia da pesquisa pretende ser bibliográfica. A bibliografia referente ao tema será pesquisada nos seguintes meios: livros, revistas científicas, revistas informativas, jornais impressos, sites da internet, artigos, periódicos, entre outros. Com a recente inserção de duas Leis ao Direito Brasileiro, fica demonstrada a preocupação do Estado em proteger o ambiente digital, adequando o Direito à nova realidade.

PALAVRAS-CHAVE: Direito digital. Direito penal. Crime cibernético. Internet. Projeto de Lei 84/1999.

ABSTRACT

Arrangements criminal evolve swiftly amid community. Progress occurs so quickly that the law is not able to keep up. The existing crimes and understood in the legal sphere is perfect, so that users of the World Wide Web are exposed with their safety compromised. Every social problem requires Juridical Science be even more dynamic in response to so-called cybercrimes through preventive and repressive. Analyze innovations that Law 12.735/2012 and 12.737/2012 brought to the legal parental rights, and the Brazilian landscape and lack of specific rules that protect the digital space are the main objectives of this work. However, before delving into the matter, brief explanations will be made to obtain a better understanding about the subject. Origin of the Internet and its evolution, classifications, active and passive subjects of crimes, principles of legality, prior law and territoriality are some of the topics briefly clarified. The research methodology is intended to be literature. The literature on the topic will be investigated in the following media: books, journals, news magazines, newspapers, websites, articles, periodicals, among others. With the recent inclusion of the two Acts Brazilian law, is demonstrated the concern of the State in protecting the digital environment, adapting the law to the new reality.

KEYWORDS: Digital Law. Criminal Law. Cybercrime. Internet. Bill 84/1999.

SUMÁRIO

1 INTRODUÇÃO 15

2 DO TELÉGRAFO À INTERNET 17

3 TERMINOLOGIAS E SUJEITOS DOS CRIMES CIBERNÉTICOS 21
3.1 Internet 21
3.2 Crime cibernético 21
3.3 Os criminosos (sujeito ativo) 22
3.3.1 *Hacker (White Hat)* 22
3.3.2 *Cracker* 23
3.3.3 Demais sujeitos 23
3.4 As vítimas (sujeito passivo) 24

4 PRINCÍPIOS NORTEADORES 25
4.1 Princípio da legalidade (reserva legal) 25
4.2 Princípio da anterioridade da lei penal 26
4.3 Princípio da territorialidade 26

5 LEGISLAÇÃO APLICÁVEL 29
5.1 Legislação internacional 29
5.2 Legislação brasileira 31

6 ATUAL PANORAMA NO BRASIL 35

7 CONSIDERAÇÕES FINAIS 37

REFERÊNCIAS 39

1 INTRODUÇÃO

Existente há mais de vinte anos, a internet foi criada no ápice da Guerra Fria, durante a década de sessenta, a partir de um projeto militar norte-americano do Departamento de Defesa dos Estados Unidos.

Com o passar dos anos, o incremento e aperfeiçoamento deste novo veículo de comunicação, cumulados com a popularização mundial de tecnologias avançadas, propiciaram o surgimento de novas práticas ilícitas, tais como a invasão de computadores, roubo de identidade e fraudes no comércio eletrônico, assédio e molestamento por meio de comunidades virtuais, além de impulsionar a prática de crimes já existentes no âmbito físico, como o tráfico de drogas, órgãos e armas e, ainda, a biopirataria.

O delito cometido por meio da rede mundial, com o auxílio de computador, é denominado crime cibernético. De uma forma ampla, o Departamento de Justiça dos Estados Unidos define o crime cibernético como “quaisquer violações de leis criminais que envolvam, para sua perpetração, investigação ou persecução, o conhecimento de tecnologia de computador”. Assim, tal como a criminalidade habitual, pode ocorrer em diversos locais, a qualquer momento. Os criminosos utilizam-se de suas aptidões e conhecimentos específicos, desenvolvendo os mais variados métodos, para alcançarem seus objetivos, englobando uma gama muito ampla de ataques.

Pesquisas realizadas demonstram que inúmeras são as vítimas, já ultrapassando milhões, e elevados são os custos dos cibercrimes, com perdas financeiras contabilizadas em bilhões. O combate a esses crimes gera despesas altíssimas, além de ser uma questão cultural.

Na esfera jurídica, devido ao fato de ser ainda recente o tema, escassa é a legislação específica para coibir essa modalidade criminal. Necessário, portanto, enquadrar esses delitos nos tipos penais já previstos pelo Código Penal Brasileiro.

O político mineiro e atualmente Deputado Federal, Eduardo Azeredo, na época Senador, criou Projeto de Lei Sobre Crimes de Informática (PL 84/99), também conhecido como “Lei Azeredo”, que após processo tramitatório superior a uma década, converteu-se na Lei Ordinária Nº 12.735. O referido projeto, desde o início, provocou discussão e várias polêmicas, dividindo opiniões e sendo, constantemente, alvo de críticas.

Mesmo havendo divergência nos campos jurídico, científico e social quanto a criminalidade cibernética e uma lei especial regente, possível é dizer que, sendo crescente a prática dos delitos, torna-se necessária sua repressão, através da parceria de autoridades, especialistas da área da computação e operadores do Direito com a sociedade que, por sua vez, deve denunciar tais crimes e fiscalizar se os mesmos estão efetivamente sendo investigados, buscando-se com isso, uma conscientização dos usuários da rede de computadores. A criminalidade cibernética é extensa e as novas tecnologias, que surgem a cada instante, desafiam os conhecimentos acumulados.

