PONTIFÍCIA UNIVERSIDADE CATÓLICA DE SÃO PAULO
PUC-SP

Marina Giantomassi Della Torre

Aspectos processuais e penais dos crimes de computador

MESTRADO EM DIREITO

SÃO PAULO

2009

PONTIFÍCIA UNIVERSIDADE CATÓLICA DE SÃO PAULO
PUC-SP

Marina Giantomassi Della Torre

Aspectos processuais e penais dos crimes de computador

MESTRADO EM DIREITO

Dissertação apresentada à Banca Examinadora da Pontifícia Universidade Católica de São Paulo, como exigência parcial para a obtenção do título de Mestre em Direito Processual Penal, sob a orientação do Professor Doutor Antônio Carlos da Ponte.

SÃO PAULO

2009

Banca Examinadora

_____

_____

_____

“O importante não é a utópica concordância de todos sobre os problemas científicos do direito, mas a coerência com que cada um sustenta os próprios pontos de vista”. (Cândido Rangel Dinamarco, *Fundamentos do processo civil moderno*, p.37).

Aos meus pais, Valter e Virginia, pelo amor incondicional.

Ao meu marido, Vinicius, pelo carinho, compreensão, estímulo e companheirismo.

AGRADECIMENTOS

Aos meus pais, Valter e Virginia, responsáveis pelos momentos mais importantes da minha vida. Sem vocês esse trabalho não existiria.

Ao meu marido, Vinicius, também responsável por boa parte da minha felicidade e das minhas conquistas. Pessoa admirável e fonte de incentivo e estímulo.

Às minhas amadas irmãs, Ana Adelina e Mariana, batalhadoras e vencedoras, pelos incentivos constantes e pensamentos positivos.

À minha tia, Melânia Dalla Torre, minha segunda mãe e um exemplo a ser seguido.

Aos meus sogros, Antônio e Edna Canheu, pelo carinho, apoio e manifestações de alegria nas vitórias alcançadas.

Aos meus colegas professores e coordenadores da Universidade Paulista, *campus* São Paulo e São José do Rio Pardo, pela colaboração, paciência, confiança e oportunidades concedidas.

Ao meu querido Professor orientador, Doutor Antônio Carlos da Ponte, homem generoso, professor brilhante e culto, profissional honrado, mais que um tutor intelectual, a quem, por toda a minha vida, serei grata.

RESUMO

Vivemos uma revolução no âmbito da tecnologia. Neste despertar de inovações, uma ordem jurídica tradicional e conservadora, baseada em relações e conceitos historicamente construídos e derivados de usos e costumes fundamentalmente dependentes de fatos e atividades perceptíveis e identificáveis, depara-se com uma "velha" e uma "nova" realidade, pela qual surgem novas relações, totalmente diversas do mundo real, e que exigem novos conceitos e interpretações.

A existência da telemática mostra-se como uma considerável mudança nos hábitos cotidianos daqueles que a utilizam, promovendo sua inclusão definitiva em um mundo cada vez mais dinâmico.

No campo do Direito, o seu surgimento propõe vários desafios, entre os quais o mais manifesto é a necessidade de se criar mecanismos reguladores para as condutas criminosas desenvolvidas nesse meio, que impõe, pelas suas características, além de paradigma de controle repressivo mais severo, um paradigma preventivo em nossa legislação.

Utilizando de uma relação entre a lei brasileira, o direito comparado, as discussões doutrinárias e jurisprudenciais e propostas dessa nova conjuntura, procuramos analisar uma série de questões, dentre elas os bens jurídicos atingidos pela criminalidade informática, o pretensos criminosos e suas vítimas, problemas acerca da tipicidade e competência.

Mostra-se necessária, também, a identificação de autoria e materialidade relativas a essa nova e complexa modalidade de ilícitos: a criminalidade informática, surgida em uma sociedade global de risco informático e da informação.

Por fim, com o objetivo de resguardar os princípios trazidos pela Constituição Federal, tanto os direitos e garantias fundamentais do cidadão quanto os direitos e garantias do Estado, devem ser assegurados, reforçando-se as bases de um Estado Democrático de Direito, por meio de um juízo de ponderação que observe o princípio da proporcionalidade, toda vez que se fizer necessária a apuração e punição da prática de crimes dessa natureza.

DELLA TORRE, Marina Giantomassi. *Aspectos processuais e penais dos crimes de computador*.

PALAVRAS-CHAVE: crimes de computador

ABSTRACT

We live in the midst of a technological revolution. In the wake of innovation, a traditional and conservative judicial order faces, simultaneously, an old and new reality. While the “old reality” is based on concepts and habits either built or resulting from facts and activities that can be perceived and identified; the “new reality” is based on a virtual mean, where new relationships arise (not necessarily connected to the real world), requiring new concepts and interpretations.

The use of telematics leads to a considerable change in the habits of those who make use of it, enabling their definitive inclusion in an increasingly dynamic world.

The emergence of telematics poses many challenges in the Law field. Among the main ones, we highlight the need to establish regulation for criminal conducts carried out in this mean. Given its characteristics, it requires the establishment of a paradigm for preventive control, in addition to severe repressive means.

Using the relationships between Brazilian law, comparative law, discussions of doctrine and jurisprudence and proposals of this new scenario, we seek to analyze a set of questions, including juridical goods affected by telematics crimes; supposed criminals and their victims; and problems related to their types and competencies.

The identification of authors and relative relevancies are also needed for this new and complex fashion of crimes: technology crimes resulting from a new global and risky information society.

Lastly, seeking to protect the principles of the Federal Constitution, both the citizen and State’s fundamental rights and guarantees must be secured, reinforcing the base of the Democratic State of law. This must be done through a judgment

consideration that observes the proportionality principle, in every single situation that requires investigation and punishment of crimes of this nature.

DELLA TORRE, Marina Giantomassi. *Aspectos processuais e penais dos crimes de computador*.

WORDS-KEY: computer crimes

SUMARIO

INTRODUÇÃO

A expansão transnacional da economia de mercado, a emergência de um mercado de capitais transnacional, a invenção de tecnologias de comunicação e de informação operando em escala global e a migração transnacional são as características mais marcantes de um processo que é usualmente chamado de 'globalização'. Quer esses processos realmente mereçam ser chamados de 'globais', quer essa caracterização seja verdadeira apenas para a parte mais rica do mundo, isso é uma questão ainda aberta. Não obstante, as suas forças dinâmicas começaram a mudar os padrões tradicionais de ordem social, em particular o modelo comum de Estado nacional soberano.

O acelerado desenvolvimento da sociedade ocidental, por conta dos grandes avanços tecnológicos, como reflexo direto do fenômeno da globalização, resultou em mudanças nas relações intersubjetivas, na economia, na cultura, na política e nas ciências, e, também, inclusão digital acelerada, a despeito da existência, hoje em dia, de uma grande quantidade de cidadãos excluídos digitalmente, mundo afora, principalmente em áreas rurais da Índia e da China e em favelas e cortiços de metrópoles dos países subdesenvolvidos. [1]

A partir do desenvolvimento da tecnologia e o acesso cada vez maior da população às suas facilidades, alguns aspectos da vida cotidiana sofreram algumas profundas transformações. Grande parte do trabalho humano foi absorvido pela automatização em vários setores da indústria e demais setores de produção.

[1] BOITEUX, Luciana. *Crimes informáticos: reflexões sobre política criminal inseridas no contexto internacional atual*. *In*: Revista Brasileira de Ciências Criminais, São Paulo: vol. 47, março/abril 2004, p. 146/187.

Nos dias atuais é impossível imaginar como seria a vida das pessoas sem a integração com a informática. Praticamente todo o desenvolvimento econômico de uma nação está baseado na tecnologia produzida em seu território e exportada para os demais consumidores.

A corrida tecnológica permitiu, também, a evolução dos meios de comunicação, que se consolidaram como imprescindíveis ao mundo globalizado. As pessoas têm à sua disposição diversas maneiras de se comunicar, fazendo das distâncias meros obstáculos superáveis.

A combinação informática e comunicação abriu fronteiras através da transmissão de dados de um computador para outro e que, atualmente, demonstra sua força maior na grande rede mundial de computadores, a internet.

A internet oferece incontáveis recursos de utilização, tais como, o correio eletrônico (e-mail), movimentação de dados, acesso a páginas eletrônicas, entre outros e, com isso, fez surgir uma nova mentalidade desta nova via de comunicação.

Enviar mensagens em tempo real, conversar em grupo como se estivesse em reunião, expressar idéias sem censura, realizar compras sem ter que se dirigir até o estabelecimento comercial são alguns dos benefícios e facilidades advindos com a internet.

As transformações provocadas pela informática e pela internet na vida do ser humano são evidentes e se solidificam dia a dia, com a interferência em todos os campos sociais: na cultura; na economia; na educação e, por conseguinte, atinge o campo do direito.

Para o direito, essa nova realidade não pode ser desprezada, pois as consequências da informática e da internet no mundo jurídico são incontestáveis e totalmente diferentes do mundo físico em que nos acostumamos a viver.

Ricardo M. Mata y Martin apontou as transformações pelas quais passou a sociedade hodierna como fator relevante para as necessárias mudanças no âmbito jurídico, que, no mais das vezes, chegam a passos lentos, eis que

> "nas últimas duas décadas tem tomado corpo a eclosão do fenômeno informático em amplas parcelas de nossa sociedade. A enorme expansão que vem gozando o processamento automatizado de dados em uma sociedade cada vez mais receptiva às possibilidades crescentes que oferecem os meios informáticos e isso tem consequências indubitáveis para o mundo do direito".[2]

A comunicação estabelecida pela internet anula os limites de espaço e tempo, fazendo nascer uma sociedade de comunicação global, em que, abatidas, hipoteticamente, as fronteiras das nações, das culturas e ideologias, têm surgido novas relações. Essa tecnologia inovadora deixa o mundo menor.

