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

TENÓRIO SILVA LACERDA SEGUNDO

CRIMES DIGITAIS: TIPIFICAÇÃO E SEGURANÇA JURÍDICA

SOUSA - PB
2009

TENÓRIO SILVA LACERDA SEGUNDO

CRIMES DIGITAIS: TIPIFICAÇÃO E SEGURANÇA JURÍDICA

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 Me. Márcio Flávio Lins de Albuquerque e Souto.

SOUSA - PB
2009

TENÓRIO SILVA LACERDA SEGUNDO

CRIMES DIGITAIS: TIPIFICAÇÃO E SEGURANÇA JURÍDICA

Trabalho de Conclusão apresentado ao Curso de Direito do Centro de Ciências Jurídicas e Sociais, da Universidade Federal de Campina Grande, em cumprimento aos requisitos necessários para obtenção do título de Bacharel em Ciências Jurídicas e Sociais.

Orientador: Prof. Mestre e Doutorando Márcio Flávio Lins Souto.

Banca Examinadora:

Data de aprovação:___/___/_____

_____

Prof. Márcio Flávio Lins Souto

Orientador

_____

Examinador

_____

Examinador

Dedico este trabalho aos meus amados pais, pelo esforço dispensado sempre no intento de proporcionar o melhor para meu crescimento profissional, bem como pela força e confiança que depositam em minha pessoa, assim como ao meu saudoso avô, Francisco Silva, pelas suas lições de honra, justiça e dignidade, vindas de um homem que não precisou de diploma para conhecer dos mais retos princípios que um ser humano deve carregar consigo.

AGRADECIMENTOS

Agradeço a Deus pela maravilha da vida, pela saúde e por todas as demais bênçãos derramadas sobre mim, concedendo-me forças para superar as dificuldades do cotidiano.

Ao meu pai, Tenório Silva Lacerda, pelo imensurável esforço para que meus sonhos sejam realizados, por ser um homem admirável diante de suas incontáveis virtudes, por tudo o que passa em nome do meu futuro e pela prova de que a distância não consegue destruir um grande amor recíproco. Minhas vitórias são suas também.

A minha mãe, Alda Maria Dias Lacerda, grande incentivadora, por me ensinar pelo exemplo, pelas suas atitudes de uma mulher inteligente, forte, determinada e vencedora, por acreditar no mais brilhante futuro para seu filho. Nossas glórias estão apenas começando.

As minhas irmãs, Tellyani e Thaís, pelo fantástico trio que formamos, pelo apoio em todos os momentos e pela alegria das vitórias. Vocês estão no meu coração.

A minha namorada, Alinne de Souza, pelo tempo que foi subtraído em nome dos meus estudos, assim como pela enorme paciência. Nos momentos em que encontrei dificuldade, descobri no seu sorriso a força para seguir em frente.

Aos meus avós maternos, Manuel Dias, e Maria do Carmo, por estarem sempre presentes na alegria de cada conquista. Vocês terão ainda mais orgulho deste neto que muito os ama.

A todos os demais familiares, pela força e pelas boas energias, porque cada um teve sua participação nesta vitória.

Ao professor orientador, Márcio Flávio Lins Souto, pela dedicação e atenção dispensada a mim no auxílio à feitura deste trabalho.

Aos meus amigos do Curso de Direito, sendo injusto nomeá-los, pelos bons momentos vivenciados durante a fase acadêmica, pelo ânimo nos momentos difíceis e pelas boas risadas. Sentirei falta de todos vocês, mas acredito ter conquistado verdadeiros amigos.

"Se o jurista se recusar a aceitar o computador, que formula um novo modo de pensar, o mundo, que certamente não dispensará a máquina, dispensará o jurista. Será o fim do estado de Direito e a democracia se transformará facilmente em tecnocracia".

Renato Borruso

RESUMO

Com o advento do computador e da internet, o mundo passou por diversas transformações, surgiram novas tecnologias, as quais proporcionaram comodidade aos usuários, com a prestação dos mais variados serviços. No entanto, apesar dos benefícios, alguns indivíduos aproveitam-se dessa imensa rede de comunicação para o cometimento de delitos, violando relevantes bens jurídicos. A sociedade, no momento atual, vive uma nova realidade, passando a interagir dentro de um universo de relações humanas, denominado "ciberespaço", um ambiente virtual carente de controle por parte do Estado, ou seja, com precária fiscalização pelos órgãos competentes, o que facilita a prática criminosa, pelo fato de o ordenamento penal brasileiro não prever penas para determinadas condutas praticadas no meio digital. Ressalte-se que o Direito surgiu para regular a convivência humana, adaptando-se às necessidades sociais pelo acompanhamento das suas mutações. Portanto, deve o ordenamento pátrio definir normas regulamentadoras do meio virtual, evitando a impunidade e proporcionando segurança jurídica e paz social.

Palavras–chave: Internet. Crimes Digitais. Segurança Jurídica.

ABSTRACT

With the advent of the computer and the internet, the world has passed through many transformations, new technologies have arisen, what has provided commodity to the users, with the offer of the most varied services. However, in spite of the benefits, some individuals take advantage of this immense net of communication to commit crimes, violating relevant judicial estates. Society, at the present moment, lives a new reality, starting to interact inside a universe of humane relations denominated "cyberspace", a virtual environment lacking of control from the State, that is, with precarious supervision by the competent organs, what facilitates the criminal practice, for the Brazilian penal ordainment does not foresee punishments to determined conducts practiced in the digital ambient. It is important to highlight that the Law has arisen to regulate the humane intimacy adjusting to the social necessities by the accompaniment of its mutations. Therefore, the paternal ordainment must define regulative standards of the virtual ambient, avoiding the impunity and providing judicial safety and social peace.

Keywords: Internet. Digital Crimes. Judicial Safety.

SUMÁRIO

1 INTRODUÇÃO

O objetivo do presente trabalho pauta-se na realização de um estudo acerca da temática de crimes cometidos no meio virtual, tendo atenção especial ao aspecto da impunidade dessas novas modalidades delituosas em decorrência da atual legislação penal, avaliando as consequências resultantes para a sociedade globalizada. Para atingir tal objetivo, seguir-se-ão alguns procedimentos metodológicos com o intuito de conferir um maior grau de cientificidade à pesquisa.

A problemática em tela demonstra-se de grande relevância e atualidade no meio jurídico, vindo desse fato o interesse do estudo e pesquisa de suas peculiaridades. Acerca do assunto, diversas pesquisas doutrinárias surgem atualmente, garantindo a contribuição ao meio acadêmico na feitura de trabalhos como este.

A jurisprudência nacional ainda apresenta poucas decisões em sede de crimes cometidos por meio de computador. Dá-se tal fato pelas dificuldades encontradas por parte dos órgãos de investigação no combate aos crimes digitais, principalmente em virtude da precária preparação técnica na área e da omissão legislativa em relação às condutas potencialmente danosas, porém não previstas na legislação vigente.

Neste trabalho, segue-se o método dedutivo. Dessa forma, a legislação penal em vigor é analisada, evidenciando suas deficiências no tocante ao tema em foco, enfatizando-se a omissão legislativa frente às novas modalidades delituosas surgidas com a mudança das relações sociais trazidas pela internet.

O método jurídico adotado constitui no sistemático, e, nesse sentido, a pesquisa situou-se dentro do sistema jurídico-penal vigente no País, o qual se encontra desatualizado, perfazendo uma análise crítica do problema, observados os pontos que deveriam ser aperfeiçoados, a exemplo da premente necessidade de uma lei específica para o controle dessa nova onda de criminalidade, tratando dos crimes já existentes na legislação, praticados de modo diferente, bem como dos novos delitos surgidos com a informática.

No que diz respeito ao objetivo geral, enfatiza-se as causas e consequências da regulamentação legal do tema, ou seja, da criação de uma legislação penal específica, rígida e eficaz no combate e prevenção dos crimes em rede, tendo em vista que o atual Código Penal resta-se ultrapassado em sede de "cibercrimes".

Quanto aos procedimentos técnicos utilizados, adota-se uma pesquisa bibliográfica. Para a elaboração desta pesquisa foram consultadas obras que tratam sobre o assunto, como doutrinas, artigos de internet, pesquisas em sites especializados na matéria e revistas, justificando-se, dessa forma, a classificação em questão e concedendo embasamento material ao presente estudo.

Ao iniciar a explanação da temática, tem-se o histórico da internet, tratando do advento e expansão desse meio no Brasil e no mundo. Em seguida, faz-se menção aos serviços, vantagens e desvantagens da rede mundial de computadores, ressaltando-se o tema da segurança e questionando a necessidade de inovação legislativa frente à apresentação das teorias ontológica e instrumentalista.

Por conseguinte, os crimes na internet serão abordados, no que diz respeito ao aspecto da impunidade para, posteriormente, apresentar as novas modalidades criminosas, não previstas em nosso ordenamento penal vigente.

Finalmente, far-se-á análise da necessidade de normatização do espaço virtual, no que se refere à criação de uma lei específica, apresentando-se as propostas de normatização que tramitam no Congresso Nacional, e comparando-se o tratamento legislativo do Brasil com legislações de outros países.

Portanto, trata o referido trabalho dos crimes realizados por meio do computador, viabilizados pela internet, e da insegurança jurídica em face da omissão legislativa acerca de condutas violadoras de direitos individuais fundamentais.

2 O DIREITO E A REDE MUNDIAL DE COMPUTADORES

2.1 Internet: Delineamento Histórico

Nos Estados Unidos, no final dos anos 60, em decorrência do desenvolvimento de projetos militares do Departamento de Defesa Norteamericano – *Advanced Research and Projects Agency* (ARPA), com a criação da ARPANET, a primeira rede de computadores do mundo, interligou a Universidade da Califórnia – Los Angeles, *Stanford Research Institute* (SRI); Universidade de Utah e Universidade da Califórnia – Santa Bárbara. Utilizava-se a rede telefônica convencional através do sistema de aluguel de circuitos.

Naquela época, em que a Guerra Fria representava o risco de um possível ataque nuclear russo que viesse a destruir o banco de dados de uma unidade militar americana, fez-se necessário a criação de uma rede de comunicação que conectasse os principais centros militares e, caso ocorresse um ataque, não prejudicasse a comunicação entre eles. O cenário da Guerra Fria era caracterizado pela corrida armamentista e tecnológica entre as duas potências mundiais daquele momento, onde os Estados Unidos buscavam alcançar a superioridade tecnológica e militar sobre a União Soviética. De um lado, a União das Repúblicas Socialistas Soviéticas (URSS), comandada pela Rússia, como parte do bloco socialista, e de outro os Estados Unidos da América, representando o bloco capitalista, constituindo um mundo bipolar.

A partir da ARPANET, projeto inicial da internet, foram realizadas várias pesquisas por cientistas na intenção do seu aperfeiçoamento. Na década de 70, conseguiu-se obter um conjunto de protocolos de conectividade, que hoje é a base da internet, o *Transmission Control Protocol/Internet Protocol* (TCP/IP). Na década de 80, a ARPA iniciou a integração das redes de computadores com outros centros de pesquisa de universidades norte-americanas, expandindo o que era bastante restrito.

No ano de 1985, a *National Science Foundation* (NSF), decidiu interligar seus supercomputadores, o que resultou na NSFNET, conectada em 1986 à ARPANET. Com a conexão de todos os computadores e redes a esses dois

supercomputadores, surgiu um *backbone* (estrutura basilar da rede), passando nesse momento ao surgimento oficial da INTERNET.

A partir de 1993, deixou de ser objeto exclusivo de utilização acadêmica e passou a ser explorada comercialmente pelas empresas privadas, proporcionando a sua disseminação mundial.

Em conformidade com as palavras de Castells (2004, p.33):

> Assim, em meados dos anos 90, a internet já estava privatizada e a sua arquitetura técnica aberta permitia a ligação em rede de todas as redes informáticas de qualquer ponto do planeta, a *world wide web* podia funcionar com o *software* adequado e havia vários *browsers* de fácil utilização à disposição dos utilizadores.

Surgida inicialmente nos Estados Unidos, a internet só veio a ser liberada comercialmente na década de 90 para os norte-americanos, e, em seguida, para outros países, propagando-se por todos os lugares, atingindo milhões de usuários em poucos anos, devido à tecnologia *world wide web* (www) que permitia a ligação de todas as redes informáticas do mundo. As técnicas básicas de comunicação criadas pelos militares desenvolveram-se, passando a ter outras finalidades e utilidades, quando liberadas comercialmente para a população civil.

2.1.2 Internet no Brasil

No Brasil, essa inovação tecnológica chegou aproximadamente em 1988, acompanhando a tendência mundial, inicialmente restrita às universidades e centros de pesquisa, por iniciativa das instituições acadêmicas de São Paulo (Fundação de Amparo à Pesquisa do Estado de São Paulo - FAPESP), do Rio de Janeiro (Universidade Federal do Rio de Janeiro - UFRJ) e do Laboratório Nacional de Computação Científica.

Com a intervenção do Governo Federal, em 1989, por intermédio do Ministério da Ciência e Tecnologia, foi criada a Rede Nacional de Pesquisas – RNP. Instituição encarregada de iniciar o processo de disponibilização dos serviços de internet no Brasil, através da criação do *backbone* RNP que interligava, inicialmente,

11 estados a partir de pontos de presença em suas capitais (*Points of Presence* - POP).

Posteriormente, por volta de 1994, foi liberada para uso doméstico, através dos provedores de acesso que disponibilizavam comercialmente o serviço, tendo como pioneira a Empresa Brasileira de Telecomunicação (EMBRATEL), por meio de uma forma de acesso através de linha discada.

Seguindo a tendência mundial, a difusão da internet no Brasil ocorreu de forma impressionante, ao passo que o Estado deparou-se com uma nova conjuntura social, tendo em vista que, associado a todo um avanço tecnológico, diversos problemas surgiram principalmente quanto à inovação da criminalidade.