O ordenamento jurídico brasileiro, embora tenha inserido recentemente duas novas leis específicas para tratar desses ilícitos, é iniciante na seara do Direito Digital; os operadores ainda não estão completamente aptos para enfrentar a nova realidade. Ressalte-se que as dificuldades de identificação e controle de usuários, as controvérsias e discussões sobre a produção de provas baseadas em fontes cibernéticas, dentre tantos outros, são fatores que estabelecem amplas barreiras no combate a esses crimes. Assim, com finalidade de que haja efetiva aplicação da norma faz-se necessário estudo meticuloso do texto legal regimentar, bem como aquisição de conhecimentos de informática pelos profissionais da área, vez que as informações disseminadas pela internet fluem num tempo muito mais célere do que a lei pelos órgãos envolvidos nesse combate.

Múltiplos questionamentos existem no tocante as infrações cometidas em âmbito virtual. O que é crime cibernético; quais suas modalidades e, dentre elas, as mais praticadas; qual o perfil das vítimas desses crimes e os métodos preventivos aplicáveis são apenas alguns que caracterizam os mais recorrentes.

Uma resposta plausível em meio a tantas incógnitas consiste na investigação dos avanços e impactos dessa nova modalidade ilícita, considerada transnacional, em busca da consolidação da lei especial, bem como na capacitação dos operadores do Direito e conscientização da população. Dessa forma, haverá redução no índice de criminalidade, bem como consequente melhoria na segurança social.

2 DO TELÉGRAFO À INTERNET

Segundo Ethevaldo Siqueira (2007, p.274) a rede mundial de computadores, comumente conhecida por internet, apresenta como origem remota o século XIX, quando do ano de 1844 fora criado o telégrafo elétrico, que interligou duas máquinas transmissoras de mensagens codificadas com alfabeto Morse, em uma linguagem binária, composta por pontos e traços. Já no ano de 1876, com a criação do telefone, eis que surge o meio de comunicação por voz. Assim, estreia-se o século XX com duas redes de comunicação.

Já o computador, um dos símbolos do fenômeno "globalização" e grande protagonista da era digital, foi introduzido à história no ano de 1944, quando concluído projeto *Mark I*, iniciado no ano de 1937, da Universidade de Harvard e a *International Business Machines* (IBM) - empresa responsável pela disseminação da informática. Por ter sido a primeira máquina desse seguimento a ser finalizada, foi de suma importância no cenário da Guerra Fria, sendo utilizado pela Marinha Americana.

Ainda baseado nos estudos de Ethevaldo Siqueira (2007, p. 131), constata-se que pouco depois, no ano de 1946, foi exibido o primeiro computador eletrônico pela Universidade da Pensilvânia, alcunhado *Eniac*, projetado e construído a fim de contribuir nos estudos e planejamentos pertencentes também à Marinha Americana. Neste período, encontrando-se frente a frente Estados Unidos e a extinta União das Repúblicas Socialistas Soviéticas (URSS), quaisquer progressos tecnológicos contribuiriam no exercício da forte influência por parte desta ou daquela perante as demais nações.

Os Estados Unidos se posicionaram em resposta ao avanço da URSS (lançamento do primeiro satélite artificial, *Sputnik I*, em 04 de outubro de 1957). Iniciava-se, então, em outubro do mesmo ano, um projeto militar cujo objetivo precípuo era constituir uma rede de computadores, interligando-se centros de pesquisas que estivessem distantes um do outro e fossem imunes aos bombardeios. Assim, acaso a comunicação direta fosse interrompida, seria uma alternativa de difusão de informações confidenciais utilizada entre computadores das universidades e do exército.

Ao final da década de 1960, acrescenta Michael L. Dertouzos (1998, p.62), a *Advanced Research Projects Agency* (ARPA) é criada pelo Departamento de Defesa norte-americano, com intento de reforçar a segurança nacional. Após múltiplos investimentos e

diversos estudos surgiu, no âmbito de pesquisas da ARPA, a rede denominada ARPANET, baseada em dois fatores: o primeiro, de cunho exclusivamente militar, visando a proteção e manutenção dos bancos de dados, informações e estratégias em caso de conflito nuclear; o segundo, de caráter econômico, que estimulou a expansão do até então projeto. Os grupos financiados pela Agência exigiam mais aprimoramento e maior quantidade dos computadores.

Atentos à inconveniência da existência de um único computador central, foram elaborados mecanismos que propiciavam a transmissão de informações através de rotas que atingiriam pontos específicos, denominados "chaveamento de pacotes". A ARPA estimulou a divisão dos computadores distantes entre si nos grupos de pesquisa. Na hipótese de um dos pontos não estar conectado, as informações recuariam e seguiriam caminho por meio de outro ponto, atingindo, assim, seu objetivo.

Com os primeiros pontos instalados, foram realizadas demonstrações através de envio de mensagens simples, bem sucedido. Em 1º de setembro de 1969, as Universidades da Califórnia e de Utah interligaram-se ao *Stanford Research Institute*, por meio da primeira rede de computadores, a ARPANET.

De início, ensina Manuel Castells (1999, p.83), a rede esteve aberta aos centros de pesquisa para que estes colaborassem com o Departamento de Defesa norte-americano; aos poucos, os cientistas passaram a utilizá-la para comunicação própria, fossem os conteúdos científicos ou pessoais. Devido à dificuldade de controlar a transmissão de mensagens e separá-las, a ARPANET se dividiu em 1983, dedicando-se aos estudos científicos, enquanto a MILNET orientava as pesquisas militares.

Gradativamente estudos foram realizados e novas tecnologias surgiram, proporcionando o aperfeiçoamento dos computadores e da internet, o que, ao final, resultou na difusão e, consequentemente, na liberação do uso em caráter comercial nos Estados Unidos, dado pela primeira vez em 1987.

Conforme instrui Manuel Castells (1999, p.87), em 1990, a *World Wide Web* (www) começa a ser desenvolvida por Tim Berners-Lee, que trabalhava no Centro Europeu de Pesquisas Nucleares, em Genebra. A capacidade de transmissão de imagens ainda era muito limitada e havia dificuldade em localizar e receber informações. Enquanto isso, no Brasil, é criada a Rede Nacional de Pesquisas.