É claro que essa evolução tecnológica não traz somente vantagens.

A partir dessa cultura instalada pelo casamento entre tecnologia e comunicação, novas maneiras de praticar atos ilícitos também surgiram.

A macrocriminalidade surge como uma teia de relacionamentos ilícitos, em âmbito planetário, rompendo limites territoriais dos países envolvidos, ignorando-se quaisquer soberanias ou tratados e convenções internacionais firmados.

Marco Antônio Marques da Silva, ponderou, outrossim, que existe, de fato, uma nova criminalidade, consentânea com o processo de globalização, uma criminalidade transnacional, a saber:

---

[2] MATA Y MARTÍN, Ricardo M. *Delincuencia informática y derecho penal*. Madrid, Edisofer Libros Jurídicos, 2001, p.11. Original em espanhol: "*Em las dos últimos décadas há tomado cuerpo la eclosión del fenômeno informático em amplias parcelas de nuestra sociedad. L enorme expansión de que viene gozando el procesamiento automatizado de datos em uma sociedad cada vez más receptiva a lãs possibilidades crecientes que oferecen los médios informáticos tiene consecuencias indudables para el mundo del Derecho*."

"existe uma nova forma de criminalidade emergente, em virtude do fenômeno da globalização, que exige que os países passem a se concentrar em atitudes mais práticas, a fim de que suas abordagens sejammais eficazes no combate à criminalidade. A reflexão científica em torno da questão volta-se para satisfazer a necessidade premente de responder àquela criminalidade, muito mais do que buscar uma perfeição teórica. Trata-se de dar respostas às instâncias do poder político e de aplicação judicial do direito, que se encontram paralisados na luta dos ordenamentos nacionais contra essa nova face da criminalidade – transnacional.

A necessidade de um tratamento rápido para o problema o coloca não na discussão da possibilidade da existência de uma ciência penal supranacional, mas de *construir respostas jurídico-penais supranacionais que sejam soluções concretas para a questão*. À ciência caberia a tarefa de fornecer as bases de tais soluções.

É importante que se verifique que o fenômeno da globalização (econômica e das comunicações) produz dois efeitos sobre a delinquência. De um lado, há a necessidade de eliminarem-se determinadas figuras delitivas, como aquelas que dizem respeito a condutas vulneratórias das barreiras e controles estatais a livre circulação, pois, caso contrário, passariam a ser obstáculos às próprias finalidades perseguidas pela globalização. De outro lado, *esses mesmos fenômenos econômicos acabam por favorecer o nascimento de novos comportamentos que se tornam inovações com relação a delitos clássicos*. Assim, a integração faz nascer uma delinquência contra os interesses financeiros de toda a comunidade, produto da globalização.

A questão da delinquência como um fenômeno marginal torna-se insuficiente diante da chamada criminalidade organizada, ou seja, nela intervêm estruturas coletivas de pessoas que, a semelhança das organizações empresariais, tem uma estrutura hierárquica. Num outro lado, há uma sensível dissociação entre aqueles agentes que efetivamente detém papéis mais relevantes na organização, daqueles que diretamente executam as ações. De lado material, a criminalidade supranacional é poderosa, cujos resultados lesivos são sempre de grande magnitude, seja mo que diz respeito ao aspecto econômico, como no social e político. É uma criminalidade que detém capacidade para provocar desestabilização nos mercados financeiros e no aspecto político, além de deter uma capacidade enorme de corrupção de funcionários e governantes." [3]

[3] SILVA, Marco Antônio Marques da. *Acesso à justiça penal e Estado Democrático de Direito*. São Paulo: Juarez de Oliveira, 2001, p.137.

Além disso, a tecnologia da informação apresenta uma relação compensadora de custo-benefício para a prática do crime, oferencendo novos recursos técnicos para colocar bens jurídicos em risco. Algumas vezes, o crime pode ser praticado quase que anonimamente, sem que se deixe praticamente nenhum vestígio sobre sua origem.

Tais crimes apresentam perigo para empresas privadas, para toda a economia de um país e sua sociedade, e isso levou alguns países a celebrarem convênios nacionais e internacionais para combater os crimes cometidos através do uso de computadores.[4]

Com a interligação global de computadores em rede, qualquer sistema informático conectado pode ser atacado a partir de qualquer lugar no mundo.

Surgem novas técnicas para a prática de crimes tradicionais, bem como novas modalidades de crimes.

O ciberespaço é, hoje em dia, um *locus* de cometimento dos mais díspares delitos, seja o comércio ilegal de armas, medicamentos, produtos intelectuais contrafeitos, enfim, todo tipo de mercancia ilícita é ali praticada.

Condutas criminosas antes realizadas com o uso de armas, por exemplo, pelo contato pessoal, agora encontram meios alternativos, onde as distâncias não representam barreirras e os agentes permanecem sentados diante de um computador de onde o crime é praticado.

E são esses crimes praticados com o emprego do computador, o objeto principal do presente estudo.

A tecnologia muda o homem e muda o direito, não necessariamente no mesmo ritmo.

---

[4] SIEBER, Ulrich. *Documentación para una aproximacion al delito informatico*, *apud* LIMA, Paulo Marco Ferreira. *Crimes de computador e segurança nacional*. Campinas: Millennium Editora, 2006, p. 03.

A celeridade da dinâmica dessa sempre mutante realidade virtual, com o surgimento de novas tecnologias em interregnos curtos, é fator de causa de perplexidade aos operadores do direito, contudo, ainda que as resposta surjam lentamente há que se providenciar o cabedal de conhecimentos teóricos para que os fundamentos dessas respostas legiferantes sejam sólidos, técnicos e precisos, evitando-se, a todo custo, a voracidade do direito penal e a normatização de tudo o que se passa no ciberespaço, com reflexos diretos na intimidade e na privacidade dos cidadãos.

E essa foi a razão principal da escolha do tema do presente estudo, considerando que não há tecnologia que tenha se expandido tanto nas últimas décadas como a dos computadores, e que, comparada ao direito, tal evolução não se deu no mesmo compasso.

As inúmeras práticas delituosas perpetradas por meio de computadores crescem de forma exponencial, enquanto que as respostas estatais estão aquém do que se espera, mormente como fator – demonstração, de que a rede mundial de computadores não é uma terra sem lei, seja pela dificuldade de investigação criminal, seja pela ausência de legislação aplicada.

O direito precisa acompanhar essa nova realidade – a era da sociedade digital - e estabelecer a regulação pertinente. Mas, tal empreitada deve vir antes que a informática e a internet se transformem em feras indomáveis.

Assim, antes que a liberdade do homem, sua privacidade e sua paz, bem como o próprio Direito, sejam destruídos, faz-se mister regular e monitorar juridicamente a internet.

Diante da complexidade da questão e da característica global dos delitos cibernéticos, a existência de leis nacionais discrepantes, com o objetivo de prevenção geral, mostra-se favorável à criação de paraísos cibernéticos.[5]

Problemas surgem em questões referentes à tipicidade, aos sujeitos ativos desses crimes e às suas diversas condutas, local da infração, determinação da autoria, efetivação de perícias e competência jurisdicional.

Outra faceta manifesta dessa modalidade criminosa se refere na definição do perfil do agente criminoso virtual.

A mídia, praticamente toda semana, traz informações acerca de golpes ou fraudes de ordem econômico-financeiros praticados pela internet, lesando milhares de pessoas.

A habilidade dos *hackers* e *crackers* no maunseio das ferramentas da informática e de acesso a lugares tidos como intransponíveis por via da internet tem levado as grandes empresas de *software* e os cientistas da computação a investirem elevados recursos e enorme talento em pesquisas para previnir as condutas delituosas no mundo virtual. As grandes corporações bancárias e instituições financeiras investem, anualmente, milhões de dólares na área da segurança, particularmente no desenvolvimento da tecnologia de informática e na criação de instrumentos de criptografia de dados e de acesso à movimentação de recursos financeiros.

O Brasil ainda não possui uma legislação específica sobre o tema, mas o Poder Legislativo já vem discutindo o assunto. Há quem defenda ser inexigível a promulgação de nova Lei, teoria que não deve prevalecer.

---

[5] BOITEUX, Luciana. *Crimes informáticos: reflexões sobre política criminal inseridas no contexto internacional atual. In*: Revista Brasileira de Ciências Criminais, São Paulo: vol. 47, pp.146/187, março/abril 2004.

A precariedade da legislação, aliada à falta de conhecimentos específicos sobre a rede mundial e acerca dos métodos e forma utilizados pelos criminosos, de um lado, e a incessante expansão da Internet e também o permanente avanço da criatividade dos *hackers*, de outro, dificultam sobremaneira a questão da segurança digital. Isso porque, não só através de antivírus, *firewalls*, criptografia, etc, se combate a ação desses *experts*. A falta de regulamentação no que pertine a este tema também constitui elemento de intranquilidade. 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 lesado é de tal monta, que a sociedade clama por penalidades mais severas, veiculadas através de normas específicas.

O Direito Penal não está totalmente preparado para fazer frente à criminalidade informática. Isto cria uma incerteza na sociedade sobre o que é e o que não é permitido.

Na verdade, as mudanças tecnológicas fizeram com que a sociedade da era tecnológica elegesse novos bens socialmente relevantes, como a informação, a privacidade e o acesso às redes de computadores.