2.2 A Grande Rede: Serviços, Vantagens e Desvantagens

A internet, termo advindo da expressão *Interconnected Networks,* conceitua-se como um conjunto de redes interligadas pelo mundo inteiro, proporcionando acesso mundial de informações e serviços, através de um protocolo padrão TCP/IP, disponibilizando a todo aquele que possuir acesso a um computador conectado por um modem (dispositivo destinado a permitir o uso de linhas telefônicas para interconectar entre si computadores ou computadores e terminais), acesso à rede mundial de computadores. Tal conexão é disponibilizada por um provedor de acesso à internet.

A internet não é formada de apenas uma rede, mas de várias, em escala mundial, da qual fazem parte redes universitárias, comerciais, militares, científicas, constituída por redes locais pequenas (Local Area Networks - LANs), redes metropolitanas (Metropolitan Area Networks - MANs) e grandes redes de acesso remoto (Wide Área Networks - WANs), conectando computadores do mundo inteiro. Por tal motivo, a grande relevância para a sociedade e para o direito, não apenas do direito brasileiro, mas com reflexos no direito internacional, por transpor as fronteiras nacionais.

O *browser* é um *software,* programa, utilizado na navegação, que significa navegador/pesquisador, existindo uma variedade de opções consideráveis no

mercado, sendo os mais conhecidos, o Microsoft Internet Explorer e o Mozilla Firefox.

Seja qual for o navegador utilizado e o provedor escolhido pelo usuário, a navegação é viabilizada acessando, por meio do navegador, endereços *www* onde ficam disponibilizadas as *home pages* ou páginas de apresentação dos conteúdos.

O computador há muito tempo deixou de ser artigo de luxo para torna-se objeto de grande utilidade no cotidiano, como suporte para a prática de atividades científicas e empresariais. Com o advento da internet, além de outras funções, tornou-se um instrumento de comunicação mundial, transpondo as barreiras nacionais, possibilitando a prática dos mais variados negócios jurídicos e também como forma de lazer e difusão de informações, figurando atualmente como instrumento essencial dentro da sociedade informatizada, fruto da revolução tecnológica do século XX.

São inúmeras as vantagens da internet, como podemos destacar: a troca de informações, em escala mundial, de forma rápida e simples, gerando a quebra dos limites geográficos entre os povos, no tocante à comunicação; instrumento de pesquisa e trabalho; meio de publicidade de empresas, sendo fundamental ferramenta empresarial. Dessa maneira, configura um meio de conexão entre pessoas de diversas partes do mundo, estando em permanente expansão.

Em suma, a rede mundial possibilita aos seus usuários a prática de quase todos os atos da vida cotidiana sem necessidade de sair de casa, acessando os mais variados tipos de serviços e informações como, por exemplo, a realização de transações comerciais, interação social, serviços de instituições bancárias, acesso a sites de pesquisa científica, dentre outros.

Ressalte-se a grande utilização da tecnologia de informática nas atividades do Poder Judiciário brasileiro, o qual faz uso das inovações para garantir publicidade aos seus atos, podendo qualquer interessado, ressalvadas as demandas que tramitam em segredo de justiça, acessar sites de tribunais e sistemas de informação para acompanhar o andamento processual, garantindo-se uma prestação jurisdicional célere e social.

Apesar da tantos benefícios, a internet apresenta um lado negativo, figurando como um território sem lei onde é possível encontrar-se de tudo, a exemplo de exercício de práticas ilegais, verificando-se a mais variada presença de ilícitos, como crimes contra o indivíduo, sua imagem e liberdade, bem como contra a criança e ao

adolescente, invasão de dados e sistemas informáticos de instituições financeiras. Muitos desses delitos restam-se impunes pela justiça, por causa do anonimato proporcionado aos criminosos, dificultando sua identificação, assim como pelo fato de determinadas condutas não serem tipificadas em lei penal, ou seja, ocorrendo ausência de lei que as descrevam como crimes.

Frente às mudanças nas relações sociais, inovações no que concerne ao modo de comunicação entre os indivíduos, incumbe ao direito o exercício da adaptação para essas novas formas de interação, visando tutelar direitos fundamentais do cidadão.

Para a proteção dos bens jurídicos mais relevantes, faz-se necessária a intervenção do direito penal, por meio da tipificação de condutas reprováveis no meio social praticadas no âmbito virtual, através da fixação de penas de caráter retributivo, preventivo e ressocializador, reafirmando o direito penal através da prevenção geral, ou seja, da presença de normas penais rígidas que desestimulem tais condutas.

Com o advento de novas tecnologias, a atividade criminosa passou a ser globalizada, com repercussão mundial, servindo como um agente multiplicador de diversas condutas, como pedofilia, lavagem de dinheiro, tráfico ilícito de entorpecentes e drogas afins, tráfico internacional de pessoas, roubo de informações sigilosas, incitação à prática de ilícitos, crime contra os direitos autorais, estelionato, etc. Ocorre, em alguns casos, a prática de crimes já previstos em lei, utilizando-se os criminosos de um meio diferente de atuação, caminho este trilhado em função do anonimato proporcionado pela rede.

2.2.2 Segurança na internet

Por ser meio de comunicação rápido e econômico, a internet é bastante utilizada atualmente na obtenção de informações e na prestação de serviços, interligando uma infinidade de pessoas em todo o planeta. Em princípio, tantas facilidades parecem refletir apenas tranquilidade na vida dos usuários, porém, associado a essa idéia está o risco que se encontra nesse ambiente virtual, por

tratar-se de um espaço no qual navegam milhões de pessoas de todas as índoles e culturas das mais variadas partes do mundo.

Os dados que circulam pela rede mundial de computadores não estão totalmente seguros, tendo em vista a vulnerabilidade dos sistemas informáticos. Um ambiente inseguro facilita a prática de invasões por indivíduos dotados de conhecimentos em informática, que se aproveitam da falta de segurança para prática de crimes e outros ilícitos.

Em conformidade com Paesani (2001. p.27):

> Sistema informático é o conjunto de elementos de *hardware* (parte física do computador) e de *software* (Programa que o move/parte imaterial) composto de uma unidade central de elaboração de dados, uma unidade periférica e um *software*.

Portanto, tal sistema é passível de violação. Tanto usuários comuns quanto as pessoas jurídicas, podem ser alvo e ter seus computadores invadidos em face da capacidade daqueles que utilizam os mais variados métodos para conseguirem seus objetivos, como o envio de *Trojan Horses,* programas executáveis que transformam seu micro em um terminal de internet "aberto". Estes programas limitam ou eliminam as proteções que impedem a transferência de informações, ou seja, abrem uma porta de comunicação não monitorada.

O mercado oferece serviços e programas destinados à proteção em rede, mas muitos não utilizam os cuidados necessários para prevenção, como manter sempre o computador com antivírus, um *firewall*, programa que funciona como uma barreira impedindo acesso remoto de pessoas não autorizadas, entre outras medidas que assegurem maior segurança na navegação.

Na maioria das vezes, as invasões a sistemas são praticados por pessoas que entram e saem de um computador sem serem percebidos, dotadas de conhecimentos na área, sem a intenção de causar danos, apenas objetivando exibir sua habilidade, os chamados *Hackers.* Contudo, há casos em que os invasores agem de má-fé visando danificar o computador alheio, invadindo computadores e excluindo arquivos, movidos pela ideia de anonimato e impunidade, são os *Crackers.*

Em razão das facilidades encontradas para acesso, muitos se aproveitam para entrar na rede, anonimamente, objetivando a prática de crimes, o que torna

difícil a possibilidade de identificação do criminoso. Entretanto, é possível chegar a esses meliantes, desde que haja preparação técnica para tanto.

As medidas de segurança no ambiente informático é tema que merece destaque especial no estudo acerca da criminalidade eletrônica, haja vista que são das lacunas de que os infratores mais se aproveitam para prática delitiva.

A configuração da autoria e da materialidade do crime, apesar de tarefa difícil, é possível, uma vez tomadas medidas preventivas de monitoramento por setores especializados da polícia. Estes que devem estar muito bem preparados, com profissionais capacitados e bem aparelhados.

A segurança na rede só alcançará resultados satisfatórios quando forem implementadas uma série de medidas, exemplificando nas palavras de Vasconcelos (2003, p.56) :

> Uma providência que minimizaria alguns problemas poderia ser tomada, determinando-se aos provedores de acesso à internet que mantenham em seus sistemas os cadastros individuais de seus usuários e, durante certo período, os registros de acesso e identificadores de chamada nas linhas de acesso. A manutenção desses cadastros e registros, visando a preservar os macrointeresses da sociedade cibernética, contribuiria para a evolução segura das comunicações virtuais, exercendo os provedores papel relevante nesse emaranhado de sistemas intercomunicativos.

Dessa maneira, faz-se necessária a especialidade dos órgãos públicos de investigação em conhecimento de informática, bem como o estabelecimento de uma relação de ajuda mútua com provedores de acesso, no intuito de diminuir os ilícitos e, em conseqüência, o conhecimento da identidade do sujeito invasor, para as devidas providências.

Pode-se citar como exemplo de avanço quanto a esse tema o fato de existir um acordo, realizado em 2008, entre o Ministério Público Federal no Estado de São Paulo, e o site Google no tocante ao desbloqueio de informações em sites de relacionamento, e dispondo ao órgão ministerial o acesso a conteúdos duvidosos, gerando a quebra de sigilo digital.

Em conformidade com informações do site Safernet Brasil, instituição de combate à pedofilia na internet, em cerca de um ano após o acordo, o Ministério Público Federal de São Paulo (MPF/SP) já requereu a quebra de sigilo digital de 1.287 perfis de usuários do Orkut, rede social mantida pela empresa norte-americana, com intuito de investigar casos suspeitos de crimes digitais.

Ainda em relação aos indicadores do citado endereço eletrônico, no Estado de São Paulo, foram instaurados 263 inquéritos policiais, sendo 174 na Capital e 89 no interior. Os dados são mais elevados na Capital pelo fato de o Google enviar, de forma direta, ao MPF da capital as informações com indícios de pornografia infantil para a devida apuração. Então, inicia-se um procedimento e, conforme o caso, os dados são enviados aos órgãos ministeriais de outras cidades. Dessa maneira, comprova-se a efetiva aplicação prática do acordo firmado entre o Ministério Público Federal de São Paulo e o site Google.

Enfim, em matéria de prevenção em rede, demonstra-se eficaz a cópia de segurança dos arquivos mais importantes para o usuário, com intuito de proteger de eventual contaminação por vírus e outros códigos maliciosos, pois, na ocorrência de dano, os dados apagados poderão ser recuperados, deve estar sempre atento com os arquivos e dados transferidos pela internet, tendo em vista a alta vulnerabilidade dos sistemas, devendo tomar atitudes preventivas, minimizando os riscos, podendo qualquer indivíduo ser vítima das práticas mencionadas.

2.3 Sociedade Informatizada e Segurança Jurídica

Através da fixação de normas, regras e leis coercitivas reguladoras da atuação de cada um dos seus membros no meio social, busca a Ciência Jurídica a adaptação frente às inovações e mudanças nas relações sociais, com o objetivo de reger os negócios jurídicos, assegurar direitos fundamentais, instituir competências, atribuir prerrogativas, buscando a harmonia e paz social, sem as quais se estaria diante de total insegurança jurídica.

Configura o Direito uma ciência social, pois sua existência está atrelada à sociedade, ocorrendo uma relação de dependência entre o direito e o social, porque um existe em decorrência do outro, não havendo sociedade organizada sem um mínimo de ordem e paz social, não se podendo conceber qualquer atividade desprovida de forma e garantias jurídicas, nem qualquer regra jurídica que não esteja direcionada aos indivíduos.

A mera existência de uma norma com objetivo de regular as atividades humanas não implica, de forma direta, na sua efetiva aplicabilidade perante fatos

novos acontecidos, pois nem sempre se aplica da melhor forma ao caso concreto, devido à sua impropriedade. É o que se percebe frente à tentativa de aplicar as normas previstas no Código Penal na repressão aos crimes da era digital.

A tecnologia de informação e interação trouxe consigo muitas vantagens e desvantagens para a sociedade moderna, sobretudo com a inovação da informática, fenômeno trazido pela globalização, existindo computadores interligados a uma rede mundial que dispõe da maior variedade existente de serviços e informações, passíveis de acesso a todos que disponham de um computador conectado a internet. Mas, por outro lado, também trouxe a ocorrência de novas modalidades delituosas, como também do cometimento de crimes já previstos em lei.

A edição de leis no Brasil não acompanhou a evolução trazida pela era digital, com a elaboração de novas normas que se adaptem à atual realidade e necessidade sociais. Dessa forma é preciso uma atitude por parte do poder legislativo para suprir tal omissão, possibilitando aos órgãos de investigação a atuação no sentido de se buscar a punição a tais indivíduos, que se aproveitam das omissões legais, da falta de previsão compatível, para lesarem bens jurídicos não protegidos de forma específica pela legislação penal vigente.

2.4 A Legislação Atual e Necessidade de Lei Específica

Tendo em vista que as transformações sociais ocorrem em velocidade muito mais intensa que a inovação das leis, o legislativo, incumbido da função típica normativa, não é tão rápido e eficiente como os cientistas que se dedicam ao avanço da alta tecnologia. O que existe de concreto até então são propostas para regulamentação dessa problemática, através de projetos de lei que tramitam pela Câmara dos Deputados e pelo Senado Federal, muitos deles, em decorrência do tempo, encontram-se arquivados.