Embora os primeiros traços de rede tenham surgido em 1988, interligando universidades do Brasil às instituições norte-americanas, a internet foi inserida comercialmente no país apenas no ano de 1995, por meio da Norma nº 004 do Ministério das Comunicações, que gere a utilização dos meios da rede pública de telecomunicações para o provimento e utilização de serviços de conexão à Internet.

A partir de 1997 surgiram inovações no campo da ciência e tecnologia que propiciaram avanço e aperfeiçoamento gradativo das redes no Brasil, com o fornecimento de infraestrutura e manutenção das redes. Destarte, depois de vinte anos, aproximadamente, o número de usuários brasileiros chega ultrapassar a marca de um milhão, em todas as regiões do país. Todavia, a penetração da internet no país ainda é muito baixa.

3 TERMINOLOGIAS E SUJEITOS DOS CRIMES CIBERNÉTICOS

Tal qual a sociedade, a tecnologia modifica-se, passando por processos evolutivos. Porém, este processo se dá de forma tão célere que o Direito, ciência regente da sociedade, não é capaz de acompanha-lo. Assim, os crimes já existentes e compreendidos na esfera jurídica se aperfeiçoam e outras modalidades delituosas surgem.

Com o advento do computador e o fenômeno da globalização, a acessibilidade das pessoas à internet alargou-se proporcionalmente à velocidade de aperfeiçoamento da tecnologia. Embora o Direito já disponibilize instrumentos mais atualizados, o combate aos delitos cometidos no âmbito virtual ainda é retrógrado, tornando o cenário muito mais atrativo para os infratores.

Devido à dificuldade em administrar o mundo digital cumulada com lacunas existentes na legislação nacional, os usuários da rede mundial de computadores estão expostos, com sua segurança comprometida.

Assim como ocorre nas demais relações encontradas na seara criminal, no tocante aos crimes cibernéticos há duas espécies de sujeitos, o meio onde o delito é perpetrado e conceituações pertinentes; pontos vitais para a capitulação deste crime, que devem ser conceituados para melhor compreensão da matéria.

3.1 Internet

Para Fabrízio Rosa (2006, p. 35) “a internet consiste num conjunto de tecnologias para acesso, distribuição e disseminação de informação em redes de computadores”.

Numa definição mais popularizada, a internet trata de sistema de rede e computadores ininterruptamente conectados entre si a nível mundial, pela qual são realizados transmissões e compartilhamentos de mensagens, imagens e sons.

3.2 Crime cibernético

De maneira ampla, o Departamento de Justiça dos Estados Unidos define o crime cibernético como sendo quaisquer violações de leis criminais que envolvam, para sua perpetração, investigação ou persecução, o conhecimento de tecnologia de computador.

A Symantec, empresa especializada em segurança de computadores, proteção de dados e software de gerenciamento remoto, conhecida graças ao antivírus “Norton”, baseada em diversas definições de crime cibernético, o define como qualquer delito em que tenha sido utilizado um computador, uma rede ou um dispositivo de hardware.

Portanto, independente do tipo de afronta às leis, se feitas por meio de computador, está caracterizado o crime cibernético.

3.3 Os criminosos (sujeito ativo)

Segundo Sandra Gouvêa (1997, p.60), pode-se afirmar que, a princípio, mais precisamente na década de 1970, os agentes cometedores dos delitos cibernéticos eram programadores, vez que detinham o vasto conhecimento técnico necessário à época para manusear os computadores, caracterizados por serem de uso dificultoso.

Com a abertura do mercado e a facilidade de acesso às máquinas, a disseminação dos crimes foi questão de tempo.

As primeiras fraudes bancárias foram detectadas na década de 1980. Os funcionários de bancos possuem acesso a dados relativos à movimentação de inúmeras contas correntes, aplicações, dentre outras operações características.

Pesquisas do Centro Nacional de Dados sobre Crimes por Computador, nos Estados Unidos, demonstram que funcionários e ex-funcionários são maioria na prática de delitos cibernéticos, atacando seus próprios empregadores, correspondendo, assim, a 75% dos agentes criminosos.

Outras vezes, os mesmos delitos são praticados por jovens amadores, entre 18 e 30 anos, que se glorificam por suas atividades.

Atualmente, devido à massificação dos computadores e da internet, quaisquer pessoas podem praticar delitos no âmbito digital.

3.3.1 *Hacker (White Hat)*

Com fulcro na obra de Henrique Cesar Ulbrich e James Della Valle (2004, p.29) o termo popularizou-se na década de 1960, como sinônimo de programador e especialista em

computadores, entretanto, era comum utilizá-lo para definir qualquer especialista, em diferentes áreas: mecânica, astronomia ou mesmo engenharia.

Devido à pejoratividade prestada pelos jornalistas à comunidade *hacker*, o vocábulo é utilizado presentemente com a finalidade de referir-se aos criminosos cibernéticos. Entende-se, portanto, ser especialista que domina variadas técnicas de invasão, sendo dotado de profundo conhecimento de ao menos um sistema operacional. Excepcional programador e administrador de sistemas. Todavia, contrariamente ao que a população acredita, possui rígido código de ética e não se utiliza de seus conhecimentos para práticas criminosas.

A comunidade *hacker* tradicional ojeriza por completo tal definição. Para eles, aqueles que praticam atividades ilegais por meio da internet são denominados *crackers*.

3.3.2 *Cracker*

Também denominado "*hacker* do mal" ou "*hacker* sem ética", Henrique Cesar Ulbrich e James Della Valle (2004, p.30) afirmam que esse indivíduo é, normalmente, especializado em quebrar traves de *softwares* comerciais a fim de pirateá-los. Usa seus conhecimentos, ainda, para invadir computadores e sites com propósitos ilícitos.

Muitas vezes é excelente programador e pode criar programas que infectem ou destruam por completo sistemas alheios sem deixar vestígios. Notório conhecedor, faz uso de ferramentas que explorem vulnerabilidades nos sistemas que pretendam invadir, tendo noções suficientes para improvisar acaso ocorra algum imprevisto.