Segundo Ivette Senise Ferreira, a preocupação com essa questão surge nas últimas décadas com a popularização dessa nova tecnologia, manifestando-se também através da promulgação de leis relativas à informática e na menção de competência privativa da União (Constituição Federal, art. 22, inciso IV) para legislar sobre a matéria.[6]

A mesma autora ainda aponta a existência de lacunas da chamada "legislação inadequada existente, que estão a exigir uma solução mais condizente com

[6] FERREIRA, Ivette Senise. *A criminalidade informática*. *In*: LUCCA, Newton de, SIMÃO FILHO, Adalberto (Coordenadores) e outros. *Direito e internet – aspectos jurídicos relevantes*. 2ª edição, São Paulo: Quartier Latin, 2005, p.208.

sua gravidade e a sua incidência" e que essa mesma legislação "econtra-se extremamente defasada e desvinculada da realidade", apontando que

> "urge disciplinar a utilização abusiva da informática, hoje transformada num dos mais importantes veículos de comunicação, com alcance imediato em todo o mundo, dando-se atenção à questão da definição dos limites da ilictude, e da conveniência para o meio social, do material que é transmitido por essa via". [7]

Os prejuízos causados à sociedade continuam e, por isso, existe a necessidade de combater essa nova modalidade criminosa. As dificuldades são inúmeras, já que a técnica intelectual é farta e o anonimato permitido pela internet atrapalha na identificação da autoria.

Inúmeros são os delitos que podem ser praticados com o uso de computadores conectados à *web*, desde os mais óbvios, como os crimes contra a honra, subtração e fraudes diversas, até aqueles ligados à corrupção de menores, pedofilia, homicídio, terrorismo e violações à propriedade intelectual e industrial.

Alguns dos delitos são passíveis de tipificaçã o pela atual estrutura normativa penal, em outros a solução estaria no aumento da pena e alguns ainda são desapercebidos e, para que tenham força coercitiva, são imprecindíveis novas previsões e definições legais.

Existem algumas propostas tramitando nas casas legislativas, embora não seja possível afirmar quando ou qual proposta será aprovada. Contudo, verifica-se desnecessária a criação de um novo universo jurídico, vez que o ordenamento jurídico atual é suficiente para a recepção dessa nova realidade, contudo, a legislação atual é

[7] FERREIRA, Ivette Senise. *A criminalidade informática*. *In*: LUCCA, Newton de, SIMÃO FILHO, Adalberto (Coordenadores) e outros. *Direito e internet – aspectos jurídicos relevantes.* 2ª edição, São Paulo: Quartier Latin, 2005, p.236.

mesmo incapaz de atender de forma eficaz todas as questões atinentes a essa prática criminosa, necessitando, assim, de indispensável e manifesta reformulação.

Diferente do que possa parecer, não se trata de um raciocínio contraditório, mas somente sugere-se a adaptação de leis e conceitos, visando a proteção de bens jurídicos a serem tutelados pelo Direito Penal da Internet.

Com o escopo de buscar soluções para toda a problemática dos crimes de informática, há em nossos dias perigosa adaptação dos princípios constitucionais norteadores do Direito Penal, principalmente o denominado Princípio da Legalidade, previsto no art. 5º, inciso XXXIX, da Cosntituição Federal, segundo o qual "não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal".

A interpretação de tal dispositivo nos leva a concluir que a descrição do delitos de informática há de ser específica e deverá individualizar o comportamento do criminoso, sob pena se não trazer nenhuma garantia real e efetiva.

Em matéria penal, não há como se conceber uma lei demasiadamente genérica. Dever ser tratada de forma detalhada a identificação de cada conduta que se tenha como delituosa, evitando-se, assim, a ameaça e a mitigação das liberdades individuais.

Nessa esteira, oportunas são as lições de Luiz Vicente Cernicchiaro e Paulo José da Costa Junior quando afirmam que

> "a finalidade do princípio é dar a conhecer ao agente a conduta vedada, especificamente descrita. Não é bastante simples referência ao bem juridicamente tutelado. O delito, fundamentalmente, é a conduta que produz o resultado. A garantia constitucional somente estará realizada se a indicação do proibido compreender todos os elementos do fato delituoso (ação e resultado)".[8]

[8] *Direito penal na constituição.* 2 ed. São Paulo: Editora Revista dos Tribunais, 1991, p. 16.

Diferente não é o entendimento de Vladimir Aras, segundo o qual

> "a internet permite a prática de delitos à distância no anonimato, com um poder de lesividade muito mais expressivo que a criminalidade dita convencional, em alguns casos. Em face dessa perspectiva e diante da difusão da internet no Brasil, o Estado deve prever positivamente os mecanismos preventivos e repressivos de práticas ilícitas".[9]

Diante desse raciocínio, concluimos que em um Direito Penal democrático o crime não pode ser havido como qualquer ação, mas sim uma ação determinada em lei.

O cidadão do mundo virtual é, antes de tudo, um cidadão do mundo real e da mesma forma deve ser encarado como o agente criminoso. É exatamente nesta interseção que o Direito punitivo deverá incidir, todavia, tal incisão deverá se dar com a devida moderação, verificadas as particularidades de cada caso, não podendo ser aplicada cega e inadvertidamente.[10]

O Estado brasileiro deve sim intervir nas relações havidas por meio de computadores, seja legislando e disciplinando o uso da internet, seja deixando ao âmbito do legislador penal a tipificação de crimes, seja censurando e controlando as informações havidas na Rede, porém, sempre obedecendo os preceitos constitucionais.

A internet não pode ser considerada uma terra de ninguém, sem fronteiras, e, sim, deve ser obrigatoriamente regida pelos princípios gerais do direito, devendo o Estado atuar para coibir práticas e condutas nefastas, zelando pela liberdade individual e pelo interesse público.

---

[9] ARAS, Vladimir. *Crimes de informática – uma nova criminalidade*. Acesso em: http://jus2.uol.com.br/doutrina/texto.asp?id=2250, em 04/03/2008, às 11h41min.

[10] OPICE BLUM, Renato M. S., DAOUN, Alexandre Jean. *Cybercrimes*. *In* LUCCA, Newton de, SIMÃO FILHO, Adalberto (Coordenadores) e outros. *Direito e internet – aspectos jurídicos relevantes*. 2ª edição, São Paulo: Quartier Latin, 2005, p.118.

O fato de a conduta humana, nesses casos especificamente, ser realizada por intermédio de computadores não a afasta da esfera do direito.

O Direito é a única forma de controle capaz de conter o avanço da criminalidade no mundo virtual, isto porque, de todos os sistemas de controle social, o Direito é o único que se reveste das características da coercitividade, sancionando as condutas havidas por ilícitas, quer seja na esfera civil, penal ou administrativa.

Entretanto, a criação de novas leis são insuficientes para estancar as ilegalidades cometidas no ciberespaço. É crucial ao Estado e à iniciativa privada investir em campanhas educativas para conscientização dos internautas. Há pessoas que nem imaginam que compartilhar arquivos protegidos pelo direito autoral pode ser ilegal, mesmo que para uso privado. Há outras que nem desconfiam dos riscos envolvidos com a exposição da vida privada proporcionada pelos sites de relacionamento.

Cada vez mais, precisa-se confiar na informática, da qual depende a vida de milhares de pessoas. Evidencia-se, assim, ser crucial a organização do Estado brasileiro para o combate à crimialidade informática. Faz-se necessária uma reforma na legislação criminal, nos âmbitos nacional e internacional, bem como proporcionar aos órgãos de investigação melhor estrutura de maneira que estes possam combater de forma eficaz essa nova criminalidade.

Embora alguns países já tenham assinalado a forma de como deverão proceder a regulamentação dos crimes particados via internet, ainda não há um consenso como tal controvérsia será dirimida. Os Estados Unidos da América, por exemplo, entendem que, pelo fato de a internet se tratar de um meio de comunicação ainda em fase de aperfeiçoamento, uma regulamentação, pelo menos no atual estágio,

seria uma medida um tanto prematura.[11] Em novembro de 2001, influenciada pelos episódios de 11 de setembro do mesmo ano, na cidade de *New York*, a Comunidade Européia editou Convenção sobre o "cybercrime", estabelecendo conceitos basilares, quer de direito material, quer de direito processual, sugerindo-se rol de "tipos- padrão" para os países signatários, evidenciando o interesse de que haja a desejada padronização universal, tendo em vista uma das principais características desse tipo de criminalidade – a transnacionalidade. O desapego a qualquer forma de fronteira faz desaparecer arraigados conceitos de soberania nacional e, consequentemente, de tradicionais regras de competência.

O número de reclamações com relação a crimes na internet quase triplicou entre os anos de 2005 e 2006. Segundo dados do Centro de Estudos Resposta e Tratamento de Incidentes de Segurança no Brasil (Cert.Br) foram cerca de 68 (sessenta e oito) mil casos registrados em 2005 e 197,9 (cento e noventa e sete virgula nove) mil casos em 2006. Em projeção baseada no número de ocorrências até março de 2007, cerca de 56 (cinqüenta e seis) mil, devem se registrar 224 (duzentos e vinte e quatro) mil casos em 2007.[12] O número de procedimentos abertos pelo Ministério Público Federal (MPF) em São Paulo para investigar crimes pela internet explodiu 318% entre 2007 e 2008, revelou[13] o Grupo de Combate aos Crimes Cibernéticos que rastreia denúncias sobre pedofilia, intolerância racial, pornografia infantil, xenofobia e crimes de ódio. Foram instauradas 620 (seiscentos e vinte) investigações em 2007 e 1.975 (um mil novecentos e setenta e cinco) em 2008.[14]

---

[11] Exemplo citado por FRAGA, Antônio Celso Galdino. *Crimes de informática: a ameaça virtual na era da informação digital. In*: SCHOUERI, Luís Eduardo (Organizador). *Internet: o direito na era virtual*. Rio de Janeiro: Forense, 2001, p.366.

[12] Dados fornecidos pelo Clipping Eletrônico da Associação dos Advogados de São Paulo, edição de 04 de dezembro de 2007.

[13] Informação dada em 10 de fevereiro de 2009 e publicada pelo Clipping Eletrônico da Associação dos Advogados de São Paulo, edição de 11 de fevereiro de 2009.

[14] Dados fornecidos pelo Clipping Eletrônico da Associação dos Advogados de São Paulo, edição de 11 de fevereiro de 2009.