A legislação penal brasileira, mais especificadamente o Código Penal, já se mostra impotente e sem eficácia no combate à nova criminalidade surgida com o advento da informática, tendo em vista que, na década de 1940, época de sua origem, a sociedade vivia uma realidade bastante diversa da vivida na atualidade, com outros problemas e uma noção de interação com outras culturas e países muito

limitada da que se tem hodiernamente. Frente aos fenômenos atuais, há um descompasso em relação à lei vigente e, principalmente, em relação ao princípio constitucional do *nullun crimen, nulla poena sine lege,* que veda expressamente a criação de crimes por analogia, o que faz surgir certa situação de impunidade no meio social. Dessa forma, não há crime e, consequentemente, não há pena sem lei que preveja a ação como delituosa. Não se pode, por analogia, imputar crime a alguém sem lei anterior que assim o defina.

O crescimento dos crimes de informática tem como principais fatores a facilidade de acesso à internet, por intermédio de um computador, um bem cada vez mais acessível à população, associado à ousadia de certos indivíduos, visando obter, em detrimento de outros, vantagens econômicas ou meramente de satisfação própria, toda essa conjuntura envolvida na possibilidade de impunidade e certeza do anonimato no meio eletrônico, beneficiados pela carência legislativa sobre a matéria.

O crime via internet e por meio de computadores, mostra-se muito dinâmico, isto é, sempre em constante atualização, evoluindo junto com os avanços da internet. O *Cracker*, o criminoso especializado na prática de crimes informáticos, com seus conhecimentos específicos, desafia as polícias de diversos países, o que nos mostra a necessidade da criação de setores de inteligência especializados e aperfeiçoamento dos já existentes, no combate e repressão aos crimes de rede, a exemplo das Delegacias especializadas em crimes eletrônicos existentes na Região Sudeste e Sul, bem como na Capital Federal, dentre outras.

A nova sociedade surgida com o advento da internet possui características próprias, sendo uma sociedade global e virtual, totalmente heterogênea, onde os cidadãos são os usuários que podem estar em qualquer parte do mundo e possuir as mais variadas intenções. Bastante pertinente a observação de Greco (2001, p.5):

> A civilização que conhecemos nos últimos quatro mil anos apóia-se predominantemente em referenciais de caráter físico para definir valores econômicos e relações jurídicas. A informática fez nascer os bens virtuais e a separação entre meio físico e mensagens que a ele podem estar agregadas.

Nos dizeres do respeitado autor, todo esse avanço tecnológico criou uma realidade distinta de tudo o que já foi vivenciado pelo homem, ao passo que a humanidade pautava-se em valores e referências concretas, para administrar seu cotidiano e criar soluções para seus conflitos. Diferentemente do evidenciado

modernamente, em que distâncias são diminuídas, vínculos são criados a milhares de quilômetros, negócios jurídicos são fechados, originando uma imensa comunidade virtual, composta pelos seus usuários.

Por tais motivos, que se demonstra patente a necessidade de adequação legislativa do direito brasileiro frente a um cenário extremamente dinâmico e criador de problemas sociais.

Também, há a questão de que o crime deve ser um fato típico, antijurídico e culpável, de acordo com o entendimento dominante na doutrina. Então, se ausente um desses requisitos, a conduta não pode ser considerada como crime, fugindo da esfera penal de punição, em virtude do respeito ao princípio da legalidade e da anterioridade da lei penal, previstos no art. 5º, inciso XXXIX e XL da Constituição Federal, bem como no art. 1º do Código Penal.

Faz-se necessária a participação de todos, entre usuários, provedores, organizações internacionais, órgãos do Estado, dentre outros, como forma de coibir esse tipo de abuso, de maneira a reduzir ao mínimo os riscos, por meio de campanhas educativas pela sociedade civil e por maior investimento por parte do Poder Público, no sentido de melhor aparelhar a justiça e órgãos de investigação.

Na atualidade, as atenções devem estar voltadas para o ciberespaço, tendo em vista que o índice de criminalidade nesse ambiente vem crescendo de maneira significativa e, em face da ausência de leis específicas, que regulamentem a matéria, impondo limites na utilização dos recursos informáticos, temos na rede mundial de computadores um lugar suscetível ao cometimento de delitos, tanto na esfera nacional quanto na internacional.

O *Safernet* Brasil, instituição já mencionada nesse trabalho, é uma associação civil com atuação em todo o país, fundada por estudiosos da computação, bacharéis em Direito e professores, sem fins lucrativos ou econômicos, ou qualquer ligação político-partidária, que defende a causa dos Direitos Humanos na Internet, onde possui site o qual disponibiliza indicadores e dados relativos às denúncias recebidas pela instituição sobre crimes cibernéticos, a exemplo de pornografia infantil, incitação e apologia a crimes contra a vida, dentre outros. No endereço eletrônico, pode-se constatar a crescente expansão dos crimes virtuais no Brasil, mas, em compensação, as denúncias aumentam a cada dia, o que demonstra que a sociedade está auxiliando aos órgãos que se propõem a enfrentar

esta nobre causa, pois as vítimas mais recorrentes são as crianças e jovens usuários da rede.

2.4.1 As teorias: ontológica e instrumentalista

O meio eletrônico é um ambiente novo e de extremo dinamismo. Sendo assim, buscam os estudiosos a definição da real necessidade de leis específicas para tratar das demandas que dele inevitavelmente surgem. No tocante a tal necessidade, os posicionamentos acerca da função do direito em regular tais relações dividem-se em dois grupos.

O grupo ontológico defende a ideia de que, com a era da informática, estamos diante de um novo mundo, que demanda um tratamento legislativo diferente. Por seu turno, o grupo instrumentalista é defensor da adaptação das normas já previstas no ordenamento atual, por meio da analogia.

Em conformidade com o pensamento ontológico, a sociedade está diante de um mundo virtual diverso do físico, no qual surge um novo modo de pensar que segue paradigmas digitais. Nesse sentido, sustenta-se que o direito que conhecemos não está apto a regular este novo mundo e também não tem muitas funções a desempenhar, ocasionando insegurança jurídica no meio eletrônico.

Em contrapartida, os instrumentalistas defendem que os conflitos existentes nas relações jurídicas tradicionais e nas do meio digital são similares, devendo-se empregar a analogia na solução de tais casos, ou seja, aplicando o previsto no Código Penal e nas leis já existentes, sendo prescindível a inovação legislativa.

Frente ao extremismo das duas correntes, há aqueles que buscam um ponto de equilíbrio, ou seja, um posicionamento intermediário, conforme a lição de Brito (2009, p.31):

> Em síntese, os princípios jurídicos e os valores construídos ao longo de séculos de história devem permanecer no ordenamento, como uma âncora; no entanto, como os conflitos permanecem, mas o meio os modifica, é necessário que o Direito acompanhe as mudanças e as regule de forma específica quantos às situações fáticas ou a sociedade assim o exigirem.

Tal tendência intermediária parece a mais sensata em termos de aplicabilidade, pelo fato de demonstrar a importância do equilíbrio entre falta de normas e existência de novos conflitos, respeitando as leis existentes e aplicando-as quando possível, mas também defendendo a questão da inovação legislativa no que concerne aos crimes digitais.

3 MODALIDADES CRIMINOSAS

3.1 Crimes na Internet

A convivência humana em sociedade determinou a necessidade de um respeito mútuo para com o direito do seu semelhante. Desse modo, fez-se necessária a taxação de condutas que seriam danosas e prejudiciais ao próprio homem, que feriam direitos alheios e não poderiam ser admitidas na coletividade, sob o risco de desorganizá-la. Desde então, dava-se início à tipificação do ilícito, ou seja, da conduta, omissiva ou comissiva, contrária ao direito, moral e aos bons costumes.

Com o avanço da sociedade, foram criadas leis capazes de regulamentar as relações entre os sujeitos, conforme a demanda social e suas constantes modificações. Foi assim com o Código Penal de 40, atendendo às necessidades daquela época. Contudo, com o passar das décadas, a realidade atual é totalmente diversa.

É nesse breve contexto histórico que se apresenta a real necessidade da tipificação, por meio de atualização legislativa, de condutas potencialmente maléficas aos interesses de terceiros, em face da presente conjuntura da criminalidade informatizada.

A atual legislação penal brasileira, ao ser analisada, demonstra-se desatualizada frente ao grande avanço da criminalidade no âmbito digital.

O advento da internet, como forma de praticar quase todos os atos da vida, teve como uma de suas consequências, o surgimento de uma nova sociedade, a qual tem como principal objetivo a informação.

Dessa maneira, diante dos diversos serviços proporcionados pela rede, e com a intensidade de atuação criminosa na internet, fez com que surgisse a preocupação em regulamentar, de forma eficiente, as relações humanas nela desenvolvidas.

3.1.1 Definição legal de crime

O art. 1º da Lei de Introdução ao Código Penal traz a definição de crime e contravenção penal:

> Considera-se crime a infração penal a que a lei comina pena de reclusão ou de detenção, quer isoladamente, quer alternativamente ou cumulativamente com a pena de multa; contravenção, a infração penal a que a lei comina, isoladamente, pena de prisão simples ou de multa, ou ambas, alternativamente ou cumulativamente.

Tal definição abrange apenas o conceito no aspecto puramente formal, ou seja, as penas correspondentes às contravenções penais e aos crimes, considerando-se crime ou contravenção penal, nesse sentido, as condutas humanas proibidas pela norma penal, ou seja, em contrariedade a uma proibição legal.

A repressão às infrações cometidas na era informatizada encontra-se, em alguns aspectos, dificultada pelas lacunas legislativas existentes, levando-se em conta o princípio da reserva legal, limitador do direito de punir do Estado, que veda a punição de condutas não definidas em lei como crimes, nem da aplicação de penas sem que sejam previamente cominadas.

Um fato é materialmente antijurídico quando implicar lesão ou ameaça a um bem jurídico legalmente protegido. Assim, formalmente, a antijuridicidade é caracterizada como um desrespeito à norma jurídica, enquanto que, materialmente, ela constitui um ataque aos bens jurídicos relevantes, tutelados pelo ordenamento.

Pela definição analítica de infração penal, considera-se crime todo fato típico, antijurídico e culpável, ou seja, sempre configurado quando observados seus elementos constitutivos e fundamentais, de acordo com a posição majoritária da doutrina. Dessa forma, a conduta deve estar descrita em lei, sendo contrária ao ordenamento e sobre o indivíduo deve recair a imputabilidade. A ausência de qualquer desses elementos desnatura a conduta como sendo criminosa.

No estudo do crime e da sua evolução na sociedade, faz-se necessária a pesquisa de fatores que não sejam meramente jurídicos para compreensão do crime em si, bem como de fatores sociais, políticos e econômicos.

Observa-se uma inovação na modalidade delituosa do crime digital, não apenas no modo de cometer o ilícito, mas também na figura do agente criminoso que, diferentemente dos criminosos comuns, apresenta-se como um indivíduo detentor de conhecimentos técnicos avançados na área da informática e pertencente a uma classe social melhor favorecida do que os demais criminosos.

3.1.2 Classificação dos crimes informáticos

Os crimes de informática, doutrinariamente, podem ser classificados da seguinte forma: crime de informática puro, crime de informática misto e crime de informática comum.

O primeiro é caracterizado pela conduta típica, antijurídica e culpável direcionada contra dados em processamento automático e/ou eletrônico ou em transmissão, através da utilização de equipamentos de informática, são cometidos com uso de recursos informáticos e contra dados informáticos. O alvo da conduta criminosa do agente é, exclusivamente, o sistema informático, em sentido amplo, que compreende todo elemento componente da informática, como dados e sistemas do computador, *hardware* (parte física como o próprio computador e periféricos), *software* (programas), unidades de armazenamento externo e etc.

Pode-se mencionar como exemplo de crime informático puro: invasão de sistemas, ataques contra a integridade física dos sistemas, acesso indevido aos dados contidos no computador, acesso não autorizado de computador, dentre outras modalidades variáveis de acordo com a criatividade dos infratores.

Será crime informático puro toda conduta delituosa direcionada contra o sistema de informática em geral, conforme dito, o que não é objeto de tutela jurídica pelo direito penal.

No segundo tipo, também são utilizados equipamentos de informática, porém, o alvo da conduta delituosa é direcionado contra objetos distintos do sistema informático, como, por exemplo, invadir um site de instituição bancária ou financeira para se apropriar de senhas de cartão de crédito.

O alvo da conduta é um bem juridicamente protegido, diferente do informático, sendo que é através da informática, utilizada como uma ferramenta no cometimento do delito, que se consuma o crime.

O crime de informática misto é verificado, por exemplo, quando é utilizado o meio informático para transferir ilicitamente dinheiro de uma conta bancária para outra. Em tal caso, incidem as normas penais e processuais penais na apuração do crime, tendo em vista que o alvo da conduta delituosa, o objeto, a coisa alheia móvel, é juridicamente tutelado, bem como de normas referentes à informática, no

que se refere ao mau uso do computador e da rede para obtenção de vantagem ilícita.

Por seu turno, na terceira modalidade criminosa, os crimes podem ser cometidos independentemente do uso de meios informáticos, isto é, esse meio é utilizado como forma inovadora. A diferença está no *modus operandi*. Em síntese, são crimes comuns, ou seja, a configuração de tipos já existentes, praticados de forma não convencional, ou seja, por meio da utilização dos recursos informáticos.

Os crimes de informática comuns são todas as condutas nas quais o agente utiliza a informática como mera ferramenta para a prática de um crime já tipificado na lei penal. Nesses casos, os crimes podem ser consumados independentemente do uso do computador.

Vislumbra-se, nos crimes de informática mistos e nos crimes comuns, a possibilidade de aplicação da atual legislação penal no caso concreto, mesmo que de forma insuficiente e precária. Tal aplicação não seria possível em se tratando de crimes de informática puros, tendo em vista que o objeto jurídico, alvo da conduta criminosa, no caso, o sistema informático, não é tutelado pela atual legislação.