3.3.3 Demais sujeitos

Wannabe (wannabee) – é o usuário comum de internet que almeja ser *hacker*. O termo pode ser utilizado de forma positiva, quando se refere ao indivíduo que estudou por considerável período e está prestes a ingressar em um nível intermediário, antecessor ao de programador. Este é o ensinamento de Henrique Cesar Ulbrich e James Della Valle (2004, p.29).

Na forma pejorativa, trata-se daquele que deseja entrar no âmbito *hacker*, contudo, não possui mínima noção do que deve ser feito.

Phreaker – este é o *hacker* de sistemas telefônicos; detentor de conhecimentos avançados de eletrônica e telefonia, podendo fazer chamadas de qualquer local sem, contudo, pagar por elas. Conceituação dada por Henrique Cesar Ulbrich e James Della Valle (2004, p.30).

Carder – assim é denominado o especialista em fraudes com cartões de crédito. Consegue obter listas de cartões válidos em sites que os utilizam, gerando numeração falsa que é reconhecida pela verificação, roubando e clonando cartões verdadeiros. Assim ensinam Henrique Cesar Ulbrich e James Della Valle (2004, p.30).

War driver – este tipo é recente em relação aos demais. Utiliza-se das inúmeras vulnerabilidades das redes sem fio, conectando-se a elas. Denominação lecionada por Henrique Cesar Ulbrich e James Della Valle (2004, p.30).

3.4 As vítimas (sujeito passivo)

Pesquisas sobre vítimas de crimes cibernéticos são unânimes na afirmação de que estatísticas não são confiáveis.

Na maioria dos casos a vítima sequer sabe que está sendo atingida pelos agentes. Quando descobrem – observe-se que há uma parcela que continua sem perceber que os crimes estão ocorrendo – preferem calar-se, arcando com os prejuízos sofridos, a estampar páginas de jornais e revistas, admitindo sua vulnerabilidade e perdendo credibilidade, como nos casos de grandes empresários e bancos.

Os principais alvos dos criminosos são instituições financeiras e empresas de telefonia. Sabe-se, no entanto, que não se pode restringir a tutela para determinados agentes.

Assim como quaisquer pessoas podem praticar delitos no ambiente cibernético, qualquer indivíduo usuário da rede de computadores poderá ser vítima.

4 PRINCÍPIOS NORTEADORES

Um dos maiores desafios atuais do Direito é a tutela do ciberespaço. A internet, por ser detentora de caráter global, possibilita a prática de crime em específico local sem que o agente ali se faça presente. Destarte, necessário conhecer acerca dos princípios pertinentes à matéria no âmbito penal, fonte das leis regulamentadoras pertinentes ao tema.

Os princípios da legalidade e da anterioridade da lei penal estão insculpidos no ordenamento jurídico brasileiro através Constituição Da República de 1988, em seu art. 5º, XXXIX, bem como pelo Código Penal, no art.1º. Quanto ao princípio da territorialidade, este encontra previsão no Código Penal, no art.5º.

Trata-se, portanto, de princípios basilares coligados aos textos legais, sendo garantidores da liberdade e segurança dos indivíduos, bem como da norma penal. Logo, são elencados como garantias fundamentais arroladas pela Carta Magna, assegurando à coletividade proteção "contra toda e qualquer invasão arbitrária do Estado em seu direito de liberdade", como ensina Fernando Capez (2005, p.40).

4.1 Princípio da legalidade (reserva legal)

O princípio da reserva legal determina que somente a lei em sentido estrito, nos moldes traçados pela Constituição Pátria, instituída a partir de processo legislativo, pode estatuir o que é crime, estabelecer seus elementos e especificar a pena cabível para sua prática.

A *Magna Charta Libertatum Britânica* de 1215, traz em seu art.39:

> Nenhum homem livre será detido, nem preso, nem despojado de sua propriedade, de suas liberdades ou livres usos, nem posto fora da lei, nem exilado, nem perturbado de maneira alguma; e não poderemos, nem faremos por a mão sobre ele, a não ser em virtude de um juízo legal de seus pares e segundo as leis do país. (GRECO, 2005, p.104)

Por consequência de tal exclusividade da lei na disciplina penal, os demais textos legais (decretos, medidas provisórias, dentre outros) estão impedidos de tratar da matéria, ainda que para benefício do acusado, visando-se maior segurança jurídica.

4.2 Princípio da anterioridade da lei penal

O princípio da anterioridade concebe que para a consideração do crime, sua definição legal e a aplicabilidade da respectiva pena deverão ser cominadas anteriormente ao acontecimento do fato delituoso. A lei deve, portanto, viger no momento da prática infracional.

Nas palavras de José Afonso Silva (2005, p.429) "sem que a lei o tenha feito não haverá crime nem pena a ser imposta". Nesse sentido a lei somente se aplica a fatos futuros, não alcançando os anteriores à sua vigência, ainda que venham a ser futuramente tidos como crime.

Note-se que o princípio implica ainda na irretroatividade da lei penal, salvo para beneficiar o réu; garantia penal recepcionada pela Constituição da República, encontrando previsão no art.5º, XL.

4.3 Princípio da territorialidade

O Código Penal alude em sua parte geral, no art.5º, §§ 1º e 2º:

> Art. 5º - Aplica-se a lei brasileira, sem prejuízo de convenções, tratados e regras de direito internacional, ao crime cometido no território nacional.
> § 1º - 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.
> § 2º - 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.