O aumento de casos levados ao Ministério Público Federal se deve a dois fatores, segundo os procuradores da República. Primeiramente, destaca-se o acordo de cooperação firmado com o Google, maior site de buscas, que passou a tirar do ar páginas suspeitas, preservando e encaminhando ao referido órgão provas de conteúdos ilegais postados no Orkut. O segundo fator foi a mudança no Estatuto da Criança e do Adolescente (ECA), que passou a tornar crime condutas antes não penalizadas, como a posse de material de pornografia infantil.[15]

Para o advogado Renato Opice Blum[16], o número de processos com relação a crimes na internet, representa uma média muito acima de todos os países da União Européia, onde existe legislação específica para este tipo de crime. Ainda segundo o advogado, o que falta hoje no Brasil é conscientização preventiva da segurança da informação, sugerindo que as autoridades façam um controle de acesso a esse meio, solicitem a identificação, autenticação e autorização individuais, ofereça o mínimo de acesso e segregue o uso de acordo com a função.

No trabalho em tela, após a introdução, há um capítulo com um escorço histórico sobre os crimes de computador. Tal apanhado histórico também permeou o corpo de toda a presente pesquisa através da exposição dos avanços tecnológicos mais importantes que resultaram nesse ente abstrato que é o verdadeiro *locus* de cometimento dos crimes de computador – a Internet, com os seus consectários, como a idéia de ciberespaço.

Logo depois, um capítulo referente aos bens juridicamente protegidos, os conceitos e denominações, classificações e sujeitos desse tipo de criminalidade. Ainda

[15] Dados fornecidos pelo Clipping Eletrônico da Associação dos Advogados de São Paulo, edição de 11 de fevereiro de 2009.
[16] Dados fornecidos pelo Clipping Eletrônico da Associação dos Advogados de São Paulo, edição de 04 de dezembro de 2007.

no mesmo capítulo, abordamos os principais problemas e dificuldades no tocante à tipicidade, competência e autoria.

Faz-se necessária uma distinção, ainda que didática, acerca dos termos, definição e conceito, pois todo trabalho científico que aspira à seriedade intelectual há de possuir precisa delimitação do marco teórico, para que teleológica e pragmaticamente, seu labor científico tenha um único objeto.

Além disso, aprofundou-se o estudo acerca do fenômeno expansionista do direito penal e sua funcionalização, principalmente como instrumento de política criminal.

O estudo do direito comparado também se torna fundamental, com o escopo de buscar uma estrutura penal compatível sob a óptica internacional. Optou-se, como objeto de estudo comparado com o direito brasileiro, na Europa, pelo direito Alemão, Espanhol, Francês, Italiano, Inglês e Português. Na América Latina, pelos direito da Argentina e do Chile. Em derradeiro, os Estados Unidos, pelos avanços nas discussões acerca do tema.

A análise da teoria do Direito Penal do inimigo frente à criminalidade informática também se faz necessária, uma vez que, em alguns casos, o Direito Penal Clássico, com suas regras e princípios rígidos, não está preparado para o combate dessa nova modalidade criminosa.

Por fim, um capítulo dedicado às figuras típicas da informática existentes na legislação brasileira, bem como as propostas legislativas pendentes de votação no Congresso Nacional.

Vale lembrar ainda que a conclusão desse trabalho não se fecha em si mesma, não tendo a pretensão de esgostar todo tema, uma vez que isso seria impossível quando se trata de informática e de condutas criminosas a esta relacionada. Mas almeja-

se, que a leitura deste possibilite perceber essa nova realidade de Sociedade da Informação, no desiderato de contribuir para a elaboração de normas adequadas, bem como para a revisão de normas antigas que se mostrem inadequadas à nova realidade.

CAPÍTULO I – SURGIMENTO DOS CRIMES DE COMPUTADOR

1.0- Escorço histórico

Os crimes de computador surgiram nas últimas décadas do século XX, em meados dos anos sessenta, conforme destaca Ulrich Sieber[17], professor da Universidade de Würzburg e grande especialista no assunto, o qual afirma que o surgimento dessa espécie de criminalidade remonta à década de 1960, época em que apareceram na imprensa e na literatura científica os primeiros casos do uso do computador para a prática de delitos, constituído, sobretudo, por manipulações, sabotagens, espionagem e uso abusivo de computadores e sistemas, denunciados em matérias jornalísticas.

A partir da década de setenta, apareceram os primeiros estudos empíricos sobre a criminalidade informática. Eles deram destaque a um número limitado de casos, mas ao mesmo tempo salientaram que uma quantidade considerável de condutas criminosas ora não eram detectadas, ora sequer eram divulgadas por suas vítimas, em virtude de temerem danos à sua imagem.

Os dois primeiros casos estudados que, posteriormente, se tornaram famosos, envolveram a American Equity Fund, uma empresa de seguro, e o Herstatt-Bank.[18]

O primeiro caso constitui um exemplo clássico de crime de computador de natureza econômica. Seus diretores armazenaram num computador 56.000 apólices de seguro de vida falsas, com um valor de venda de US$30 milhões. Essas apólices

[17] SIEBER, Ulrich. *Delitos informáticos e outros delitos contra a tecnologia da informação*. Comentário e questionário preparatório para o Colóquio da Association Internationale de Droit Penal, Würzburg, 1992.

[18] SIEBER, Ulrich. *The Emergence of Criminal Information Law. In: Amongst Friends in Computers and Law*. Ed. H.W.K. Kaspersen e A. Oskamp. Deventer/Boston: Kluwer Law and Taxation Publishes, 1990, p.118, *apud* GAGLIARDI, Pedro Luiz Ricardo. *Crimes cometidos com uso de computador*. Tese de Doutorado, USP, p.36.

representavam cerca de dois terços do valor de mercado da empresa. A prática do crime foi grandemente facilitada mediante a utilização do sistema de informática do próprio empreendimento. Os diretores da empresa de seguro acrescentaram os dados dos contratos de seguro fictícios aos dados no arquivo. Para fazer isto, fitas magnéticas foram utilizadas contendo dados de antigos contratos já celebrados. Um *software* especialmente redigido foi utilizado para modificar os antigos números de seguro e multiplicar tanto as somas dos prêmios como dos seguros a serem pagos por um fator igual a 1,8 (um vírgula oito). Com isso, o programa de computador assegurou que os dados fictícios entrassem no balanço da empresa. A resseguradora estava prestes a aceitar os textos impressos como prova da existência dos contratos de seguro.

A partir da década de oitenta, os crimes de computador assumiram outra dimensão, quando deixaram de constituir um crime com projeção exclusivamente econômica, passando a incluir ataques a sistemas informáticos pertencentes, por exemplo, a instituições hospitalares.[19]

O surgimento do crime informático em redes abertas de computadores, indicação do nascimento do crime praticado via internet, pode ser datado a partir de 1989, quando investigações criminais levadas a cabo na Alemanha identificaram *hackers* alemães lançando mão de redes de transmissão de dados internacionais para ganhar acesso a dados sigilosos mantidos em sistemas informáticos situados em território americano e inglês, com o objetivo de vendê-los ao serviço secreto russo.[20] Pouco antes, em 1988, o perigo da disseminação de vírus tornou-se óbvio, quando o Internet Worm, criado por um estudante americano, infectou dentro de poucos dias

[19] SIEBER, Ulrich. *The Emergence of Criminal Information Law. In: Amongst Friends in Computers and Law*. Ed. H.W.K. Kaspersen e A. Oskamp. Deventer/Boston: Kluwer Law and Taxation Publishes, 1990, p.118, *apud* GAGLIARDI, Pedro Luiz Ricardo. *Crimes cometidos com uso de computador*. Tese de Doutorado, USP, p.37.

[20] SIEBER, Ulrich. *The Emergence of Criminal Information Law. In: Amongst Friends in Computers and Law*. Ed. H.W.K. Kaspersen e A. Oskamp. Deventer/Boston: Kluwer Law and Taxation Publishes, 1990, p.119, *apud* GAGLIARDI, Pedro Luiz Ricardo. *Crimes cometidos com uso de computador*. Tese de Doutorado, USP, p.37.

cerca de 6.000 sistemas informáticos conectados, que tiveram de ser fechados para desinfecção.[21]

Alguns casos bem sucedidos se assemelham pelo perfil de seus autores, ou seja, pessoas anti-sociais, inteligentes, jovens e solitárias. Estudantes secundaristas, a partir de computadores domésticos, já chegaram a invadir a central de processamento de dados do Chase Manhattan Bank, através de um modem. Dentro do sistema, eles modificaram todos os códigos de entrada para que o banco não pudesse mais acessar seus próprios dados. Outro caso de grande notoriedade foi o de um prisioneiro dos Estados Unidos, que estava trabalhando num programa de ressocialização e que, ao ser matriculado num curso de computação, conseguiu acessar os arquivos sobre os detidos, alterando dados sobre o tempo de cumprimento de pena e, consequentemente, antecipando sua libertação. Também já houve casos em que hackers modificaram dados sobre a dosagem da irradiação a ser ministrada em pacientes, em sistemas informáticos pertencentes a hospitais.[22]

Estima-se uma grande quantidade de crimes informáticos com significativas perdas econômicas, bem como um grande número de casos não detectados em todo o mundo. Na Alemanha, por exemplo, estatísticas criminais apontam 3.067 (três mil e sessenta e sete) casos de crimes informáticos comunicados à polícia, já em 1987 (mil novecentos e oitenta e sete). Cerca de 2.777 (dois mil setecentos e setenta e sete) destes casos foram considerados como constituindo estelionato informático à luz do Código Penal Alemão, artigo 263a. A maioria envolvia terminais bancários automáticos. Também foram identficados casos de violação de segredo informático, dano

[21] SIEBER, Ulrich. *The Emergence of Criminal Information Law. In: Amongst Friends in Computers and Law*. Ed. H.W.K. Kaspersen e A. Oskamp. Deventer/Boston: Kluwer Law and Taxation Publishes, 1990, p.119, *apud* GAGLIARDI, Pedro Luiz Ricardo. *Crimes cometidos com uso de computador*. Tese de Doutorado, USP, p.37.