Apesar de ser possível a aplicação da lei penal existente aos crimes comuns realizados com uso da informática, mais coerente seria, em face da inexistência de lei específica até então e das dimensões trazidas pelo grande alcance da informação, a incorporação de agravantes ao atual código penal.

Com a tecnologia da informação e o surgimento de novas formas delituosas antes nunca presenciadas no meio social, adveio a real necessidade de uma rápida e eficiente atualização legislativa, ou seja, criação de uma lei que preveja uma dura sanção para todas essas novas condutas causadoras de danos a terceiros, bem como da previsão de penas mais rígidas para os crimes cometidos por meio do computador.

Em relação às classificações dos crimes informáticos, das quais a maioria dos estudiosos faz menção à distinção entre os crimes comuns, já previstos na legislação penal comum ou especial; dos crimes inovados através dos recursos informáticos e, por final, dos crimes específicos da área da informática, várias outras classificações são elaboradas.

Dessa forma, convergem as diversas classificações em vários aspectos, tendo em vista que grande parte faz referência aos seguintes tipos de atos ilícitos:

dos atos contra o computador, sistemas e programas computacionais, contra a privacidade, liberdade individual, patrimônio, contra a propriedade intelectual, etc.

3.2 A Inflação de Leis no Ordenamento Brasileiro

Quando a questão de tipificação de delitos informáticos vem à discussão, alguns suscitam a problemática da inflação de leis no ordenamento brasileiro, ou seja, o acúmulo de normas jurídicas sem a real necessidade.

Contudo, não seria possível, no estágio atual da sociedade, a convivência organizada, tanto no meio virtual quanto no materializado, sem que haja um disciplinamento legal eficiente, ressaltando-se que as leis devem acompanhar, da melhor forma possível, a evolução da sociedade e que o atual Código Penal não é suficiente no combate a esses novos crimes.

A falta de uma lei específica, associada à falta de conhecimentos técnicos dos usuários, tendo em vista o acelerado crescimento da rede mundial e a grande criatividade dos delinquentes virtuais, por meio das mais variadas formas de ataque, são objeto de grande preocupação no meio social. A falta de regulamentação no meio eletrônico faz com que surja nesse ambiente a ideia de impunidade e insegurança, que não deve ser tolerada.

A sociedade não pode aceitar esse tipo de abuso, isto é, o aproveitamento das lacunas legais, por indivíduos mal intencionados, para que, com isso, possam implementar uma série de condutas reprováveis ao meio social, porém atípicas em relação à atual legislação penal, resultando muitas vezes em impunidade, tanto pelo fato dessas práticas delituosas não serem tipificadas, quanto pelo fato de algumas serem, de forma precária, enquadradas em um dos tipos penais da legislação vigente.

Nas palavras de Ferreira (2008, p.208):

> A preocupação com essa questão, surgida no Brasil nas últimas décadas com a popularização dos seus procedimentos e com a caracterização de novas situações originadas dos processos de informatização de dados e das operações realizadas com as novas tecnologias, manifestou-se na promulgação de algumas leis relativas à informática, na menção à competência privativa da União para legislar sobre tal matéria, feita pela

> Constituição Federal de 1988 no seu art.22, IV, e em muitos projetos que tramitam no Congresso Nacional sem resolver os problemas mais prementes provocados pelas lacunas da legislação inadequada existente, que estão a exigir uma solução mais condizente com a sua gravidade e a sua incidência.

Percebe-se a problemática em tela pelo fato de existirem muitas leis ineficazes, isso aliado ao fato de inexistir lei específica e eficiente que regulamente os crimes cometidos na internet ou através dela.

Ainda no mesmo artigo, segue a referida autora com tal posicionamento, melhor explicitado nessa lição:

> Em 1987, a lei nº 7.646 limitou-se a dispor sobre a proteção da propriedade intelectual sobre os programas de computador e a sua comercialização no país, disposições que depois foram revogadas pela lei nº 9.609/98 que a substituiu. Essas leis, todavia, longe de esgotarem o assunto, deixaram mais patente a necessidade de aperfeiçoamento de uma legislação relativa à informática para a prevenção e repressão de atos ilícitos específicos, não previstos ou não cabíveis nos limites da tipificação penal de uma legislação que já conta com mais de meio século de existência. O Código Penal brasileiro, cuja parte especial data de 1940, e, portanto, elaborado numa época em que se dava primazia à proteção individual, apesar do volume da legislação especial que o acompanhou posteriormente, não se mostra suficiente e adequado para suprir as necessidades nesse setor e coibir os abusos que se verificam de forma crescente e diversificada, com a constituição de novas modalidades de ofensas a interesses legítimos, no plano individual e social, que ao Estado cumpre coibir, sobretudo, através do direito penal, se os conflitos não puderem ser solucionados de outra forma, como dispõe a boa doutrina, segundo o princípio da subsidiariedade.

Alguns doutrinadores entendem ser perfeitamente viável a aplicação do atual código a esses novos delitos, o que não se demonstra cauteloso, em face desse "improviso". Até porque não era da intenção do legislador daquela época a punição dessa nova onda de criminalidade, e nem poderia, tendo em vista que o computador e a internet são acontecimentos históricos bem mais atuais.

Em artigo jurídico de autoria de Concerino (2001, p.153):

> A falta de regulamentação no que pertine a este tema também constitui elemento de intranqüilidade. Embora esteja sendo aplicada, por exemplo, a legislação comum (Código Penal) a alguns crimes praticados através da rede, o fato é que em determinadas situações, o grau de ofensa ao bem da vida é de tal monta, que a sociedade clama por penalidades mais severas, veiculadas através de normas específicas.

Em tal citação, o autor trata da intranquilidade trazida pela falta de regulamentação da matéria de delitos digitais, chamando a atenção para os efeitos

de um crime praticado na rede virtual, tendo consequências mais amplas do que as de um delito comum, questão já mencionada neste estudo.

3.3 Direito Penal da Informática

No Brasil, o ramo do direito que, em caráter embrionário, tem se preocupado com o estudo das relações sociais viabilizadas pela informática é o direito da informática, por meio da aplicação de normas legais de controle do meio virtual, da transmissão de informações, como forma de prevenir os efeitos negativos trazidos à sociedade em virtude do surgimento dessas novas tecnologias.

O objeto de estudo de tal disciplina constitui na análise das conseqüências jurídicas trazidas ao meio social informatizado, ressaltando-se o rápido crescimento da utilização de novas tecnologias de informação, levando-se em conta o crescente uso da internet como meio dominante de comunicação global.

Pode-se defini-la como um conjunto de normas que visam regulamentar o uso da informática no meio social, tendo em vista as relações jurídicas resultantes, guardando estreita relação com o direito penal, em se tratando da regulamentação dos crimes de informática. Nesse aspecto, já se cogita o surgimento de um novo ramo do direito, o direito penal da informática.

O Direito da informática constitui uma disciplina autônoma, pelo fato de possuir objeto de estudo próprio: a informação, em caráter mediato, e a tecnologia, abrangendo a informática e telemática, em caráter imediato.

A metodologia utilizada nessa disciplina consiste no uso de conceitos técnicos e na aplicação de normas jurídicas existentes para a resolução das questões sociais resultantes. Tem como fontes próprias a lei, a doutrina e a jurisprudência.

Como disciplina autônoma, o direito da informática aborda a proteção de dados informáticos pessoais, proteção de programas de computador, dos contratos realizados no meio informático, a responsabilidade civil derivada das relações originadas pelo uso de novas tecnologias e os crimes ou delitos de informática, objeto central deste estudo, dentre outros aspectos.

3.3.1 Dos bens jurídicos tutelados

Em relação à proteção dos dados pessoais, ressalte-se o aspecto do uso do meio informático para a prática de delitos, como dano à honra (calúnia, injúria e difamação), da ofensa ao nome da pessoa e à imagem. Em tais casos, resta configurada a modalidade de crime informático comum, ou seja, daquele crime que pode ser cometido independentemente do uso do meio informático e contra bens jurídicos tutelados pelo ordenamento penal.

Nesses casos, a internet é utilizada como uma ferramenta bastante eficaz de propagação de informações não autorizadas, em escala global, o que torna ainda mais danoso o delito cometido nesse ambiente. Dessa forma, a violação da privacidade no meio desmaterializado, na maioria dos casos, ocorre quando informações íntimas ou pessoais do usuário passam a ser difundidas, de forma não autorizada, geralmente por um *hacker* ou por pessoa mal intencionada, para conhecimento de todas as pessoas que tenham acesso a rede mundial de computadores.

No que se refere à ofensa ao nome, destaca-se a proteção dispensada à personalidade jurídica da pessoa, tendo em vista que o nome consiste na exteriorização da personalidade humana no meio social e familiar. O nome é protegido pelo ordenamento jurídico contra abusos de terceiros que o exponham ao ridículo. A internet pode funcionar como ferramenta bastante eficiente nessa prática delituosa, tomando por base o seu caráter disseminador de informações.

A ofensa à imagem pode ser configurada, por exemplo, numa situação em que um indivíduo venha a expor uma fotografia de um terceiro, sem o seu consentimento, com objetivo de difundir fato pessoal perante a sociedade. A proteção à imagem está respaldada constitucionalmente, prevendo-se indenização pelo dano moral ou material decorrente da sua violação.

Aduz o Art. 5º, X, da Constituição Federal de 1988: "São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação".

A questão reside na adequação do direito de liberdade de informação em conformidade com o direito à privacidade, ambos constitucionalmente protegidos. No

exercício de um direito, o indivíduo não pode agir de forma a prejudicar terceiros, sob pena de ser responsabilizado pelos danos que vier a causar com a sua conduta.

É também objeto de atenção pelo direito, a proteção dispensada ao *Software* (programa de computador). Nesse aspecto, já existe lei que regula a matéria, a Lei nº. 9.609/98 trata da proteção aos programas de computador, da mesma forma que tutela as obras literárias, observadas as particularidades do caso concreto. No mesmo sentido, a lei 9.610/98 que dispõe sobre os direitos autorais, dispensando igual proteção aos programas de computador.

No tocante aos contratos informáticos, ressalta-se a diferença existente entre esses e os contratos comuns, realizados pela rede. Contratos informáticos são aqueles que têm por objeto um bem ou um serviço informático, qualquer que seja como base de dados, programas, serviços de manutenção de redes, serviços de segurança informática, dentre outros. Como exemplo de contratos informáticos, pode-se mencionar o contrato de acesso à internet, entre usuário e provedor de acesso, contrato de desenho e desenvolvimento de páginas na rede (*webdesigners)* e contratos de hospedagem de sites na rede.

Em relação aos contratos comuns, previstos na legislação civil, celebrados por meio eletrônico, estes não perdem suas características intrínsecas pelo motivo de serem realizados de forma diversa da comumente celebrada, ou seja, aperfeiçoados mediante o uso da informática.

Dessa forma, um contrato de compra e venda será o mesmo, guardará sempre suas peculiaridades, seja qual for a forma de celebração, se ele vai ser feito em papel ou se vai ser inovado com a utilização de programas de computador, através da assinatura digital.

Na melhor técnica jurídica, para definição e diferenciação dos contratos informáticos, os contratos usuais, realizados com recursos informáticos, guardarão suas características, como por exemplo, contrato de locação, de compra e venda, de prestação de serviços, serão sempre assim denominados, independente da forma como serão celebrados.

A responsabilidade civil, apurada nas condutas praticadas no ambiente virtual, será sempre configurada, da mesma forma que no meio materializado, aplicando-se as mesmas regras contidas no Código Civil de 2002. O fato de uma conduta, prejudicial ao interesse de terceiro, ser realizada por intermédio do computador

conectado a rede, não exclui a responsabilidade do indivíduo em indenizar outrem pelos danos indevidamente suportados.

A responsabilidade civil, derivada do uso de novas tecnologias, sempre que possível, será configurada. No entanto, encontrará o indivíduo prejudicado, em face da conduta danosa aos seus interesses, as mesmas dificuldades encontradas pela justiça penal, na identificação da autoria do delinquente, em virtude da facilidade de acesso, do anonimato e pelo pouco controle na rede mundial por parte dos provedores de acesso, dentre outros aspectos.

Por fim, questão preocupante para o direito da informática diz respeito aos crimes digitais. Nesse aspecto, nota-se a grande aproximação desta disciplina com o direito penal, ramo jurídico encarregado de tutelar os bens jurídicos de maior relevância na sociedade.

A preocupação com o fenômeno da criminalidade na internet é de interesse de todos os povos civilizados, tendo em vista o caráter internacional de relações humanas viabilizadas na rede mundial.

3.4 Ciberdelinquentes e Ciberterroristas

Os chamados ciberdelinquentes são indivíduos que buscam o profundo conhecimento técnico para executar atividades ilícitas, sobretudo no ciberespaço. Os *hackers* e *crackers* são espécies do gênero. A distinção entre os ambos reside no fato de que os *hackers* entram e saem dos sistemas invadidos sem deixarem vestígios nem prejuízos materiais ou imateriais, ao contrário dos *crackers* que fazem questão de serem notados, provocando diversos danos.

Os *Hackers,* em princípio, não são criminosos. São especialistas em informática que procuram defeitos nos sistemas operacionais e programas, e quando os descobrem, comunicam aos fabricantes e a toda a comunidade interessada, através de informativos periódicos, lista de discussão, etc. São indivíduos com grande habilidade e conhecimento de informática e podem utilizar seus conhecimentos na área para atividades lícitas ou para atividades criminosas, em especial a invasão de sistemas de computadores, criação de vírus, etc.