Julio Fabbrini Mirabete conceitua territorialidade e a respectiva aplicação e abrangência na legislação penal brasileira:

> Para definir a possibilidade de aplicação da lei nacional a fatos que ocorram no país ou fora dele ou que violem interesses nacionais embora cometidos no exterior, estabelece a lei os princípios de aplicação penal no espaço, adotando como base o princípio da territorialidade, decorrente da soberania, segundo o qual se aplica a lei brasileira ao crime cometido no território nacional. Em sentido estrito, material, o território abrange o solo (e subsolo), sem solução de continuidade e com limites

> reconhecidos, as águas interiores, o mar territorial, a plataforma continental e o espaço aéreo. [...]. (MIRABETE, 2003, p.119)

Salvo exceções já previstas no *caput* do art.5º, aplicar-se-á lei brasileira ao crime praticado no território nacional, desconsiderando-se a nacionalidade do autor do fato delituoso e da vítima, titular do bem jurídico lesado.

Quanto à extraterritorialidade, prevê o Código Penal em seu art.7º:

> 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;
> *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.
> § 3o 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.
> Pena cumprida no estrangeiro

Nesse sentido, entende-se que o princípio da territorialidade é adotado pelo Brasil em nome da soberania estatal.

Em se tratando de crimes cibernéticos, mais importante que o entendimento de qual lei deverá ser aplicada ao caso concreto é a cooperação mútua dos Estados em seu combate.

5 LEGISLAÇÃO APLICÁVEL

O avanço tecnológico e a era digital foram grandes colaboradores da composição dos denominados crimes cibernéticos.

A insuficiência da legislação específica apropriada para tutelar o espaço digital constitui trunfo para os criminosos, tornando as infrações mais atrativas. A deficiência da proteção legal gera insegurança aos usuários da rede, obrigando-os a investir pesadamente em programas para se resguardarem dos agentes e, ainda assim, correndo riscos de serem vítimas desses indivíduos.

O crescimento acelerado dos crimes digitais preocupa governos e departamentos de segurança dos Estados, fato que despertou interesse das nações em abordar a matéria em seus ordenamentos jurídicos. Contudo, para maior eficiência no combate aos delitos, imprescindível é a cooperação entre os Estados e uniformização das leis no sentido de harmonizar a aplicabilidade das penas cabíveis.

5.1 Legislação internacional

Embora já houvesse o crime cibernético ao final do século XX na Europa, as primeiras medidas repressoras foram tomadas apenas no curso de uma reunião realizada por subgrupo de nações do grupo G8, dispostos a examinar a prática infracional que apresentava como instrumento aparelhagem eletrônica e a própria rede de computadores. Ali o termo *cibercrime* foi utilizado pela primeira vez e empregado para designar de forma ampla as modalidades de crimes praticados no âmbito virtual.

Em 23 de novembro 2001 foi inaugurada a Convenção sobre o Cibercrime, solenizada em Budapest, na Hungria, pelos Estados Unidos e mais trinta e três outros países (principalmente europeus, além do Japão, Canadá e África do Sul); convenção esta da qual foram signatários 43 países, dentre os quais o Brasil não se encontra.

A convenção propõe aos países membros as medidas colaboração em matéria penal a serem tomadas para efetivo combate às infrações; prevê que os países deverão legislar a respeito das sanções a serem impostas a cada uma, a possibilidade de aplicação de pena

privativa de liberdade, matéria processual pertinente e a competência e autoridade suficiente para julgamento dos crimes. Por fim, estabeleceu alguns princípios de cooperação internacional e auxílio mútuo, o que tornaria menos árduo o processo punitivo dos infratores, ainda que cada país possua sua própria legislação.

No Peru, o Código Penal traz dispositivos de coerção aos crimes de informática, introduzidos ao ordenamento jurídico do país pela Lei nº 27.309, de 17 de julho de 2009.

O legislador peruano preocupou-se em proteger os interesses particulares dos usuários da internet, mediante penalização das condutas que provoquem danos à propriedade privada.

O Chile, segundo Fabrízio Rosa (2006, p.84), consta no rol dos poucos países latino-americanos que possuem uma legislação específica acerca dos crimes em âmbito virtual, a Lei nº 19.223. Muito sucinta, é alvo de várias críticas. Embora o país seja precursor na elaboração de normas específicas regentes da matéria, o legislador deixa de abarcar as possibilidades de infrações no âmbito digital em sua totalidade, priorizando determinados assuntos e excluindo os demais.

Os Estados Unidos estão entre os pioneiros na questão de legislação aplicável aos cibercrimes. Já ao final da década de 1970 legislava sobre o tema e em 1986 criminalizava determinadas condutas realizadas por meio de sistema de informática.

> Os EUA começaram a legislar sobre os crimes de informática no fim da década de 1970; a primeira lei federal sobre crimes de informática foi a *Computer Fraud anda Abuse Act – CFAA*, de 1986, que criminalizava condutas como, por exemplo, o acesso não autorizado, seja para obtenção de segredos nacionais com intenção de prejudicar os EUA, seja para obter informações financeiras e de créditos, ou, ainda, o simples acesso não-autorizado a computador do Governo Federal. (ROSA, 2006, p.82)

Possuidor de várias leis sobre a matéria, um dos países mais preocupados no combate os crimes de informática, aplicando leis rígidas, especialmente depois do ataque terrorista sofrido em 11 de setembro de 2001, que deixou explícito o ciberterrorismo.

Na Inglaterra, a *Computer Misuse Act*, de 1990 é a principal lei de combate aos delitos do espaço digital. Embora criticada devido à sua amplitude, tem suma importância na repressão da criminalidade, demonstrando grande preocupação do país nesse sentido.