[22] FRANKEN, Hans. Computing and Security. *In: Amongst Friends in Computers and Law.* Ed. H.W.K. Kaspersen e A. Oskamp. Deventer/Boston: Kluwer Law and Taxation Publishes, 1990, p.131, *apud* GAGLIARDI, Pedro Luiz Ricardo. *Crimes cometidos com uso de computador*. Tese de Doutorado, USP, p.38.

informático, atentado contra a segurança de sistema informático e falsificação informática.[23] Investigações na Alemanha, há cerca de dez anos, já indicavam perdas em função de crimes informáticos da ordem de DM 200.000 a DM 300.000, tendo crescido nos anos seguintes.[24]

As estimativas acerca da extensão da criminalidade informática variam consideravelmente. Embora seja possível uma apresentação geral da diversificação dessa criminalidade, é impossível a apresentação de dados precisos e integrais a respeito do número de casos ocorridos no Brasil e em outros países do mundo, uma vez que, muitas vezes, as vítimas relutam em divulgar o ocorrido, preferindo mantê-lo em segredo.

Apesar das discordâncias, poucos casos relevantes são revelados. A maioria das empresas atingidas raramente divulga seus problemas de segurança ao público. As instituições bancárias, em especial, temem que seus clientes percam a confiança em seus serviços. Caso um serviço bancário virtual for alvo de uma conduta criminosa, uma grande quantidade de dinheiro pode ser perdida num curto espaço de tempo, além de desmoralizar e causar danos à imagem da entidade financeira, seja ela pública ou pivada. A dificuldade de detectação e de comprovação da prática desses crimes, o desconhecimento técnico por parte das autoridades policiais e a ausência de uma legislação adequada sobre o assunto, são outros fatores que contribuem para que suas práticas sejam mantidas em sigilo.

---

[23] Computer –related Crime (Recommendation n. R89 (91). Strasbourg, Council of Europe, 1990, p.16, *apud* GAGLIARDI, Pedro Luiz Ricardo. *Crimes cometidos com uso de computador*. Tese de Doutorado, USP, p.39.

[24] Computer –related Crime (Recommendation n. R89 (91). Strasbourg, Council of Europe, 1990, p.17, *apud* GAGLIARDI, Pedro Luiz Ricardo. *Crimes cometidos com uso de computador*. Tese de Doutorado, USP, p.39.

A criminalidade informática é um fenômeno real, atual e em constante expansão. Os casos tendem a crescer a medida que o número de computadores pessoais e de sistemas informáticos também aumentarem.

A solução para esse problema estaria em adotar não apenas medidas extrajurídicas, medidas de segurança, como já vêm fazendo inúmeras empresas, mas, também, medidas jurídicas, com uma legislação adequada.

CAPÍTULO II – CRIMES DE COMPUTADOR

1.0- Bem jurídico penal

Atualmente, entende-se majoritariamente que a finalidade do Direito Penal é garantir a vida em sociedade das pessoas e também garantir as condições necessárias para que os indivíduos se realizem e desenvolvam sua personalidade.

Dessa forma, procurando atingir essa finalidade, o Estado, observando a vida em sociedade, elege aqueles bens jurídicos que considera fundamentais, cria tipos penais criminalizando condutas que violam tais bens jurídicos, e esse conjunto de normas jurídicas, a grande maioria delas definindo crimes e impondo penas, é, em suma, o Direito Penal.

Pode-se concluir, pois, que a defesa social é o fim do direito punitivo. Definidos os bens jurídicos garantidores da vida em sociedade e de pleno desenvolvimento do indivíduo, o Estado chama a si a tarefa de tutelá-los, e tal tutela se dá penalmente, através da criação de crimes e imposição de sanções.

O Direito Penal tem por escopo fundamental a proteção de bens jurídicos, e não poderia ser diferente em um Regime Democrático de Direito.

Dessa forma, está reservada ao Direito Penal a tarefa de tutelar bens jurídicos fundamentais de uma comunidade, visando, com isso, garantir a estabilidade, garantir a vida em sociedade e o pleno desenvolvimento dos indivíduos. Vê-se, então, que o elemento norteador da tutela criminal é o bem jurídico.

Bem jurídico que, nas palavras de Francisco Assis de Toledo, é "aquele valor ético-social que o direito seleciona, com o objetivo de assegurar a paz social,

colocando sob a sua proteção para que não seja exposto a perigo de ataque ou lesões efetivas".[25]

Para Heleno Cláudio Fragoso[26],

> "o bem jurídico não é apenas um esquema conceitual, visando proporcionar uma solução técnica de nossa questão: é um bem humano ou da vida social que se procura preservar, cuja natureza e qualidade dependem, sem dúvida, do sentido que a norma tem ou que a ela é atribuído, constituindo, em qualquer caso, uma realidade contemplada pelo direito. Bem jurídico é um bem protegido pelo direito: é, portanto, um valor da vida humana que o direito reconhece, e a cuja preservação é disposta na norma".

O renomado jurista português, Figueiredo Dias, destaca que para a referida proteção se faz necessária "uma expressão de um interesse, da pessoa ou da comunidade, na manutenção ou integridade de um certo estado, objeto ou bem em si mesmo socialmente relevante e por isso juridicamente reconhecido como valioso".[27]

Na linguagem jurídica, bens são valores materiais ou imateriais que servem de objeto a uma relação jurídica.[28]

Embora haja, como vimos, uma gama de opiniões a respeito de bens jurídicos, gerando várias conceituações, pode-se afirmar que o Direito Penal, circunda, tutela, dá proteção aos bens jurídicos que são fundamentais para a sociedade.

Portanto, toda a construção tipológica penal, toda a atuação estatal na repressão criminal tem em mira, tem por objetivo, a defesa de bens jurídicos, os quais

---

[25] TOLEDO, Francisco de Assis. *Princípios básicos do direito penal*. 4ª edição, São Paulo: Saraiva, 1991.
[26] FRAGOSO, Heleno Cláudio. *Lições de direito penal*. Rio de Janeiro: Forense, 7 ed., 1985, p. 277/278
[27] DIAS, Jorge Figueiredo. *Questões de direito penal revisitadas*. São Paulo: Editora Revista dos Tribunais, 1999, p.63.
[28] NUNES, Luiz Antonio. *Manual de introdução ao estudo do direito*. São Paulo: Saraiva, 1996, p.121. "O termo "bem jurídico"tem o sentido de valor, utilidade ou interesse de natureza material, econômica ou moral, ou em outras palavras, é tudo aquilo que é protegido pelo Direito, tendo ou não conteúdo ou valorização econômica. Dessa forma, pode-se dizer que o conceito jurídico de "bem" tem significação mais ampla do que o mero conceito econômico de bem".

não são eleitos aleatoriamente, mas definidos na medida de sua importância para a vida do homem em sociedade e para garantir-lhe o desenvolvimento da personalidade, em suma, garantir-lhe a dignidade.

Uma questão fundamental, no entanto, se apresenta. Quais são os bens jurídicos que merecem a tutela penal? De que maneira são identificados para serem tutelados penalmente? Quando se faz necessária a intervenção penal para essa tutela?

Essas indagações se fazem necessárias porque em um Estado Democrático de Direito, e assim é a República Federativa do Brasil, consoante dispõe o art. 1º da Constituição Federal de 1988, que tem o ser humano – e sua dignidade- como centro da organização estatal, deve haver um limite, um norte a ser seguido pelo legislador na tarefa interventiva penal, possibilitando, logicamente, a tutela de bens fundamentais para o cidadão, todavia, impedindo uma ingerência exagerada na vida do indivíduo e da sociedade, evitando-se, assim, o império do poder repressivo do Estado frente ao direito de liberdade da pessoa.

Antônio Henrique Graciano Suxberger[29] destaca a tendência acerca da legitimidade da intervenção penal e do papel da Constituição como verdadeira pauta valorativa dos bens jurídicos dignos de proteção na esfera penal.

[29] Para o autor "acerca da missão do direito penal de exclusiva proteção de bens jurídicos, vê-se que a Constituição traduz uma norma portadora de determinados valores materiais, que conduzem a uma totalidade do ordenamento jurídico: uma unidade de sentido material. A Carta Política, portanto, responde a uma concepção valorativa da vida social e istaura um marco básico de princípios que conformam a convivência da sociedade. Veicula uma pauta de valores e determina diretrizes que devem ser respeitdas por todo o ordenamento jurídico do Estado, onde se inclui também o direito penal. A Constituição assume papel relevante ativo na construção da tipologia penal, na medida em que seleciona mediante critérios e parâmetros os bens jurídicos relevantes na esteira de valores esculpidos pelo constituinte, delineando um determinado modelo de sistema penal e, com isso, lançando as bases de uma política criminal extraída da própria norma fundante do sistema jurídico. O sistema penal, portanto, há de se expressar positivamente, reproduzindo e conformando, os valores constitucionalmente definidos. Esses valores jurídicos fundamentais do ordenamento jurídico estatal – em particular, o penal, por meio de sua norma básica, prestar-se-ão como critérios para medir a legitimidade das diversas manifestações do sistema de legalidade. Assim, como limite do poder estatal ou mesmo como garantia de liberdade, a Constituição representa o poder de fixação dos limites em que há de se situar qualquer expectativa que pretenda converter-se em direito. Num Estado Democrático de Direito, ao direito penal cabe a função de exclusiva proteção de bens fundamentais do seio social, das condições sociais básicas necessárias à livre realização da personalidade de cada indivíduo. É na

Nessa esteira, é a lição de Ivete Senise Ferreira[30], ao concluir que a preocupação do Direito Penal está em assegurar bens e interesses que representem valores essenciais à coexistência social e à plena realização da pessoa humana.