Os *Crackers* são os criminosos mais temidos da rede, pois são movidos por fama e dinheiro, procuram brechas na segurança das redes para se apoderar e violar sites, tipos de sistemas, invadindo computadores em rede e programas, quebrando proteção de *softwares.*

Por sua vez, os ciberterroristas são desenvolvedores de vírus, *worms, trojans* (softwares que causam danos aos arquivos e programas dos usuários), são criadores de programas prejudiciais ao sistema informático.

As duas modalidades de agente repercutem de forma negativa em esfera mundial.

3.4.1 Ataques em rede

Em sede de segurança, os ataques em rede são implementados por indivíduos mal intencionados denominados *crackers*.

Pode-se, dessa maneira, dividir a segurança como: ataques em rede e suas formas; e ameaças à segurança, levando em consideração, quanto a essas últimas, os ataques mais sofisticados e perigosos, que causam a vulnerabilidade dos sistemas. Citem-se como exemplos: roubo, destruição, deturpação, modificação de informações, interrupção de serviços, vírus, divulgação de senhas, acessos indevidos, além da atuação dos *hackers*, que embora não dolosamente violem as barreiras de privacidade alheia, utilizam de suas habilidades, muitas vezes de forma abusiva, ultrapassando os limites da legalidade pelo mero prazer em ter posto em prática os conhecimentos, em detrimento das vítimas que, em boa parte, possuem o mínimo de conhecimento na área, fato que as tornam alvos indefesos.

3.4.2. Formas de ataque

Por variadas formas de ataque se utilizam os delinquentes virtuais para o cometimento de crimes, devido à grande criatividade e mutação nas suas condutas.

As formas mais comuns utilizadas por esses indivíduos para o cometimento de delitos serão adiante elencadas.

Os Vírus são programas ou fragmentos de código parasita, requerem um hospedeiro para funcionar, da mesma forma de um vírus biológico que ataca um ser humano. São os mais conhecidos no meio informático e suas consequências são desastrosas nos computadores e sistemas.

As principais formas de propagação desses códigos maliciosos são através de infecção de outros programas, pelo envio de programas infectados por e-mail mal intencionado, enviado a correios eletrônicos.

Uma definição mais técnica, no que concerne aos vírus de computador, pode-se extrair das palavras de Vasconcelos *apud* Concerino (2001, p.136):

> Um vírus é um programa escrito em linguagem de programação, que faz a contaminação de outros programas do computador através de sua modificação de forma a incluir uma cópia de si mesmo. A denominação vírus vem de uma analogia com o vírus biológico, que transforma a célula numa fábrica de cópias. O vírus pode ser descrito como um programa altamente sofisticado, capaz de tomar decisões automaticamente, funcionar em diferentes tipos de computador, e apresentar um baixo índice de problemas ou *bugs*. Sendo um programa de computador sofisticado, que usa técnicas de inteligência artificial, ele obedece a um conjunto de instruções contidas em seu código, algumas com datas específicas a serem ativadas. Tem capacidade de se replicar e se alojar em outros programas ou arquivos, resultando na realização de ações não solicitadas, destruindo arquivos do sistema e corrompendo dados. Por sua invisibilidade e forma furtiva de imiscuir nos sistemas e também pelo prejuízo que são capazes de causar, receberam oficialmente o nome de "vírus".

Os vírus podem residir na memória, vírus de *boot*, vírus de programas, etc. Ele é um tipo de código malicioso que apresenta um comportamento inesperado, grande responsável por problemas nos sistemas de informática.

Os Vermes, também chamados *Worms*, são programas independentes que tem como objetivo infectar sistemas em rede e propagar-se de forma muito rápida, prejudicando milhares de sistemas em pouco tempo.

A Engenharia Social é uma forma de ataque que consiste em usar métodos não técnicos para obter acessos a um sistema e roubar informações sigilosas, ou convencer a vítima a executar ações indevidas e perigosas, tendo como métodos típicos conversas por telefone ou correio eletrônico.

A Quebra de senhas tem por objetivo descobrir a senha de algum usuário/recurso através de tentativas sobre várias possibilidades de senhas; existem

vários programas "quebra-senhas" (*crackers*) disponíveis para a maioria dos sistemas operacionais.

A Interrupção de Serviço é modalidade de ataque que consiste em derrubar a máquina servidora, de forma a gerar uma indisponibilidade geral de um serviço.

O *spam* é a mensagem não solicitada enviada através dos serviços de correio eletrônico. São os e-mails indesejados que, muitas vezes, trazem em seu conteúdo algum código malicioso e que, uma vez aberta a mensagem, o sistema será infectado e tornar-se-á vulnerável.

O Código malicioso é o gênero, abrange todo programa que apresenta um comportamento inesperado, tendo-se como exemplos: vírus, vermes, cavalos de tróia, *back-doors*, bombas lógicas.

O Cavalo de Tróia é o programa maléfico que se esconde dentro de outros programas ou se disfarça de programas legítimos para atacar os sistemas. Tem como característica marcante em relação aos demais o fato de não se propagar para outros sistemas, mas é altamente maléfico ao computador alvo.

A Bomba lógica é o programa ou fragmento de programa malicioso ativado por determinada condição lógica.

A Varredura é a forma de ataque comum de *hackers* para reconhecimento de sistemas informáticos, como forma de conhecê-lo melhor.

Spoofing é a forma delituosa consistente na falsificação de identidade de um usuário, também potencialmente danosa, tendo em vista que o delinquente com essa prática, visa o anonimato, dificultando a sua identificação.

Sniffing é o ataque por monitoramento, ou seja, é a forma de ataque que consiste no monitoramento de pacotes transitando em redes; um programa *sniffer* pode monitorar endereços IP, senhas, etc.; a utilização de programas *sniffer* é difícil de ser detectada, dificultando o trabalho da polícia.

Back doors ou *trap doors* consistem em pontos de entrada secretos que podem ser explorados para ganhar acesso a um sistema; este tipo de código malicioso pode ser criado pelo projetista do sistema ou introduzido por terceiros para permitir acesso privilegiado a alguém. São portas de entrada ocultas, consistindo numa vulnerabilidade do sistema.

Portanto, após o breve e importante conhecimento acerca das modalidades e formas de ataque em rede, passa-se à análise do tratamento legislativo frente aos problemas suscitados nesse trabalho.

4 DO TRATAMENTO LEGISLATIVO E FORMA DE CONTROLE

4.1 Da Tutela Jurisdicional

Pertence ao Estado, detentor do monopólio da aplicação da lei penal, o direito de punir (*jus puniendi),* de forma a assegurar a ordem e o bem estar social, por meio da proteção dos bens jurídicos mais relevantes. Contudo, esse poder é limitado, devido à existência de princípios, tais como o da legalidade, que norteiam a sua atuação, objetivando preservar o direito de liberdade do cidadão, direito humano fundamental.

Diante do quadro de aumento da criminalidade no meio virtual, do atraso da justiça brasileira em face dessa nova realidade surgida, tendo em vista a ausência de mecanismos reguladores e repressivos eficientes em relação aos crimes digitais, no ambiente desmaterializado impera a ideia de impunidade e a sociedade exige providências rápidas e eficazes.

A criação de uma legislação penal específica para proteção dos bens informáticos e outros igualmente importantes, constitui medida indispensável, sendo de essencial relevância para que tais bens jurídicos sejam resguardados pelo Estado, através da eficiente prestação da tutela jurisdicional.

Para alguns conflitos cibernéticos, nada impede que seja plenamente possível a aplicação da legislação infraconstitucional existente, tomando por base a Constituição Federal, o Código de Defesa do Consumidor, o Código Civil, a Lei dos Direitos Autorais, Lei do Software e bem como do Código Penal vigente. Entretanto, não é cautelosa essa aplicação em todos os casos, principalmente em se tratando da esfera penal, no que se refere às condutas não tipificadas.

A questão não é de fácil solução, pelo fato de existirem vários fatores que dificultam a persecução penal desses criminosos, levando-se em conta que tais delitos provocam efeitos transnacionais, o que a doutrina convencionou chamar de crimes à distância. Do mesmo modo, tem-se a problemática da falta de segurança dos sistemas e a dificuldade na identificação da autoria, a facilidade de acesso, a deficiência de órgãos policiais, devendo-se ressalvar a atuação das Delegacias Especializadas existentes no País, ainda poucas para reprimir a crescente atuação

criminosa, mas constituindo iniciativa louvável que permite maior investigação de tais casos.

Estabelece a Constituição Federal, em seu art. 5º, inciso XXXV: "A lei não excluirá da apreciação do Poder Judiciário lesão ou ameaça a direito".

Conforme visto, a Carta Magna trata da questão objeto do presente estudo, ainda que de forma geral, restando ao ordenamento infraconstitucional normatizar o espaço virtual de relações humanas, tendo em vista o aumento exponencial de lesões aos direitos.

Quando não for possível a resolução por outros ramos do direito, caberão ao Direito Penal as questões envolvendo os conflitos surgidos nesse meio, observados os princípios delineadores da atuação do Estado.

Dessa maneira, tais fatos não podem ficar afastados de apreciação do Poder Judiciário, bem como tais condutas devem ser objeto de tipificação legal, por meio da inovação legislativa, no tocante à criação de uma lei específica que aborde essa nova demanda, em atendimento ao princípio da reserva legal, já mencionado anteriormente.

4.2 Da Lei Penal no Espaço e a Fixação da Competência

A Internet não constitui fenômeno restrito apenas a um país. Ao contrário, desde seu advento, assumiu uma postura muito diversa da pretensão dos seus criadores, interligando pessoas de diversas partes do mundo. Do seu nascimento até os dias atuais, disseminou-se rapidamente, atingindo em poucos anos um grande número de países, e hodiernamente presente na quase totalidade do globo terrestre.

As nações alcançadas pela rede mundial possuem jurisdições diferentes, de forma que a internet não reside especificamente em país nenhum que possa controlá-la de uma forma juridicamente homogênea. Por tal motivo, surgem importantes questões como da possibilidade de determinado país combater um determinado crime e outro não, e também no que concerne à fixação da competência em relação a um crime praticado em determinado lugar e obtido resultado em outro, com legislação totalmente diversa.

No tocante à lei penal, sabe-se que esta é elaborada para viger dentro dos limites em que o Estado exerce sua soberania. Sendo assim, como cada Estado é soberano dentro de seus limites territoriais, surge a questão da fixação da competência em razão da delimitação espacial no âmbito da eficácia da legislação penal, que é matéria de Direito Penal Internacional.

Existem alguns princípios norteadores da atividade punitiva do Estado, enfatizando-se o princípio da territorialidade, consagrado no art. 5º do Código Penal de 1940: "Aplica-se a lei brasileira, sem prejuízo de convenções, tratados e regras de direito internacional, ao crime cometido no território nacional".

Em relação ao lugar do crime, o Código Penal, em seu art.6º, adota a teoria da ubiquidade, onde estabelece: "Considera-se praticado o crime no lugar em que ocorreu a ação ou omissão, no todo ou em parte, bem como onde se produziu ou deveria produzir-se o resultado".

Assim, para a efetiva aplicação do princípio da territorialidade, nos chamados crimes à distância ou transnacionais, é preciso que se defina exatamente em que lugar se consumou a infração. Desse modo, ao contrário do Código Penal com a teoria da ubiqüidade (art. 6º), o Código de Processo Penal, em seu art. 70, adotou, para fixação da competência, a teoria do resultado ao estabelecer que: "A competência será, de regra, determinada pelo lugar em que se consumou a infração, ou, no caso de tentativa, pelo lugar em que foi praticado o último ato de execução".

Dessa forma, como punir uma conduta praticada em lugar onde não seja prevista como crime, sendo tal conduta efetivada com auxílio de um computador conectado a internet? Para muitos doutrinadores, a questão seria resolvida na adoção do direito penal internacional, através da estipulação de tratados e acordos internacionais entre os países. Dessa forma, ficaria o tribunal penal internacional competente para dirimir os conflitos envolvendo crimes de internet, em face do seu caráter transnacional, ou seja, os crimes à distância.

Essa linha de pensamento visa evitar a impunidade de tais delitos, no aspecto territorial, uma vez que tais ilícitos são cometidos de um país e consumados em outro, no qual inexista legislação punitiva para aquela determinada conduta.

Na realidade, é medida de difícil implementação, tendo em vista os problemas sempre existentes em matéria de direito internacional, como a relativização da soberania dos estados signatários, em face da atuação do tribunal penal internacional e também pelo fato de que os crimes de internet atingem todo o globo

terrestre, e nem todos os países iriam ratificar o referido acordo, assim como se verifica em matéria de proteção ao meio ambiente.

4.3 Tratamento Legal

A questão da ilicitude na informática é tratada como um grande problema da atualidade. É na Constituição Federal de 1988 que se encontra prevista competência privativa da União para legislar sobre a matéria, em seu art. 22, inciso IV.

Até então, sobre informática, temos poucas leis, como a de proteção ao *software* e sobre direitos autorais. No que se refere à parte especial do Código Penal de 1940, em poucas situações podemos enquadrar condutas às figuras tipificadas.

Ao contrário de vários países como Estados Unidos, Portugal e outros países da Europa, onde seguiram o posicionamento ontológico, brevemente esboçado no início deste trabalho, no Brasil não há nenhuma legislação penal ou processual penal específica sobre o tema, existindo apenas propostas de regulamentação a seguir explanadas.

4.4 Projetos de Lei Existentes no País

Inúmeros projetos de lei tramitam em nossas casas legislativas, mas nenhum até agora foi transformado em lei, pois boa parte encontra-se arquivado.

Os crimes de informática devem classificados de maneira específica, de forma que os nossos legisladores possam elaborar normas eficientes que regulem de forma adequada o ambiente digital.

Alguns projetos de lei (PL) merecem destaque no Brasil, como: PL 1.806/99, o PL 84/99 e o PL 1.713/96. Todos com influência no direito estrangeiro, em especial no norte-americano e no português, apresentando propostas para regulamentação do ciberespaço.