Acerca da lei inglesa, ensina Carla Rodrigues Araújo de Castro:

> O Computer Act, de 1990, disciplinou várias condutas criminosas ligadas à informática, como, por exemplo, a obtenção de acesso não autorizado a programa ou informação. Dispôs a excludente de responsabilidade criminal sempre que o agente, sem saber, obtém a informação, ou seja, não houve intenção de violar o sistema alheio. (CASTRO, 2003, p. 162)

Fabrízio Rosa também aborda o *Computer Misuse Act*:

> A lei inglesa que dispõe a respeito dos "crimes de informática" foi elaborada em 1990, quando foi introduzido, no ordenamento jurídico, o delito de acesso não-autorizado, dispondo no art.3º, inc. 2º, que a pessoa deve ter a intenção de modificar o conteúdo de qualquer computador através dos seguintes comportamentos:
> * impedindo a operação de qualquer computador; ou
> * impedindo ou dificultando o acesso a qualquer programa, ou a confiança desses dados;
> * impedindo a execução de qualquer dos programas, ou a confiança desses dados. (ROSA, 2006, p.83)

Já em Portugal, desde 1991 a Lei 109 tem sido a ferramenta no confronto com os infratores cibernéticos, onde condutas envolvendo a informática foram tipificadas. O país não se preocupou em punir tão somente as pessoas naturais, mas também as jurídicas, lá chamadas de *pessoas colectivas*.

Observa Paulo de Sousa Mendes acerca da responsabilidade e punição aplicada às pessoas jurídicas em casos específicos não previstos pelo Código Penal Português:

> A localização de certo tipo incriminador dentro ou fora do Código Penal, '[parecendo] ser questão menor, de mera sistemática, tem afinal importantes consequências substantivas'. Por exemplo, a burla informática foi incluída no próprio Código Penal português, no art. 221º, por se considerar que tinha o mesmo significado que burla em geral, ao passo que o dano informático aparece no art. 5º da lei de criminalidade informática. Por consequência, as pessoas colectivas respondem criminalmente pelo dano informático, mas já não respondem pela burla informática[1]

Em 15 de setembro de 2009, nova lei fora publicada com o intuito de adequar a legislação interna às normas estabelecidas pelo Conselho da Europa, atentando para a cooperação determinada na Convenção de Budapeste.

5.2 Legislação brasileira

O ordenamento jurídico pátrio ainda é limitado em se tratando da tutela da esfera virtual, uma vez que a norma penal é antiga e, mesmo com a recente inserção de duas novas

[1]http://www.apdi.pt/APDI/DOUTRINA/A%20responsabilidade%20de%20pessoas%20colectivas%20no%20%C3%A2mbito%20da%20criminalidade%20inform%C3%A1tica%20em%20Portugal.pdf

leis específicas, Lei Nº 12.735 e Lei Nº 12.737, ainda é preciso adequar os crimes cometidos no ciberespaço aos tipos existentes no Código Penal Brasileiro.

O político mineiro e atualmente Deputado Federal, Eduardo Azeredo, na época Senador, criou o Projeto de Lei Sobre Crimes de Informática (PL 84/99), também conhecido como “Lei Azeredo”, no ano de 1999. Desde o início, provocou discussão e várias polêmicas, sendo alvo de críticas constantemente.

O Projeto de Lei passou pela Comissão de Segurança Pública e Combate ao Crime Organizado. A Comissão de Constituição e Justiça da Câmara emitiu parecer favorável à aprovação do Projeto de Lei, e o texto apresentado por ela expôs modificações ao projeto original enviado por Eduardo Azeredo à Câmara em 2008.

Múltiplas pontuações foram feitas no decorrer da tramitação do Projeto: se a norma específica para esta modalidade criminal observava princípios constitucionais, sua viabilidade e, ainda, se demonstrava ser suficiente e eficaz no combate às infrações. Produção de provas, competência, dificuldade de fiscalização e responsabilidade dos servidores também foram importantes tópicos suscitados na discussão em torno do assunto. Logo, a repercussão do Projeto (expressão de seu ineditismo) tornou mais árduo e moroso seu processamento, dividindo opiniões e criando correntes. A primeira corrente enxergava a necessidade de criação e aprovação de uma lei civil regulamentadora da internet, para que, posteriormente, fosse discutido projeto criminal da matéria. A segunda agrupava adeptos à aprovação completa do Projeto de Lei enquanto a terceira contava com aqueles que optavam pela parcial. A quarta e última, reuniu ala significativa que desejava descartar o Projeto.

Em maio desse ano ocorreu aceleração no trâmite do Projeto de Lei 84/99 e outros a ele conexos (que estiveram sob análise por mais de uma década) em virtude do cibercrime que vitimou a atriz brasileira Carolina Dieckmann. A mídia trouxe à tona o episódio do roubo de fotos íntimas do computador pessoal da artista, que foram publicadas na rede. O apelo dos meios de comunicação e a solidariedade do público, em especial dos fãs, exerceram função de estímulo ao Legislativo.

Já em 07 de novembro, na capital nacional, foram aprovados dois Projetos de Leis que preveem pena privativa de liberdade para aqueles que cometem crimes na internet, dentre eles o Projeto de Lei de autoria de Eduardo Azeredo. Sancionados pela Presidente da

República, Dilma Rousseff, e convertidos nas Leis nº 12.735 e 12.737, publicados no Diário Oficial da União em 03 de dezembro.

Enquanto as duas novas Leis não entram em vigor, permanecem lacunas que obrigam o Poder Judiciário a coibir a cibercriminalidade com a aplicação dos Códigos Civil e Penal e demais meios instrumentais que abrangem os casos concretos.

6 ATUAL PANORAMA NO BRASIL

Não obstante a explícita atualidade do tema no cenário do Direito Brasileiro, há grande dificuldade em se tutelar o ambiente digital em razão do dinamismo e da veloz mutação tecnológica. Todavia, ainda que de forma gradativa, os Poderes Legislativo e Judiciário vêm trabalhando a matéria em busca de um arcabouço legal satisfatório.

Houve quem defendesse ser desnecessária a promulgação de nova Lei, posição justificada pelo pensamento de que os crimes praticados na internet são os mesmos já elencados no Código Penal Brasileiro, apenas são diversos os instrumentos utilizados pelos infratores. Portanto, à luz da lei criminal, o cibercrime configuraria conduta típica, ilícita e punível da mesma maneira que todos os demais tipos penais já descritos pelo ordenamento jurídico.