Igualmente, José Francisco de F aria da Costa, ao explicar a trajetória mutável de proteção de bens jurídicos relevantes pelo direito penal asseriu que "a função primacial do direito penal é a de proteger bens jurídicos que revistam dignidade penal".[31]

Assim, podemos extrair que o Direito Penal é o portal de expiação daquelas condutas que atingem a intolerabilidade social, e é o último bastião dos interesses fundamentais para a vida em sociedade e sua completa realização, devendo haver a intervenção penal, pois, em todas as oportunidades em que bens jurídicos de extrema significância, de extrema importância para o pleno desenvolvimento da pessoa humana forem violados.

Sendo o Direito Penal, pois, um instrumento de proteção de bens fundamentais da sociedade, cabendo-lhe a finalidade de garantir a convivência social e as mínimas condições para o pleno desenvolvimento da pessoa humana, consequentemente garantir a dignidade humana, "*ratio essendi*" da sua própria existência, podemos concluir, pois, que os bens jurídicos que são inerentes, condições essenciais para que essa dignidade seja alcançada, são os bens jurídicos a merecerem

---

Cosntituição, portanto, que o legislador deve buscar os bens jurídicos aptos a receber a proteção penal. SUXBERGER, Antônio Henrique Graciano. *Legitimidade da intervenção penal*. Rio de Janeiro: Lumen Juris, 2006, p. 167.

[30] "Essa preocupação norteou a atuação do Direito Penal desde os seus primórdios na defesa de bens e interesses que, em cada sociedade em cada época, foram considerados merecedores da proteção legal porque representavem valores essenciais à coexistência social e à plena realização da pessoa humana". FERREIRA, Ivete Senise . A tutela penal do patrimônio cultural. São Paulo: Revista dos Tribunais, 1995, p.67.

[31] O autor defende que "o bem jurídico assume uma importância primordial para o correto enquadramento de uma qualquer área incriminadora. Isto é: a qualificação do bem jurídico que a norma incriminadora quer tutelar vai determinar, de certa maneira, a própria norma incriminadora. E aqui intromete-se a idéia da contínua mutação do direito penal." COSTA, José Francisco de Faria. *O crime de abuso de informação privilegiada (insider trading) – a informação enquanto problema jurídico – penal*. Coimbra: Editora Coimbra, 2006, p. 35/36.

tutela penal, portanto, tais bens jurídicos penais são o limite e fundamento da tutela criminal.

Além disso, diante de seu caráter subsidiário, o Direito Penal somente deve cuidar de proteger e tutelar bens mais relevantes e imprescindíveis nas relações sociais. O Direito Penal não pode intervir sempre e em todas as ações lesivas da vida em sociedade, mas apenas quando a proteção de valores fundamentais não se mostrar eficaz de outra forma, impondo ao Direito Penal uma atuação como *ultima ratio*.

Não se admite a intervenção penal diante de qualquer afetação ao bem jurídico, mas tão-somente quando as agressões se apresentem intoleráveis no seio social.

Uma das principais características do atual direito penal é essa opção de um ordenamento jurídico-penal que não busque proteger, nem querer proteger, todos os bens jurídicos, mas tão-somente bens certos e determinados, aqueles que acrescentem à dignidade penal, deixando para a esfera do direito civil e outras tantas questões que, por sua própria natureza, devem estar distanciadas dos valores essenciais do direito penal.[32]

Assim, neste novo ramo do Direito Penal, denominado de Direito Penal da Informática, pode-se falar que há um bem jurídico autônomo identificado? O que exatamente se busca proteger?

Com a difusão da tecnologia informática, cada vez mais indispensável e presente nas relações sociais, o Direito Penal deve se preocupar em estabelecer valores penalmente relevantes, criando normas protetoras com o escopo de garantir a segurança dessas relações.

Tal proteção não deve ser limitada a bens jurídicos tradicionalmente reconhecidos e lesionados com o uso da tecnologia informática, mas, sim, deve ser

[32] FARIA COSTA, José Francisco de. *Direito penal da comunicação – alguns escritos*. Coimbra : Coimbra Editora, 1999, p. 63, *apud* LIMA, Paulo Marco Ferreira. *Crimes de computador e segurança nacional*. Campinas: Millennium Editora, 2006, p. 10.

estendida a outros bens e valores recentemente surgidos com a criação e proliferação dos computadores.

Nesse sentido, Ivette Senise Ferreira destaca que

> "a informatização crescente das várias atividades desenvolvidas individual ou coletivamente na sociedade veio colocar novos instrumentos nas mãos dos criminosos, cujo alcance ainda não foi corretamente avaliado, pois surgem a cada dia novas modalidades de lesões aos mais variados bens e interesses que incumbe ao Estado tutelar, propiciando a formação de uma criminalidade específica da informática, cuja tendência é aumentar quantitativamente e, qualitativamente, aperfeiçoar os seus métodos de execução". [33]

Para delimitar em que sentido se dará a proteção penal na esfera do direito informático, é imprescindível que se identifique qual o bem jurídico a ser penalmente tutelado nesta área, indagando, ainda, se há na estrutura constitucional a possibilidade de amparo pelo direito penal. Sempre considerando o que já foi afirmado, de tal ramo do direito deve somente agir na preservação dos bens mais relevantes e imprescindíveis das relações sociais, sempre dentro dos limites da intervenção mínima.[34]

No tocante aos bens jurídicos passíveis de afetação com os delitos informáticos, podemos identificar dois grupos de valores que merecem amparo específico pela legislação penal.

No primeiro deles estão os bens jurídicos já tradicionalmente protegidos pelo Direito Penal, tais como a honra, a vida, o patrimônio, a integridade física, a fé pública, a propriedade industrial etc., que são violados por um novo *modus operandi*,

---

[33] FERREIRA, Ivette Senise. *A criminalidade informática*. *In*: LUCCA, Newton de, SIMÃO FILHO, Adalberto (Coordenadores) e outros. *Direito e internet – aspectos jurídicos relevantes*. 2ª edição, São Paulo: Quartier Latin, 2005, p.208.

[34] LIMA, Paulo Marco Ferreira. *Crimes de computador e segurança nacional.* Campinas: Millennium Editora, 2006, p. 16.

pois o que separa os crimes de computador dos crimes comuns é a utilização da máquina para atingir seu objetivo em proveito próprio ou para lesionar outrem.

A título de exemplo, podemos apontar o estelionato, cuja figura típica consiste na obtenção de vantagem ilícita com prejuízo alheio mediante a utilização de inúmeros expedientes. Se praticada a conduta com o uso do computador, o agente está incurso nas penas do dispositivo penal, sendo desnecessária a criação de uma nova figura penal a fim de se coibir a conduta ilícita, pois houve alteração tão-somente da forma, do instrumento da prática delituosa.

Sob essa optica, nossa legislação penal, com alguns ajustes referentes a aumento de pena, está apta a coibir esses delitos, pois a conduta humana ilícita ali perpetrada, seja ativa ou omissiva, já está tipificada na norma, passível, portanto, de sanção penal.

Entretanto, nem todas as condutas praticadas através dos computadores recaem sobre os bens jurídicos tradicionais.

No segundo grupo de valores merecedores de proteção legal estão os objetos informáticos propriamente ditos, como o *hardware*, *software*, dados, documentos eletrônicos etc.

No setor de informática, a necessidade de proteção ao *software* e ao *hardware* se apresenta como ponto crucial para o desenvolvimento das nações, para o controle de mercados e possibilidade (ou impossibilidade) de transferência de tecnologias.

A possibilidade de o equipamento eletrônico, ou *hardware*[35], ser objeto material de conduta ilícita não guarda nenhuma dificuldade e pode ser resolvida à luz do direito penal comum. O *mouse*, o teclado, o visor, a cpu, ou seja, todos os equipamentos

[35] "*Hardware* é o termo usado para designar os equipamentos que compõem o computador. É o componente físico da máquina". BASTOS, Aurélio Wander. *Dicionário brasileiro de propriedade industrial e assuntos conexos.* Rio de Janeiro: Lumen Juris, 1997, p.119.

que compõem o *hardware* e que pode ser materialmente determinado, são passíveis de ações ilícitas e, por serem considerados coisa móvel, encontram proteção na legislação penal.

Segundo Maria Helena Junqueira Reis, coisa "é toda susbstância corpórea material, ainda que não tangível, suscetível de apreensão e que tem um valor qualquer".[36] No mesmo sentido é o conceito trazido por Luiz Regis Prado, para quem a expressão "coisa", "é tudo o que possa ser objeto de ação física de crime (material e corpórea), sendo passível de deslocamento, remoção ou apreensão, enfim, podendo ser transportada de um lugar para outro". [37]

Na mesma esteira, Liliana Minardi Paesani entende que o

> "Sistema informático em sua configuração complexa constituída por computadores e periféricos, *software* de base e aplicativos, suportes magnéticos e componentes de memórias auxiliares, será qualificado como universalidade de coisas móveis. O Sistema informático, analisado em sua configuração mínima, é uma coisa composta que apresenta algumas particularidades. É difícil individualizar uma coisa principal e outras acessórias, pois todas são partes complementares entre si e cada uma é integrante da outra".[38]

Dessa forma, considerando o equipamento como coisa, pode-se vizualizá-lo como objeto material de ação delitiva, passível, por exemplo, de furto, dano, receptação, roubo e apropriação indébita.

Diferente não é, também, a proteção recebida pelos *softwares* ou programas de computador.

---

[36] *Computer Crimes: a criminalidade na era dos computadores*. Belo Horizonte: Del Rey, 1996, p.39.
[37] PRADO, Luiz Regis. *Curso de direito penal brasileiro*. Parte especial, vol. 04, São Paulo: Editora Revista dos Tribunais, 2005, p. 369.
[38] PAESANI, Liliana Minardi. Direito de informática – comercialização e desenvolvimento internacional de software. 2ª edição, São Paulo: Editora Atlas, 1999, p.25.