Acerca desses projetos em trâmite no Congresso Nacional, faz-se necessária uma breve análise.

4.4.1 Projeto de lei nº 1.806/99

O PL nº 1.806/99 tem como autor o Deputado Freire Júnior e, ao tratar da questão, o faz de forma restrita, isto é, refere-se exclusivamente ao crime de furto no sistema informático. Apresenta em sua redação a previsão para o acréscimo de dois incisos ao parágrafo 3º do artigo 155 do Código Penal.

De tal maneira, para fins de persecução penal, as condutas de acesso aos serviços de comunicação e aos sistemas de armazenamento, manipulação ou transferência de dados eletrônicos, de acordo com esse projeto, seriam equiparadas à coisa alheia móvel, ao lado da energia elétrica, assim possibilitando a punição desses infratores, sem necessidade de se aplicar a interpretação analógica que, como é cediço, é vedada em desfavor do réu.

Em análise textual ao referido projeto de lei, verifica-se uma impropriedade, que é a de assemelhar, por exemplo, o *acesso* à coisa móvel. Nota-se claramente a diferença entre ambos, uma vez que coisa móvel é algo corpóreo, material e não algo imaterial como o acesso, derivado do verbo acessar. Portanto, uma ação ou conduta de acessar determinado sistema não configura uma coisa móvel, pois não se trata de algo materializado. Quando alguém furta, o faz em relação a dados informáticos em si e não ao acesso.

Cumpre ressaltar, então, que tal projeto já é um avanço em relação à nossa legislação vigente. Entretanto, apresenta-se falho e provavelmente não será transformado em lei.

4.4.2 Projeto de lei nº 84/99

No que pertine ao projeto de lei 84/99, que tem como autor o Deputado Luiz Piauhylino, percebe-se um avanço substancial em relação ao do Deputado Freire Júnior, pelo fato de apresentar uma abordagem mais adequada à problemática dos crimes digitais, da fixação de penalidades e outras providências no sentido.

Prevê o referido projeto sete novos tipos penais, tendo como objetivo atualizar a legislação vigente, de forma a suprir as lacunas do atual código penal, prevendo penalidades que podem chegar até 6 (seis) anos de reclusão e multa.

Tendo em vista uma melhor regulamentação legal do ambiente virtual de relações humanas e inspirado no adequado funcionamento dos computadores e redes, o autor tratou de tipificar algumas condutas não admissíveis nesse meio, fixando penalidades em caso de violação da norma.

Esse projeto objetiva fixar a responsabilidade de certos indivíduos, encarregados desde o acesso indevido a computadores públicos ou privados, até a interceptação de dados, informações pessoais, dentre outras práticas.

Em suma, pode-se destacar como principal meta a ser alcançada por esse projeto, no caso de conversão em lei, a tipificação e punição de novas condutas potencialmente danosas ao uso regular da rede e do computador, ainda não previstas em nossa legislação penal como crimes, em sentido técnico, sem implicar prejuízo na cominação legal já prevista em outros diplomas legais.

Na análise do citado projeto, é relevante a observância ao art. 1º, tendo em vista ser ele incumbido de fixar o panorama geral sobre a questão, uma vez que este é o responsável pela elaboração de diretrizes básicas relativas à prestação de serviços por redes integradas de computadores. Aduz o Art. 1º do Projeto de Lei nº 84/99:

> O acesso, o tratamento e a disseminação de informações através das redes de computadores devem estar a serviço do cidadão e da sociedade, respeitados os critérios de garantia dos direitos individuais e coletivos e da privacidade e segurança de pessoas físicas e jurídicas e da garantia de acesso às informações disseminadas pelos serviços de rede.

Nota-se a proteção dispensada aos bens informáticos, redes, informações e dados, na categoria de bens coletivos, assim como da abordagem da questão da segurança e privacidade, de forma inovadora em nosso ordenamento.

Tal projeto de lei reserva um capítulo específico para tratar dos crimes de informática, prevendo sete novos tipos penais e as respectivas penas, fazendo com que sejam elevados os bens informáticos à categoria de bens jurídicos relevantes, consequentemente, oferecendo a eficiente tutela jurídica da qual se necessita.

O PL nº 84/99, desde sua proposição, tramitou por diversas comissões na Câmara dos Deputados, a exemplo da Comissão de Segurança Pública e Combate

ao Crime Organizado (CSPCCO) e da Comissão de Constituição, Justiça e Cidadania (CCJC), na qual, no primeiro trimestre de 2009, obteve parecer do relator, o Deputado Régis de Oliveira (PSC-SP), pela constitucionalidade, juridicidade e técnica legislativa, e no mérito, pela aprovação.

Resta à sociedade aguardar pelos trâmites legais e pela vontade política para vislumbrar a tão desejada segurança jurídica em sede de criminalidade digital.

4.4.3 Projeto de lei nº 1.713/96

Em relação ao PL 1.713/96, de autoria de Cássio Cunha Lima, faz-se a uma breve análise. Nesse projeto, dispõe-se sobre o acesso, a prestação de serviços na internet, a responsabilidade pelos ilícitos e dos crimes cometidos na rede. Trata-se do primeiro projeto de lei que objetiva oferecer uma proposta legal para a regulamentação do espaço virtual, abordando de maneira eficiente a questão dos crimes em rede.

Esse projeto apresenta tipos penais já existentes no atual código, buscando nesses tipos aplicar as especificidades das condutas inovadas com auxílio de meios informáticos, como do estelionato, violação de correspondência, a falsidade documental, a divulgação de segredo, dentre outros ilícitos oriundos do uso irregular da rede.

Tal projeto dispensou atenção peculiar aos dados informáticos e informações que percorrem a rede mundial de computadores, como bens individuais e coletivos merecedores de proteção pelo direito, o que não poderia ser diferente em face do atual estágio de evolução da sociedade.

Atualmente, este projeto encontra-se arquivado, após tramitar pela Comissão de Ciência e Tecnologia, Comunicação e Informática, e teve como relator o deputado Luiz Piauhylino que apresentou seu projeto nº 84/99, como substituto para o mesmo.

Ante o exposto, a sociedade aguarda pela atenção do Poder Legislativo no sentido de regulamentar de forma definitiva o meio virtual, buscando dar seguimento ao andamento de bons projetos, como o PL n° 84/99, no sentido de aprovar uma lei específica, retificando o que julgarem pertinente nas referidas propostas.

A situação atual gera insegurança jurídica, bem como um mal estar social em virtude do sentimento de impunidade predominante no ambiente da internet.

Faz-se necessária não só a edição de leis rígidas, como também deve estar preparado o ente estatal para atendimento dessa nova demanda, com aperfeiçoamento dos setores especializados da polícia judiciária, o que já vem ocorrendo com as Delegacias Especializadas, com profissionais bem preparados e nível de conhecimento comparado ao dos *hackers*.

Da mesma forma, os usuários da rede devem ser mais instruídos no sentido de adotar as medidas de segurança necessárias contra ataques.

E, por fim, a responsabilização dos provedores de acesso no gerenciamento de seus clientes, adotando medidas repressivas a práticas abusivas no meio digital.

4.4.4 Legislações estrangeiras e a era digital

Em comparação com o tratamento dispensado aos crimes digitais no Brasil, diversos países encontram-se em fase avançada no que concerne a essa temática, possuindo legislação específica para a matéria.

A Inglaterra, Estados Unidos e Portugal são nações que já possuem uma legislação específica sobre o tema, possibilitando a atuação mais precisa do judiciário na punição desses delitos, estando a legislação lusitana em anexo deste trabalho.

Dessa forma, tem-se o entendimento de que não se pretende um amontoado de leis sem aplicação, mas sim, uma legislação pertinente e em consonância com as consequências trazidas pelos crimes virtuais, a exemplo de tais nações. Só assim poderemos alcançar os anseios sociais de justiça e segurança jurídica, através da elaboração de uma lei específica que regulamente essa situação, para minimizar a impunidade no âmbito da rede mundial de computadores.

5 CONCLUSÃO

A população mundial presencia a expansão de um fenômeno que modificou a forma de interação entre os povos, diminuiu as distâncias e tornou rápida a disseminação de informações em todo o globo terrestre. Tal acontecimento constitui no advento da internet.

O mundo globalizado faz uso dessa ferramenta, o que a torna indispensável em diversos setores, sendo primordial ao desenvolvimento econômico, social e político.

São inúmeros os benefícios advindos da informatização, ao passo que se podem realizar os mais variados atos da vida civil por meio do computador, a exemplo de movimentações bancárias, ensino à distância, contratos de compra e venda, divulgação publicitária, pesquisa bibliográfica, acesso à informação em tempo real, dentre a infinidade de serviços prestados pela rede.

O número de usuários aumenta intensamente, tendo em vista o apoio governamental em projetos de inclusão digital, fazendo com que a informática alcance pessoas de camadas sociais menos favorecidas, o que demonstra cumprir com sua responsabilidade social, diminuindo as desigualdades.

Diante desse novo mundo, em detrimento às mencionadas vantagens, emergem as notórias consequências advindas da má fé de determinados indivíduos, os quais transformam o meio virtual em um ambiente propício à prática de crimes contra a honra, a vida, a imagem das pessoas, dentre outras condutas reprimíveis.

Além da prática de crimes já tipificados na lei penal vigente, há crimes contra a rede de informações e contra o próprio computador, condutas não abrangidas na legislação, ocasionando a omissão quanto à matéria e, dessa forma, estimulando a atuação delituosa em rede, tendo o infrator aliados como o anonimato e a dificuldade de investigação do caso, como o que se explanou neste trabalho, gerando graves prejuízos incalculáveis às vítimas.

A atuação dos deliquentes pode transpor as fronteiras nacionais, denominados delitos transnacionais, isto é, em diversos casos, o prejuízo é suportado em outro país, o que, de certa maneira, representa estímulo à prática criminosa.

Diante desse quadro, surge a necessidade de intervenção do Estado por meio da inovação legislativa, editando leis que venham a prevenir e reprimir tais atitudes abusivas.

Constitui medida inicial a edição de lei específica sobre a matéria, sendo indispensável à regulamentação do uso do computador e da internet no Brasil, de forma que a falta de previsão legal para enquadramento de determinadas condutas delituosas obsta todo o processo de persecução penal do infrator digital, tendo em vista que a atual legislação não é capaz de suprir as demandas atuais, devendo haver intervenção do Estado de forma eficiente, com o intuito de regular as relações oriundas dessa nova conjuntura.

Apesar de se tratar de fenômeno recente, vários países já tem se manifestado no sentido de criar normas que regulem o uso da rede e do computador, ao determinar penalidades para aqueles que ultrapassem os limites previamente estabelecidos, atingindo bens jurídicos, inclusive bens informáticos relevantes, e de maneira a protegê-los.

Por seu turno, no Brasil, algumas atitudes vem sendo tomadas, mesmo que de forma primitiva, como a formulação de alguns projetos de lei, na maioria inspirados na legislação estrangeira. Tais projetos se encontram no Congresso Nacional e apresentam-se como propostas para regulamentação do espaço virtual, no qual predomina um sentimento de impunidade, em face da ausência de tratamento legal específico, conjugados com outros fatores, como das dificuldades encontradas pela polícia na identificação da autoria e materialidade do crime, bem como do enquadramento, na atual legislação, desses novos delitos.

Faz-se necessária a ação por parte dos legisladores pátrios, na criação de uma lei especial, bem como na existência de uma polícia eficiente e bem aparelhada, capaz de prevenir, repreender e desestimular a prática de condutas delituosas cometidas no meio virtual, para que esse espaço não venha a ser tido como um território sem lei, onde predomina a impunidade.

Desse modo, há uma deficiência legislativa que acarreta consequências desastrosas, tendo em vista que impede a atuação eficiente do Poder Judiciário e do Ministério Público, em face da ausência de previsão legal para condutas não determinadas em lei como criminosas, ou seja, não tipificadas, já que o Código Penal veda a interpretação analógica, respaldando-se na própria Constituição Federal de 1988.

Sobretudo, é preciso atenção para essa nova realidade no meio virtual, expandindo e aperfeiçoando os setores da polícia encarregados na prevenção e combate a esses crimes, uma maior participação do Ministério Público, mais orientação por parte dos usuários e uma efetiva cobrança por segurança aos provedores e servidores de internet, entendendo-se, assim, que apenas uma lei, de forma isolada, não resolveria a questão, sendo imperiosa a junção de várias medidas.

Diante de todo o exposto neste trabalho, aguarda o cidadão pela atitude do Poder Legislativo em impulsionar os projetos existentes para sua futura aprovação e aplicação, reprimindo práticas abusivas que ocorrem no meio virtual, pois, diferentemente do meio, as consequências são lamentavelmente reais.

REFERÊNCIAS

BITENCOURT, Cezar Roberto. *Tratado de direito penal*: parte geral. V. 1. 11. ed. atual. São Paulo: Saraiva, 2007.

BRASIL, Câmara Federal. Projeto de Lei n° 84/99. *Dispõe sobre os crimes cometidos na área da informática, suas penalidades e dá outras providências.* Disponível em: <http://www.camara.gov.br/sileg/Prop_Detalhe.asp?id=15028>. Acesso em: 22.set.2009.

_____. *Constituição da República Federativa do Brasil*, 05 de outubro de 1988. *Diário Oficial da União*. Brasília, 05.out.1988.

_____. Decreto-lei n° 2.848, de 07 de dezembro de 1940. *Código Penal*. In: vade mecum. 7. ed. São Paulo: Saraiva, 2009.

_____. Decreto-lei n° 3.689, de 03 de outubro de 1941. *Código de Processo Penal*. In: vade mecum. 7. ed. São Paulo: Saraiva, 2009.