Lado outro, a proposta de uma legislação específica que tratasse dos crimes cibernéticos foi defendida por importantes figuras sociais, especialmente das áreas do Direito e Ciências da Computação, dentre os quais é possível citar o atualmente Deputado Federal, Eduardo Azeredo, criador do Projeto de Lei Sobre Crimes de Informática (PL 84/99), convertido na Lei Ordinária Nº 12.735.

A divergência entre as correntes é notável e a discussão sobre o assunto ainda está longe de ser encerrada, principalmente após a publicação de uma pesquisa realizada *Ponemon Institute*, em 08 de novembro desse ano, demonstrando que o Brasil é, atualmente, o segundo país na cibercriminalidade. O estudo foi intitulado “Percepções sobre segurança de rede”, onde inúmeras empresas foram entrevistadas, fornecendo dados e informações que possibilitaram a montagem de gráficos demonstrativos (a notícia foi disponibilizada na página “canaltech”, pertencente ao grupo R7).

Em 05 de setembro desse ano, a *Symantec*, empresa mundialmente conhecida por oferecer medidas protetivas de informações, especialmente pela linha de antivírus “Norton”, divulgou o resultado de seu relatório anual embasado em dados coletados sobre fraudes digitais, o *Cybercrime Report 2012*.

A pesquisa demonstra que os crimes têm se expandido sobretudo nas redes sociais, em razão do aumento do acesso às mídias pelos usuários e da falta de cuidados básicos para sua proteção.

Em decorrência do descuido dos usuários o cibercrime tem gerado prejuízos superiores a bilhões de dólares por ano em todo o globo. O estudo aponta que os prejuízos com cibercrimes totalizaram em R$15,9 bilhões no Brasil no último ano, calculando-se que no país cerca de 28,3 milhões de pessoas tenham sido vítimas de algum tipo de crime pela internet.

Diante da proporção tomada pela prática dos crimes no âmbito digital, vislumbradas por meio das mais recentes pesquisas, ressaltando o rico histórico dos mais variáveis delitos já praticados, notável a necessidade da tomada de medidas de urgência a fim de coibir os ilícitos e proporcionar maior segurança ao usuário da internet.

A aprovação de dois Projetos de Leis, convertidos em Leis Ordinárias e publicados no Diário Oficial da União, em 03 de dezembro, demonstra a preocupação com a vulnerabilidade daqueles que acessam a internet, partindo-se em busca da tutela Estatal. Trata-se de grande avanço na seara do Direito Digital, entretanto, ainda é insuficiente. Mais importante que instituir leis abrangentes, é prover condições para que as mesmas sejam executadas. Essa é, pois, uma das premissas trazidas pela Lei Nº 12.735, em seu art.4º:

> Art. 4º Os órgãos da polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado.

.

7 CONSIDERAÇÕES FINAIS

O presente trabalho teve como objetivo analisar os crimes cibernéticos sob a ótica do Direito Brasileiro, tratando de aspectos gerais desse novo ramo que necessita de tutela concretizada e eficaz, posto que a dimensão criminal situada no universo digital não se limita a conservar as perspectivas preconizadas pelas normas pátrias; traz consigo as peculiaridades da nova realidade.

A internet, introduzida ao cenário global durante a Guerra Fria, originou-se de um projeto militar, passando por modificações e evoluções, popularizando-se e culminando no acesso mundial.

Os crimes cibernéticos já existiam na Europa ainda no século XX, contudo, as primeiras medidas repressoras somente vieram a ser tomadas em 2001, quando um grupo de países se mobilizou para tratar da matéria, estabelecendo que houvesse trabalho em cooperação, para que assim os países pudessem combater os delitos. A partir de então, as nações signatárias iniciaram seus trabalhos no combate aos crimes cibernéticos, elaborando leis rígidas e tratados.

No território brasileiro o tema é recente, opiniões são divididas e a legislação é escassa. Deste modo, os delitos têm ganhado destaque em função da velocidade com que se propagam e de suas graves consequências, bem como do estímulo que a impunidade oferece aos agentes infratores.

Ao se tratar dessas infrações surgem incógnitas que, para serem erradicadas, é preciso buscar respostas além de doutrinas e textos normativos.

A lei define o crime, estabelece seus elementos de configuração, impõe pena ao fato típico, determinando as diretrizes a serem observadas e, paralelamente, o estreitamento das relações entre operadores do Direito e profissionais da área tecnológica possibilita a coerção estatal. Enquanto estes se dedicam à busca dos avanços e impactos das infrações, bem como ao entendimento do desenvolvimento da atividade criminosa, aqueles procedem com as investigações, de forma mais segura e com maiores garantias. A capacitação e o investimento no preparo dos profissionais, especialmente dos policiais e dos integrantes do Poder Judiciário em sua totalidade, bem como na infraestrutura e o fornecimento de ferramentas de trabalho ampliam as possibilidades de captura e punição dos criminosos.

Por fim, de suma importância é a conscientização e educação da coletividade, não apenas para que os cuidados básicos passem a ser tomados mas, principalmente, para que os atingidos não permaneçam omissos. Quanto mais célere a manifestação das vítimas, maior a chance de sucesso nos trabalhos investigativos, resultando em uma resposta mais rápida e satisfatória. Tais medidas devem ser tomadas visando redução no índice de criminalidade, bem como uma consequente melhoria na segurança social.

Por fim, ressalte-se que o presente trabalho não visa o exaurimento da matéria, posto que o assunto é relativamente novo, mas sim demonstrar a fragilidade da segurança dos usuários da rede mundial de computadores e a gravidade de não possuir uma estrutura legal plenamente capaz de punir os criminosos e erradicar a prática dos crimes cibernéticos.

REFERÊNCIAS

BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Código Penal. **Vade Mecum Rideel**. São Paulo: Rideel, 2012. p. 343.