Software é uma sequência de instruções a serem seguidas e/ou executadas, na manipulação, redirecionamento ou modificação de um dado/informação ou acontecimento. *Software* também é o nome dado ao comportamento exibido por essa seqüência de instruções quando executada em um computador ou máquina semelhante. Tecnicamente, é o nome dado ao conjunto de produtos desenvolvidos durante o processo de *software*, o que inclui não só o programa de computador propriamente dito, mas também manuais, especificações, planos de teste, etc.[39]

O programa de computador foi pela primeira vez analisado juridicamente de forma sistêmica por Renato Borruso[40], o qual delineou o sistema informático como um conjunto de elementos *software*, *hardware* e *firmware*[41].

O programa de computador em si desprende-se de todo e qualquer meio físico (*hardware*) que possa lhe servir de suporte. Dessa maneira, é possível classificá-lo enquanto linguagem de programação como um bem jurídico incorpóreo, também chamado de imaterial, pois não possui existência física, mas abstrata.

O programa de computador se inclui entre as obras intelectuais de expressão linguística, na medida em que todo *software* exige, antes de tudo, uma anotação, que constitui na linguagem de computação, e que permitirá um procedimento, do qual se obterão resultados.

O *software* é uma criação intectual, e por ser assim considerada, é regulada e protegida à luz dos direitos autorais.[42]

---

[39] Conceito dado por Wikipédia (enciclopédia virtual). Acesso em: http://pt.wikipedia.org/wiki/Software, em 11/03/2008, às 16h03min.

[40] BORRUSO, Renato. *Civiltá del computer*. Milão: Ipsoa, 1978, p.25, *apud*, WACHOWICZ, Marcos. *O programa de computador como objeto do direito informático*, p.338. *In*: ROVER, Aires José (Organizador). *Direito e informática.* Barueri – SP: Manole, 2004.

[41] "Considera-se *firmware* rotinas de *software* armazenadas em memória disponível apenas para leitura (ROM). Pressupõe a existência de uma parte física (o circuito/*hardware* do qual é constituída a memória), e outra intangível (conjunto de instruções que compõe as rotinas de *software*). BASTOS, Aurélio Wander. *Dicionário brasileiro de propriedade industrial e assuntos conexos*. Rio de Janeiro: Lumen Juris, 1997, p.336.

O bem jurídico pelo legislador é, portanto, o produto da criação intelectual. Entretanto, ressalte-se que o direito autoral somente passa a existir no momento em que se materializa, seja qual for o "*corpus mechanicus*". As idéias em si não são protegidas.[43]

Os programas de computador merecem estar protegidos, uma vez que são facilmente copiáveis. Ao contrário dos livros, é possível copiar um programa de computador com milhões de letras e números em poucos segundos, o que se dá graças à própria evolução tecnológica. Para tanto, transfere-se o conteúdo do suporte físico em que ele se encontra para outro, que pode ser ou não da mesma natureza do primeiro.

Na maioria das vezes, não é necessário ser um perito para realizar cópias de programas. Essa atividade nem sempre é legal e, quando realizada ilicitamente denomina-se, no meio técnico, pirataria. Os agentes do ato ilícito são os piratas. As cópias piratas representam hoje a maioria do total de cópias circulantes em todo o mundo, o que se dá graças à difícil fiscalização e do avanço paralelo de modernas técnicas de cópias de programas que visam burlar toda e qualquer forma de proteção tecnológica contida nos mesmos.

Justamente para evitar injustiças é que o Direito se faz necessário. A implementação de normas de proteção à propriedade intelectual está diretamente relacionada com as possibilidades de desenvolvimento econômico. Muitas são as formas utilizadas, cada qual com resultados diferentes, satisfazendo ou não os anseios do setor e contribuindo ou prejudicando os interesses nacionais.

---

[42] O art. 7, inciso XII, da Lei 6.910/98 diz: "Sào obras intelectuais protegidas as criações do espírito, expressas por qualquer meio ou fixadas em qualquer suporte, tangível ou intangível, conhecido ou que se invente no futuro, tais como: (...) XII- os programas de computador. Parágrafo 1: Os programas de computador são objeto de legislação específica, observadas as diposições desta Lei que lhes sejam aplicáveis.

[43] OPICE BLUM, Renato M. S., ABRUSIO, Juliana Canha. *Direito e internet: Direito autoral eletrônico. In*: Caderno Jurídico da Escola Superior do Ministério Público do Estado de São Paulo, ano 2, vol. 1, nº4, julho de 2002, p.52.

José de Oliveira Ascensão[44] defende a proteção jurídica dos programas de computador por entender que, ao delineá-los como uma criação passível de tutela jurídica e, conceituá-los como objeto de propriedade intelectual, significa entendê-los como atividade meio, e que envolto na sociedade de informação adquire múltiplos contornos e formas de comercialização, ora requerendo proteção pelas esferas do direito civil e do direito penal, ora pelo direito internacional.

A proteção jurídica dos programas de computador no campo internacional, começou a ficar delineada pela Convenção de Concessão de Patentes Européias, na Convenção de Munique em 1973, tendo aí consagrada a impossibilidade de atribuição de patentes a programas de computador.[45]

Os demais países europeus paulatinamente adotaram em suas legislações internas tal orientação. A Alemanha e a França em 1985 regulamentaram o *software* como tutelado pelo Direito Autoral.[46]

Na Argentina, por meio do Decreto 165/94, foram incorporadas à legislação de Propriedade Intelectual disposições específicas sobre o *software* e base de dados, caracterizando o *software* como bem intelectual de forma ampla, abrangendo, para efeitos de proteção da lei, além do programa de computador em si, os desenhos, bem como toda a documentação técnica com a finalidade de exploração, suporte e treinamento para desenvolvimento, uso e manutenção do *software*.[47]

No Brasil, a regulamentação da propriedade intelectual sobre programas de computador e sua comercializaçào no país foi feita pela Lei 7.646/87, e que trouxe dois

---

[44] ASCENSÃO, José de Oliveira. *Direito autoral*. Rio de Janeiro: Renovar, 1997.
[45] WACHOWICZ, Marcos. *O programa de computador como objeto do direito informático,* p.344/345. *In*: ROVER, Aires José (Organizador). *Direito e informática.* Barueri – SP: Manole, 2004.
[46] WACHOWICZ, Marcos. *O programa de computador como objeto do direito informático,* p.345. *In*: ROVER, Aires José (Organizador). *Direito e informática.* Barueri – SP: Manole, 2004.
[47] WACHOWICZ, Marcos. *O programa de computador como objeto do direito informático,* p.347. *In*: ROVER, Aires José (Organizador). *Direito e informática.* Barueri – SP: Manole, 2004.

artigos com previsão de condutas criminosas: o art. 35[48], que se referia ao direito do autor de programa de computador, e o art. 37[49] se preocupava com a importação, exposição ou manutenção em depósito, para fins de comercialização, programas de computador de origem externa não cadastrados.

Atualmente, as Leis 9.609 e 9.610, ambas de 19.02.1998, revogaram a lei supra mencionada e dispõem, respectivamente, sobre a proteção da propriedade intelectual de programa de computador e sua comercialização, e altera, atualiza e consolida a legislação sobre direitos autorais.

Além desse fator, no que se refere às infrações e penalidades, há disposição expressa e específica no art. 12 da Lei 9.609/98,[50] que tipifica a conduta de violar direito autoral de programa de computador. O referido dispositivo prevê, ainda, como qualificadora da violação, a sua reprodução total ou parcial com a finalidade de comercialização, punindo-se, por fim, aquele que vende, expõe à venda, introduz no País, adquire, oculta ou tem em depósito, original ou cópia de programa de computador, produzido com violação de direito autoral.

A disponibilização de obras pela internet implicou novos contornos para os bens intelectuais, como também provocou o aparecimento de novos bens, que ganharam rapidamente relevo jurídico. Com a mesma velocidade de inserção da internet na sociedade, o programa de computador começou a ser comercializado pela rede.

---

[48] "Art. 35. Violar direito do autor de programa de computador: Pena – detenção de 6 (seis) meses a 2 (dois) anos e multa."

[49] "Art. 37. Importar, export, manter em depósito, para fins de comercilaização, programas de computador de origem externa não cadastrados: Pena – detenção de 1 (um) a 4 (quatro) anos e multa."

[50] "Art. 12. Violar direitos de autor de programa de computador: Pena- Detenção de 6 (seis) meses a 2 (dois) anos ou multa. Parágrafo 1. Se a violação consistir na reprodução, por qualquer meio, de programa de computador, no todo ou em parte, para fins de comércio, sem autorização expressa do autor ou de quem o represente: Pena- reclusão de 1 (um) a 4 (quatro) anos ou multa. Parágrafo 2. Na mesma pena do parágrafo anterior incorre quem vende, expõe à venda, introduz no País, adquire, oculta ou tem em depósito, original ou cópia de programa de computador, produzido com violação de direito autoral.

As fronteiras e barreiras alfandegárias construídas para os produtos corpóreos não possuem a mesma eficácia, particularmente no que tange à distribuição de um bem imaterial como o *software*, que, negociado pela internet, demonstra cabalmente estarem os instrumentos de controle ultrapassados. Isso porque inexiste de forma eficaz um controle de emissão de cópia dos programas de computador distribuídos na rede.[51]

A disponibilização de um programa de computador via internet pode se operacionalizar através de *home page* do titular dos direitos autorais do *software*. Os mecanismos de comandos de downloads, por mais fiscalizados que sejam, possuem limites para verificar e dificuldades técnicas de coibir a livre utilização por terceiros, que, sem prévio conhecimento do titular, podem duplicar ilegalmente os programas de computador.[52]

A proteção da propriedade intelectual na distribuição de *software* pela internet deve ser mensurada pela empresa produtora, não só observando aspectos técnicos de segurança, mas também, e em primeiro lugar, entabular métodos de proteção, considerando os diferentes aspectos dos *softwares*, cada um dos quais portadores de valor econômico-jurídico que requer proteção específica.