_____. Decreto-lei n° 3.914, de 09 de dezembro de 1941. *Lei de Introdução do Código Penal*. In: vade mecum. 7. ed. São Paulo: Saraiva, 2009.

_____. Decreto-lei n° 3.914, de 09 de dezembro de 1941. *Lei de contravenções penais*. In: vade mecum. 7. ed. São Paulo: Saraiva, 2009.

BRITO, Dante Ponte de. *A Publicidade na Internet e @ Violação dos Direitos do Consumidor.* Parnaíba: A3 Gráfica, 2009.

CAPEZ, Fernando. *Curso de Direito Penal: parte especial*. V. 2. 2. ed. São Paulo: Saraiva, 2005.

CASTELLS, Manuel. *A galáxia internet*. Lisboa: Fundação Calouste Gulbenkian, 2004.

CONCERINO, Arthur José. *Internet e segurança são compatíveis?*. Arthur José Concerino. Newton de Lucca e Adalberto Simão Filho. *Direito & Internet*: aspectos jurídicos relevantes. Bauru: Edipro, 2001.

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

FERREIRA, Ivete Senise. *A criminalidade Informática.* In: Direito & Internet: aspectos jurídicos relevantes. Bauru: Edipro, 2001.

GRECO, Marco Aurélio [et al]. *Direito e internet: Relações jurídicas na sociedade informatizada.* São Paulo: Revista dos Tribunais, 2001.

LUCCA, Newton de; SIMÃO FILHO, Adalberto (coord.). In: *Direito & Internet: aspectos jurídicos relevantes.* Bauru: Edipro, 2000.

MORAES, Alexandre de. *Direito Constitucional.* 13. ed. São Paulo: Atlas, 2003.

PAESANI, Liliana Minardi. *Direito e internet: liberdade de informação, privacidade e responsabilidade civil.* São Paulo: Atlas, 2000.

PORTUGAL, ASSEMBLEIA DA REPÚBLICA. *Lei nº 109/91 - Sobre a criminalidade informática.* Disponível em: <http://www.cnpd.pt/bin/legis/nacional/lei_10991.htm>. Acesso em: 22.set.2009.

SAFERNET BRASIL. *Acordo do MPF-SP com a Google já gerou mais de 1200 quebras telemáticas*. Disponível em: <http://www.safernet.org.br/site/noticias/acordo-mpf-sp-com-google-já-gerou-mais-1200-quebras-telemáticas>. Acesso em: 15.set.2009.

VASCONCELOS, Fernando Antônio de. *Internet: responsabilidade do provedor pelos danos praticados.* Curitiba: Juruá, 2003.

ANEXO A

PROJETO DE LEI Nº 84, DE 1999.

O Congresso Nacional decreta:

CAPÍTULO I

DOS PRINCÍPIOS QUE REGULAM A PRESTAÇÃO DE SERVIÇO POR REDES DE COMPUTADORES

Artigo 1º. O acesso o processamento e a disseminação de informações através das redes de computadores deve estar a serviço do cidadão e da sociedade, respeitados os critérios de garantia dos direitos individuais e coletivos e de privacidade e segurança de pessoas físicas e jurídicas e da garantia de acesso às informações disseminadas pelos serviços da rede.
Artigo 2º. É livre a estruturação e o funcionamento das redes de computadores e seus serviços, ressalvadas as disposições especificas reguladas em lei.

CAPÍTULO II

DO USO DE INFORMAÇÕES DISPONÍVEIS EM COMPUTADORES OU REDES DE COMPUTADORES

Artigo 3º. Para fins desta lei, entende-se por informações privadas aquelas relativas a pessoa física ou jurídica identificada ou identificável.
Parágrafo único: é identificável a pessoa cuja individuação não envolva custos ou prazos desproporcionados.

Artigo 4º. Ninguém será obrigado a fornecer informações sobre sua pessoa ou de terceiros, salvo nos casos previstos em lei.

Artigo 5º. A coleta, o processamento e a distribuição, com finalidades comerciais, de informações privadas ficam sujeitas à prévia aquiescência da pessoa a que se referem, que poderá ser tornada sem efeito a qualquer momento, ressalvando-se o pagamento de indenizações a terceiros, quando couberem.
§ 1º. A toda pessoa cadastrada. Dar-se-á conhecimento das informações privadas armazenadas e das respectivas fontes.
§ 2º. Fica assegurado o direito a retificação de qualquer informação privada incorreta.
§ 3º. Salvo por disposição legal ou determinação judicial em contrário, nenhuma informação privada será mantida à revelia da pessoa a que se refere ou além do tempo previsto para a sua validade.
§ 4º. Qualquer pessoa, física ou jurídica, tem o direto de interpelar o proprietário de rede de computadores ou provedor de serviço para saber se mantém informações a seu respeito, e o respeito do teor.

Artigo 6º. Os serviços de informações ou de acesso a bancos de dados não distribuirão informações privadas referentes, direta ou indiretamente, a origem racial, opinião política, filosófica, religiosa ou de orientação sexual, e de filiação a qualquer entidade pública ou privada, salvo autorização expressa do interessado.

Artigo 7º. O acesso de terceiros, não autorizados pelos respectivos interessados, a informações privadas mantidas em redes de computadores dependerá de prévia autorização judicial.

CAPÍTULO III

DOS CRIMES DE INFORMÁTICA

Seção I

DANO A DADO OU PROGRAMA DE COMPUTADOR

Artigo 8º. Apagar, destruir, modificar ou de qualquer forma inutilizar, total ou parcialmente, dado ou programa de computador, de forma indevida ou não autorizada.
Pena: detenção de um a três anos e multa.
Parágrafo único: se o crime é cometido:
1 - contra o interesse da união, estado, distrito federal, município, órgão ou entidade da administração direta ou indireta ou de empresa concessionária de serviços públicos,
2 - com considerável prejuízo para a vítima;
3 - com intuito de lucro ou vantagem de qualquer espécie, própria ou de terceiro;
4 - com abuso de confiança;
5 - por motivo fútil;
6 - com o uso indevido de senha ou processo de identificação de terceiro; ou
7 - com a utilização de qualquer outro meio fraudulento.
Pena: detenção, de dois a quatro anos e multa.

Seção II

ACESSO INDEVIDO OU NÃO AUTORIZADO

Artigo 9º. Obter acesso, indevido ou não autorizado, a computador ou rede de computadores.
Pena: detenção, de seis meses a um ano e multa.
Parágrafo primeiro. Na mesma pana incorre quem, sem autorização ou indevidamente, obtém, mantém ou fornece a terceiro qualquer meio de identificação ou acesso a computador ou rede de computadores.
Parágrafo segundo. Se o crime é cometido;
1 - com acesso a computador ou rede de computadores da união, estado, distrito federal, município, órgão ou entidade da administração direta ou indireta ou de empresa concessionária de serviços públicos;
2 - com considerável prejuízo para a vítima;
3 - com intuito de lucro ou vantagem de qualquer espécie, própria ou de terceiro;
4 - com abuso de confiança;

5 - por motivo fútil;
6 - com o uso indevido de senha ou processo de identificação de terceiro; ou
7 - com a utilização de qualquer outro meio fraudulento.
Pena: detenção, de um a dois anos e multa.

Seção III

ALTERAÇÃO DE SENHA OU MECANISMO DE ACESSO A PROGRAMA DE COMPUTADOR OU DADOS

Artigo 10. Apagar, destruir, alterar ou de qualquer forma inutilizar, senha ou qualquer outro mecanismo de acesso a computador, programa de computador ou dados, deforma indevida ou não autorizada.
Pena: detenção de um a dois anos e multa.

Seção IV

OBTENÇÃO INDEVIDA OU NÃO AUTORIZADA DE DADO OU INSTRUÇÃO DE COMPUTADOR

Artigo 11. Obter, manter ou fornecer, sem autorização ou indevidamente, dado ou instrução de computador.
Pena: detenção, de três meses a um ano e multa.
Parágrafo único. Se o crime é cometido:
1 - com acesso a computador ou rede de computadores da união, estado, distrito federal, município, órgão ou entidade da administração direta ou indireta ou de empresa. Concessionária de serviços públicos,
2 - com considerável prejuízo para a vítima;
3 - com intuito de lucro ou vantagem de qualquer espécie, própria ou de terceiro;
4 - com abuso de confiança;
5 - por motivo fútil;
6 - com o uso indevido de senha ou processo de identificação de terceiro; ou
7 - com a utilização de qualquer outro meio fraudulento.
Pena: detenção, de um a dois anos e multa.

Seção V

VIOLAÇÃO DE SEGREDO ARMAZENADO EM COMPUTADOR, MEIO MAGNÉTICO, DE NATUREZA MAGNÉTICA, ÓPTICA OU SIMILAR

Artigo 12. Obter segredos; de indústria ou comércio, ou informações pessoais armazenadas em computador, rede de computadores, meio eletrônico de natureza magnética, óptica ou similar, de forma indevida ou não autorizada.
Pena: detenção, de um a três anos e multa.

Seção VI

CRIAÇÃO, DESENVOLVIMENTO OU INSERÇÃO EM COMPUTADOR DE DADOS OU PROGRAMA DE COMPUTADOR COM FINS NOCIVOS

Artigo 13. Criar, desenvolver ou inserir, dado ou programa em computador ou rede de computadores, de forma indevida ou não autorizada, com a finalidade de apagar, destruir, inutilizar ou modificar dado ou programa de computador ou de qualquer forma dificultar ou impossibilitar, total ou parcialmente, a utilização de computador ou rede de computadores.
Pena. Reclusão, de um a quatro anos e multa.
Parágrafo único: se o crime é cometido:
1 - contra o interesse da união, estado, distrito federal, município, órgão ou entidade da administração direta ou indireta ou de empresa concessionária de serviços públicos;
2 - com considerável prejuízo para a vítima;
3 - com intuito de lucro ou vantagem de qualquer espécie, própria ou de terceiro;
4 - por motivo fútil;
5 - com o uso indevido de senha ou processo de identificação de terceiro ou com a utilização de qualquer outro meio fraudulento.
Pena: reclusão, de dois a seis anos e multa.

Seção VII

VEICULAÇÃO DE PORNOGRAFIA ATRAVÉS DE REDE DE COMPUTADORES

Artigo 14. Oferecer serviço ou informação de caráter pornográfico em rede de computadores, sem exibir, previamente de forma facilmente visível e destacada aviso sobre sua natureza, indicando o seu conteúdo e a inadequação para criança ou adolescentes.
Pena: detenção, de um a três anos e multa.

CAPITULO IV

DAS DISPOSIÇÕES FINAIS

Artigo 15. Se qualquer dos crimes previstos nesta lei é praticado no exercício de atividade profissional ou funcional, a pena é aumentada de um sexto até a metade.

Artigo 16. Nos crimes definidos nesta lei somente se procede mediante representação do ofendido, salvo se cometidos contra o interesse da União, Estado, Distrito Federal, Município, órgão ou entidade da administração direta ou indireta, empresa concessionária de serviços públicos, fundações instituídas ou mantidas pelo poder público, serviços sociais autônomos, instituições financeiras ou empresas que explorem ramo de atividade controlada pelo poder público, casos em que a ação é pública incondicionada.

Artigo 17. Esta lei regula os crimes relativos à informática sem prejuízo das demais cominações previstas em outros diplomas legais.

Artigo 18. Esta lei entra em vigor 30 (trinta) dias a contar da data de sua publicação.

JUSTIFICAÇÃO

Na legislatura passada o ilustre Deputado Cássio Cunha Lima apresentou o PL 1.713/96 que dispõe sobre o acesso, a responsabilidade e os crimes cometido nas redes integradas de computadores Na justificativa do nobre Deputado, houve a preocupação com a transformação dessas redes de computadores em verdadeiros mercados, no sentido econômico da palavra, onde pessoas conversam, trocam informações e realizam transações comerciais, não existindo porém nenhuma legislação específica que regule as responsabilidade dos agentes envolvidos.

Distribuído inicialmente à Comissão de Ciência e Tecnologia, Comunicação e Informática, o PL 1.713/96 foi encaminhado a minha pessoa para ser o Relator do mesmo. Iniciei a discussão na comissão, inclusive com convocação de audiência pública e, em seguida com pessoas da área de informática, buscando identificar um texto que tratasse a matéria de urna forma mais global. Sob a coordenação do professor José Henrique Barbosa Moreira Urna Neto formou-se um grupo composto dos seguintes membros:
Dr. Damásio Evangelista de Jesus, advogado (SP)
Dr. Gilberto Martins de Almeida. advogado (RJ)
Dr. Ivan Lira de carvalho. Juiz Federal (RN)
Dr. Mário César Monteiro Machado> Juiz Auditor Militar (RJ)
Dr. Carlos Alberto Etcheverry, Juiz de Direito (RS)
Dr. Júlio César Finger, Promotor de Justiça (RS)
Dra. Marília Cohen Goldman, Promotora de Justiça (RS)
Dra. Ligia Leindecker Futterleib, advogada (RS)
Dr. Paulo Sérgio Fabião, Desembargador (RJ)

Este grupo, depois de vários debates "on-line" apresentou-me urna minuta. Do substitutivo ao referido PL 1.713/96. Ocorre que, por falta de tempo suficiente o substitutivo não foi devidamente apreciado, inclusive pelas demais comissões da Câmara dos Deputados, durante a legislatura passada, razão pela qual o PL foi arquivado. Portanto apresento agora o PL abaixo, o qual é resultado de um trabalho sério, depois de ouvir a sociedade, através de pessoas da mais alta qualificação.

Não podemos permitir que pela falta de lei, que regule os crimes de informática, pessoas inescrupulosas continuem usando computadores e suas redes para propósitos escusos e criminosos. Dai a necessidade de uma lei que, defina. Os crimes cometidos na rede de informática e suas respectivas penas.