BRASIL. Decreto-Lei nº 3.689, de 3 e outubro de 1941. Código de Processo Penal. **Vade Mecum Rideel**. São Paulo: Rideel, 2012. p. 394.

BRASIL. Constituição Federal. **Vade Mecum Rideel**. São Paulo: Rideel, 2012. p. 24.

BRASIL. Lei nº 12.735, de 30 de novembro de 2012. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências.

BRASIL. Projeto de Lei n° 84, de 1999.

BRASIL. Projeto de Lei Substitutivo ao Projeto de Lei da Câmara nº 89, de 2003.

CAPEZ, Fernando. **Curso de Direito Penal:** parte geral. 8.ed. São Paulo: Impetus, 2005, v.1.

CAPEZ, Fernando. **Curso de processo penal.** 17.ed. São Paulo: Saraiva, 2010. 875 p.

CARPANEZ, Juliana. Entenda a polêmica sobre o impacto da lei de crimes cibernéticos. **G1**. São Paulo, 21 jul. 2008. Disponível em <http://g1.globo.com/Noticias/Tecnologia/0,,MUL651929-6174,00-ENTENDA+A+POLEMICA+SOBRE+O+IMPACTO+DA+LEI+DE+CRIMES+CIBERNETICOS.html>. Acesso em: 13. set. 2011

CASTELLS, Manuel. **A sociedade em rede**. Trad. Roneide Venâncio Majer. 6. Ed. São Paulo: Paz e Terra, 1999. 617 p.

CASTRO, Carla Rodrigues Araújo de. **Crimes de Informática e seus Aspectos Processuais**. 2. ed. Rio de Janeiro: Lumen Juris, 2003, 230 p.

DERTOUZOS, Michael L. **O que será: como o novo mundo da informação transformará nossas vidas**. Trad. de Celso Nogueira. São Paulo: Cia. das Letras, 1998, 416 p.

GOUVÊA, Sandra. **O Direito na Era Digital:** Crimes Praticados por meio da Informática. Rio de Janeiro: Mauad, 1997. 164 p.

GUIMARÃES, José Augusto Chaves; FURLANETO, Mário. Crimes na internet: elementos para uma reflexão sobre a ética informacional. **R. CEJ,** Brasília, n. 20, p. 67-73, Jan. / Mar. 2003

KLEINA, Nilton. A história da Internet: a década de 1990. **TECMUNDO**. Disponível em: <http://www.tecmundo.com.br/infografico/10054-a-historia-da-internet-a-decada-de-1990-infografico-.htm?utm_source=outbrain&utm_medium=recomendados&utm_campaign=outbrain=obinsit>. Acesso em: 17 mar. de 2012.

KLEINA, Nilton. A história da Internet: pré-década de 60 até anos 80. **TECMUNDO**. Disponível em: <http://www.tecmundo.com.br/infografico/9847-a-historia-da-internet-pre-decada-de-60-ate-anos-80-infografico-.htm>. Acesso em: 17 mar. de 2012.

MACHADO, Jonathan D. Como foi criada a internet. **TECMUNDO**. Disponível em: <http://www.tecmundo.com.br/internet/28279-como-foi-criada-a-internet.htm?utm_source=outbrain&utm_medium=recomendados&utm_campaign=outbrain=obinsite>. Acesso em: 14 ago. de 2012.

MENDES, Paulo de Sousa. **A responsabilidade de pessoas colectivas no âmbito da criminalidade informática em Portugal**. Portugal. Disponível em: <http://www.apdi.pt/APDI/DOUTRINA/A%20responsabilidade%20de%20pessoas%20colectivas%20no%20%C3%A2mbito%20da%20criminalidade%20inform%C3%A1tica%20em%20Portugal.pdf>. Acesso em: 20 set. de 2012.

MIRABETE, Julio Fabbrini. **Código Penal Interpretado.** 3. ed. São Paulo: Atlas, 2003. 470 p.

MORAES, Alexandre de. **Direito constitucional.** 25.ed. São Paulo: Atlas, 2010. 922 p.

NADER, Paulo. **Introdução ao Estudo do Direito.** 24. ed. São Paulo: Malheiros, 2005. 384 p.

PROCURADORIA DA REPÚBLICA EM PERNAMBUCO. Disponível em: <http://www.prpe.mpf.gov.br/internet/content/download/2770/22203/file/CONVEN%C3%87%C3%83O%20DE%20BUDAPESTE.pdf>. Acesso em 23 ago. de 2012

ROSA, Fabrízio. **Crimes de Informática**. 2. ed. Campinas: Bookseller, 2006. 141 p.

SANTOS, Coriolano Aurelio De Almeida Camargo. **As Múltiplas faces dos Crimes Eletrônicos e dos Fenômenos Tecnológicos e Seus Reflexos no Universo Jurídico**. 2. ed. São Paulo, OABSP, 2009. 162 p.

SILVA, José Afonso da. **Curso de Direito Constitucional Positivo.** 24.ed. São Paulo: Malheiros, 2005. 413 p.

SIQUEIRA, Ethevaldo. **Revolução Digital.** São Paulo: Saraiva, 2007. 369 p.

SOUZA NETO, Pedro Américo de. **Crimes de informática.** 2009. 79 f. Monografia (Bacharel em Direito) - Centro de Ciências Sociais e Jurídicas, Universidade do Vale do Itajaí, Itajaí, 2009.

TASSE, Adel El. Crimes Informáticos: da Tipificação Existente aos Cuidados para Impedir a Censura à Livre Comunicação Humana. **Revista Magister de Direito Penal e Processual Penal**, Porto Alegre: Magister, v. 6, n. 36, p. 32-55, Jun. / Jul. 2010.

2012 Norton Study: Consumer Cybercrime Estimated at $110 Billion Annually. **Symantec.** Disponível em: <http://www.symantec.com/about/news/release/article.jsp?prid=20120905_02>. Acesso em 04.out.2012