Sala das Sessões, em __ de _____ de 1999.

Deputado **LUIZ PIAUHYLINO.**

ANEXO B

Assembleia da República

Lei da criminalidade informática

Lei nº109/91 – Portugal

A Assembleia da República decreta, nos termos dos artigos 164.º, alínea d), 168.º, n.º 1, alínea c), e 169.º, n.º 3, da Constituição, o seguinte:

CAPÍTULO I

Princípios gerais

Artigo 1.º

Legislação penal

Aos crimes previstos na presente lei são subsidiariamente aplicáveis as disposições do Código Penal.

Artigo 2.º

Definições

Para efeitos da presente lei, considera-se:

a) Rede informática - um conjunto de dois ou mais computadores interconectados;

b) Sistema informático - um conjunto constituído por um ou mais computadores, equipamento periférico e suporte lógico que assegura o processamento de dados;

c) Programa informático - um conjunto de instruções capazes, quando inseridas num suporte explorável em máquina, de permitir à máquina que tem por funções o tratamento de informações indicar, executar ou produzir determinada função, tarefa ou resultado;

d) Topografia - uma série de imagens entre si ligadas, independentemente do modo como são fixadas ou codificadas, que representam a configuração tridimensional das camadas que compõem um produto semicondutor e na qual cada imagem reproduz o desenho ou parte dele de uma superfície do produto semicondutor, independentemente da fase do respectivo fabrico;

e) Produto semicondutor - a forma final ou intermédia de qualquer produto, composto por um substrato que inclua uma camada de material semicondutor e constituído por uma ou várias camadas de matérias condutoras, isolantes ou semicondutoras, segundo uma disposição conforme a uma configuração

tridimensional e destinada a cumprir, exclusivamente ou não, uma função electrónica;

f) Intercepção - o acto destinado a captar informações contidas num sistema automatizado de dados, através de dispositivos electromagnéticos, acústicos, mecânicos ou outros;

g) Valor elevado - aquele que exceder 50 unidades de conta processual penal avaliadas no momento da prática do facto;

h) Valor consideravelmente elevado - aquele que exceder 200 unidades de conta processual penal avaliadas no momento da prática do facto.

Artigo 3.º

Responsabilidade penal das pessoas colectivas e equiparadas

1 - As pessoas colectivas, sociedades e meras associações de facto são penalmente responsáveis pelos crimes previstos na lei, quando cometidos em seu nome e no interesse colectivo pelos seus órgãos ou representantes.

2 - A responsabilidade é excluída quando o agente tiver actuado contra ordens ou instruções expressas de quem de direito.

3 - A responsabilidade das entidades referidas no n.º 1 não exclui a responsabilidade individual dos respectivos agentes.

4 - As entidades referidas no n.º 1 respondem solidariamente, nos termos da lei civil, pelo pagamento das multas, indemnizações e outras prestações em que forem condenados os agentes das infracções previstas na presente lei.

CAPÍTULO II

Dos crimes ligados à informática

Artigo 4.º

Falsidade informática

1 - Quem, com intenção de provocar engano nas relações jurídicas, introduzir, modificar, apagar ou suprimir dados ou programas informáticos ou, por qualquer outra forma, interferir num tratamento informático de dados, quando esses dados ou programas sejam susceptíveis de servirem como meio de prova, de tal modo que a sua visualização produza os mesmos efeitos de um documento falsificado, ou, bem assim, os utilize para os fins descritos, será punido com pena de prisão até cinco anos ou multa de 120 a 600 dias.

2 - Nas mesmas penas incorre quem use documento produzido a partir de dados ou programas informatizados que foram objecto dos actos referidos no número anterior,

actuando com intenção de causar prejuízo a outrem ou de obter um benefício ilegítimo, para si ou para terceiros.

3 - Se os factos referidos nos números anteriores forem praticados por funcionário no exercício das suas funções, a pena é de prisão de um a cinco anos.

Artigo 5.º

Dano relativo a dados ou programas informáticos

1 - Quem, sem para tanto estar autorizado, e actuando com intenção de causar prejuízo a outrem ou de obter um benefício ilegítimo para si ou para terceiros, apagar, destruir, no todo ou em parte, danificar, suprimir ou tornar não utilizáveis dados ou programas informáticos alheios ou, por qualquer forma, lhes afectar a capacidade de uso será punido com pena de prisão até três anos ou pena de multa.

2 - A tentativa é punível.

3 - Se o dano causado for de valor elevado, a pena será a de prisão até 5 anos ou de multa até 600 dias.

4 - Se o dano causado for de valor consideravelmente elevado, a pena será a de prisão de 1 a 10 anos.

5 - Nos casos previstos nos n.os 1, 2 e 3 o procedimento penal depende da queixa.

Artigo 6.º

Sabotagem informática

1 - Quem introduzir, alterar, apagar ou suprimir dados ou programas informáticos ou, por qualquer outra forma, interferir em sistema informático, actuando com intenção de entravar ou perturbar o funcionamento de um sistema informático ou de comunicação de dados à distância, será punido com pena de prisão até 5 anos ou com pena de multa até 600 dias.

2 - A pena será a de prisão de um a cinco anos se o dano emergente da perturbação for de valor elevado.

3 - A pena será a de prisão de 1 a 10 anos se o dano emergente da perturbação for de valor consideravelmente elevado.

Artigo 7.º

Acesso ilegítimo

1 - Quem, não estando para tanto autorizado e com a intenção de alcançar, para si ou para outrem, um benefício ou vantagem ilegítimos, de qualquer modo aceder a um sistema ou rede informáticos será punido com pena de prisão até 1 ano ou com pena de multa até 120 dias.

2 - A pena será a de prisão até três anos ou multa se o acesso for conseguido através de violação de regras de segurança.
3 - A pena será a de prisão de um a cinco anos quando:
a) Através do acesso, o agente tiver tomado conhecimento de segredo comercial ou industrial ou de dados confidenciais, protegidos por lei;
b) O benefício ou vantagem patrimonial obtidos forem de valor consideravelmente elevado.

4 - A tentativa é punível.

5 - Nos casos previstos nos n.os 1, 2 e 4 o procedimento penal depende de queixa.

Artigo 8.º

Intercepção ilegítima

1 - Quem, sem para tanto estar autorizado, e através de meios técnicos, interceptar comunicações que se processam no interior de um sistema ou rede informáticos, a eles destinadas ou deles provenientes, será punido com pena de prisão até três anos ou com pena de multa.

2 - A tentativa é punível.

Artigo 9.º

Reprodução ilegítima de programa protegido

1 - Quem, não estando para tanto autorizado, reproduzir, divulgar ou comunicar ao público um programa informático protegido por lei será punido com pena de prisão até três anos ou com pena de multa.

2 - Na mesma pena incorre quem ilegitimamente reproduzir topografia de um produto semicondutor ou a explorar comercialmente ou importar, para estes fins, uma topografia ou um produto semicondutor fabricado a partir dessa topografia.

3 - A tentativa é punível.

Artigo 10.º

Penas aplicáveis às pessoas colectivas e equiparadas

1 - Pelos crimes previstos na presente lei são aplicáveis às pessoas colectivas e equiparadas as seguintes penas principais:

a) Admoestação;

b) Multa;

c) Dissolução.

2 - Aplica-se a pena de admoestação sempre que, nos termos gerais, tal pena possa ser aplicada à pessoa singular que, em representação e no interesse da pessoa colectiva ou equiparada, tiver praticado o facto.

3 - Quando aplicar a pena de admoestação, o tribunal poderá aplicar cumulativamente a pena acessória de caução de boa conduta.

4 - Cada dia de multa corresponde a uma quantia entre 10000$00 e 200000$00, que o tribunal fixará em função da situação económica e financeira da pessoa colectiva ou equiparada e dos seus encargos.

5 - Se a multa for aplicada a uma entidade sem personalidade jurídica, responderá por ela o património comum e, na sua falta ou insuficiência, o património de cada um dos associados.

6 - A pena de dissolução só será aplicada quando os titulares dos órgãos ou representantes da pessoa colectiva ou sociedade tenham agido com a intenção, exclusiva ou predominantemente, de, por meio dela, praticar os factos que integram os crimes previstos na presente lei ou quando a prática reiterada desses factos mostre que a pessoa colectiva ou sociedade está a ser utilizada para esse efeito, quer pelos seus membros, quer por quem exerça a respectiva administração.

CAPÍTULO III

Penas acessórias

Artigo 11.º

Penas acessórias

Relativamente aos crimes previstos no presente diploma, podem ser aplicadas as seguintes penas acessórias:

a) Perda de bens;

b) Caução de boa conduta;

c) Interdição temporária do exercício de certas actividades ou profissões;

d) Encerramento temporário do estabelecimento;

e) Encerramento definitivo do estabelecimento;

f) Publicidade da decisão condenatória.

Artigo 12.º

Perda de bens

1 - O tribunal pode decretar a perda dos materiais, equipamentos ou dispositivos pertencentes à pessoa condenada que tiverem servido para a prática dos crimes previstos no presente diploma.

2 - A perda de bens abrange o lucro ilícito obtido com a prática da infracção.

3 - Se o tribunal apurar que o agente adquiriu determinados bens, empregando na sua aquisição dinheiro ou valores obtidos com a prática do crime, serão os mesmos também abrangidos pela decisão que decretar a perda.

Artigo 13.º

Caução de boa conduta

1 - A caução de boa conduta implica a obrigação de o agente depositar uma quantia em dinheiro, a fixar entre 10000$00 e 1000000$00, à ordem do tribunal, pelo prazo fixado na decisão condenatório, por um período entre seis meses e dois anos.

2 - A caução de boa conduta deve, em regra, ser aplicada sempre que o tribunal condene em pena cuja execução declare suspensa.

3 - A caução será declarada perdida a favor do Estado se o agente praticar, por meio de informática, nova infracção no período fixado na sentença, pela qual venha a ser condenado, sendo-lhe restituída no caso contrário.

Artigo 14.º

Interdição temporária do exercício de certas actividades ou profissões

1 - A interdição temporária do exercício de certas actividades ou profissões pode ser decretada quando a infracção tiver sido cometida com flagrante e manifesto abuso da profissão ou no exercício de actividade que dependa de um título público ou de uma autorização ou homologação da autoridade pública.

2 - A duração da interdição tem um mínimo de dois meses e um máximo de dois anos.

3 - Incorre na pena do crime de desobediência qualificada quem, por si ou por interposta pessoa, exercer a profissão ou a actividade durante o período da interdição.

Artigo 15.º

Encerramento temporário do estabelecimento

1 - O encerramento temporário do estabelecimento pode ser decretado por um período mínimo de um mês e máximo de um ano, quando o agente tiver sido condenado em pena de prisão superior a 6 meses ou em pena de multa superior a 100 dias.

2 - Não obstam à aplicação desta pena a transmissão do estabelecimento ou a cedência de direitos de qualquer natureza, relacionados com o exercício da profissão ou actividade, efectuados após a instauração do processo ou depois de cometida a infracção, salvo se, neste último caso, o adquirente se encontrar de boa fé.

3 - O encerramento do estabelecimento nos termos do n.º 1 não constitui justa causa para o despedimento de trabalhadores nem fundamento para a suspensão ou redução do pagamento das respectivas remunerações.

Artigo 16.º

Encerramento definitivo do estabelecimento

1 - O encerramento definitivo do estabelecimento pode ser decretado quando o agente:

a) Tiver sido anteriormente condenado por infracção prevista neste diploma em pena de prisão ou multa, se as circunstâncias mostrarem que a condenação ou condenações anteriores não constituíram suficiente prevenção contra crime;

b) Tiver anteriormente sido condenado em pena de encerramento temporário;

c) For condenado em pena de prisão por infracção prevista neste diploma, que tenha determinado dano de valor consideravelmente elevado ou para um número avultado de pessoas.

2 - Aplicam-se ao encerramento definitivo as disposições dos n.os 2 e 3 do artigo anterior.

Artigo 17.º

Publicidade da decisão

1 - Quando o tribunal aplicar a pena de publicidade, será esta efectivada, a expensas do condenado, em publicação periódica editada na área da comarca da prática da infracção ou, na sua falta, em publicação da área da comarca mais próxima, bem como através da afixação de edital, por período não inferior a 30 dias, no próprio estabelecimento ou no local do exercício da actividade, por forma bem visível pelo público.

2 - Em casos particularmente graves, nomeadamente quando a infracção importe lesão de interesses não circunscritos a determinada área do território, o tribunal poderá ordenar, também a expensas do condenado, que a publicidade da decisão seja feita no Diário da República ou através de qualquer meio de comunicação social.

3 - A publicidade da decisão condenatória é feita por extracto, do qual constem os elementos da infracção e as sanções aplicáveis, bem como a identificação dos agentes.

CAPÍTULO IV

Disposições finais

Artigo 18.º

Processo de liquidação

1 - Transitada em julgado a decisão que aplicar a pena de dissolução, o Ministério Público requer a liquidação do património, observando-se, com as necessárias adaptações, o processo previsto na lei para a liquidação de patrimónios.

2 - O processo de liquidação corre no tribunal da condenação e por apenso ao processo principal.

3 - Os liquidatários são sempre nomeados pelo juiz.

4 - O Ministério Público requer as providências cautelares que se mostrem necessárias para garantir a liquidação.

Artigo 19.º

Entrada em vigor

O presente diploma entra em vigor no prazo de 120 dias a contar da sua publicação.

Aprovada em 11 de Junho de 1991. O Presidente da Assembleia da República, Vítor Pereira Crespo.

Promulgada em 26 de Julho de 1991.

Publique-se. O Presidente da República, MÁRIO SOARES.

Referendada em 31 de Julho de 1991. O Primeiro-Ministro, *Aníbal António Cavaco Silva*.