---

[51] "Agrega-se à problemática da dimensão da Internet, da gama de pessoas a que atinge e da velocidade com que propaga arquivos e informações, o fato desta ser um meio de comunicação 'virtual'. Esta característica dificulta a determinação de critério espaciais e temporais de ocorrência de fatos, como a reprodução indevida de uma obra, muitas vezes não sendo possível identificar a origem de um arquivo, bem como o momento de sua criação. A falta de regulamentação desse novo suporte material também agrava a situação jurídica dos autores que têm na Internet as suas obras veiculadas, aplicando-se até a presente data somente a Lei 9.610/98 e a Lei 9.609/98, as quais se mostram insuficientes para resguardar os direitos envolvidos. A soma das características acima mencionadas demonstra que a internet é um meio de comunicação de difícil fiscalização e de escassa regulamentação, tornando propícia a violação de direitos autorais". GOMES DOS SANTOS, Lígia Carvalho. *Direitos autorais na internet. In*: SCHOUERI, Luís Eduardo (Organizador). *Internet: o direito na era virtual*. Rio de Janeiro: Forense, 2001, p.360.

[52] Nesse sentido, é o que assevera Issac Pilati, para o qual "com o advento e a popularização cada vez maior da Internet, cresce de importância a dimensão internacional da tutela desses direitos; mas os grandes interesses econômicos parecem não reunir, eticamente força suficiente para censurar a auto-estrada da comunicação, e conformá-la, em seu benefício. Na verdade, a Internet está decretando a dessuetude da legislação vigente, de Direitos Autorais; as demandas judiciais, especialmente as travadas nos Estados Unidos, deverão indicar novos caminhos a tomar". PILATI, Issac. *Direitos autorais e internet*. *In*: ROVER, Aires José (Organizador). *Direito, sociedade e informática: limites e perspectivas da vida digital*. Florianópolis: Fundação Boiteux, 2000, p.134.

Com efeito, o *software* sendo um bem imaterial não é passível de compra e venda, mas, sim, de cessão de direito. Portanto, no momento em que se adquire um programa de computador, o negócio jurídico que se realiza é a licença do uso de um programa de computador, num meio físico (*hardware*) que lhe serve de suporte e é um bem acessório.

Na esfera cível, há a possibilidade, nos contratos de licença de uso, de incidência de multa e outras penalidades pela programação de cópias efetuadas sem autorização, como pagamento duplicado do valor de cada cópia feita sem autorização.[53]

No que tange à classificação de bens principais e acessórios, o programa de computador se apresenta como um bem principal, vale dizer, que tem existência própria, não dependendo de outro para existir. Assim, o programa de computador é o bem principal, sendo considerado como acessório o suporte físico (disquete, CD-Rom, etc).

Em suma, os programas de computador podem ser considerados como objeto material de ação delitiva, situação em que o bem jurídico afetado é o direito autoral.

Por fim, outro bem jurídico que merece proteção legal é a informação. A informação que é o resultado do tratamento computacional dos dados brutos armazenados nos ambientes computacionais, no mais das vezes, distribuídos, é vista como bem jurídico supra-individual, uma vez que há que se levar em conta que o avanço tecnológico que representa a internet e os problemas apresentados pelo uso generalizado dos sistemas informáticos fazem surgir necessidades próprias para o direito penal, que agora tem diante de si um novo interesse social digno de proteção: a informação e sua transmissão através de sistemas telemáticos.

[53] PEREIRA, Elizabeth Dias Kanthack. *A proteção jurídica do software no brasil*. Curitiba: Juruá, 2004, p. 66.

Nesse raciocínio, trazemos à baila o ensinamento doutrinário de Marcelo Batlouni Mendroni, fundamental para a compreensão do que vem a ser esse bem jurídico supra-individual que é a informação, a saber,

> "não dista muito o tempo em que a manipulação das informações ensejavam a idéia de uma atividade específica das Forças Armadas e, fora delas, somente encontravam campo nos estabelecimentos bancários, atuando principalmente na área de informações de crédito. Deste isolamento decorrem distorções, quase sempre desfavoráveis, e conceitos que geram naturais temores que no geral já não se justificam na atualidade. (...) Assim, qualquer que seja o campo da atividade, haverá sempre a constante busca de dados, elementos, estatísticas e, em última análise, a procura da informação para instruir os objetivos, formas de atuações e decisões (...) É um instrumento eficaz para as projeções futuras, mas esta eficiência é obtida sempre na razão direta da relevância, da oportunidade e da precisão das informações. (...) Informação é o conhecimento dos aspectos, circunstâncias e/ou consequências de qualquer ato, de atuação de pessoa, ou ainda o resultado objetivo do estudo de uma análise, integração e interpretação dos informes que lhes forem pertinentes".[54]

O armazenamento de informação é a substantivação de uma "coisa" que não é matéria sem energia, a despeito de que essa "coisa" esteja armazenda em algum substrato físico, como mídias ópticas ou magnéticas. Importa ressaltar que o substrato físico, no mais das vezes, tem valor ínfimo se comparado ao conteúdo informacional, os dados em si.

Aboso & Zapata[55] defendem que, além disso, parece não haver dúvida de que dita informação deve ser o objeto de tutela de um direito penal orientado à evitação de riscos e que o conteúdo de dita informação não tenha que se limitar ao seu significado ôntico, isto é, ao plano inerente à pessoa em relação com sua intimidade, a

[54] MENDRONI, Marcelo Batlouni. *Curso de investigação criminal*. São Paulo: Juarez de Oliveira, 2002, p.285/286.

[55] ABOSO, Gustavo Eduardo & ZAPATA, María Florencia. Cibercriminalidad y derecho penal. Buenos Aires: Julio Cesar Faria Editor, 2006, p.19. Original em espanhol: "*Parece no haber duda en que dicha información debe ser el objeto de tutela de um derecho penal orientado a la evitación de riesgos, y que el contenido de dicha informatión no tiene que limitarse a su significado óntico, es decir, al plano inherente de la persona en relación con su intimidad, la cual, por otra parte, ya se encuentra regulada, en mayor o menor medida, en los códigos penales*".

qual, por outra parte, já se encontra regulada, em maior ou menor medida, nos códigos penais.

A sociedade da informação faz com que os crimes de computador tenham uma configuração dos delitos pluriofensivos, pois, de forma paralela, ter-se-á, sempre, necessidade de proteção de antigos e novos interesses, estes derivados da sociedade global do risco informático e da informação, isto é, a proteção da informação em si mesma, dos dados informáticos, que são a representação daquela, e da confiabilidade e da segurança coletiva dos meios e sistemas de tratamento e transferência da informação, sem os quais não existirá a necessária unidade sistemática como que para merecerem todas essas novas modalidades a consideração de uma categoria substantiva penal específica e própria, e não meramente criminológica ou funcional. Devem se conjugar, ademais, com a proteção de bens jurídicos tradicionais, tanto individuais, quanto coletivos. [56]

Esses novos bens jurídicos podem ser facilmente constatados. Uma sociedade complexa que é dependente do parque tecnológico que armazena, processa, disponibiliza e transporta o valioso bem incorpóreo que é a informação[57], precisa

---

[56] CANTO, Enrique Rovira del. *Delincuencia informática y fraudes informáticos.* Granada: Editorial Comares, 2002, p.71. Original em espanhol: "*su configuración como um delito pluriofensivo, el que teniendo siempre concurrente la protección de los nuevos intereses derivados de la sociedad global del riesgo informático y de la información (la información em si misma, los datos informáticos, que son la representación de aquélla, y la fiabilidad y seguridad colectiva em los médios y sistemas de tratamiento y transferência de la información), sin los cuales no existirá la precisa unidad sistemática como para merecer us diversas modalidades la consideración de uma categoria substantiva penal específica y propia, y no meramente criminológica o funcional, deben conjugarse además com la protección de bienes jurídicos tradicionales, bien individuales bien colectivos.*"

[57] A informação tem tanta relevância em nosso ordenamento que a Cosntituição Federal de 1988 arrolou o verbete em inúmeras situações, a saber:
Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
XIV - é assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício profissional;
XXXIII - todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado;
LXXII - conceder-se-á "habeas-data":

a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público;
b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo;
Art. 37. A administração pública direta e indireta de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios obedecerá aos princípios de legalidade, impessoalidade, moralidade, publicidade e eficiência e, também, ao seguinte:
XXII - as administrações tributárias da União, dos Estados, do Distrito Federal e dos Municípios, atividades essenciais ao funcionamento do Estado, exercidas por servidores de carreiras específicas, terão recursos prioritários para a realização de suas atividades e atuarão de forma integrada, inclusive com o compartilhamento de cadastros e de informações fiscais, na forma da lei ou convênio.
§ 3º A lei disciplinará as formas de participação do usuário na administração pública direta e indireta, regulando especialmente:
II - o acesso dos usuários a registros administrativos e a informações sobre atos de governo, observado o disposto no art. 5º, X e XXXIII;
§ 7º A lei disporá sobre os requisitos e as restrições ao ocupante de cargo ou emprego da administração direta e indireta que possibilite o acesso a informações privilegiadas.
Art. 50. A Câmara dos Deputados e o Senado Federal, ou qualquer de suas Comissões, poderão convocar Ministro de Estado ou quaisquer titulares de órgãos diretamente subordinados à Presidência da República para prestarem, pessoalmente, informações sobre assunto previamente determinado, importando crime de responsabilidade a ausência sem justificação adequada.
§ 2º - As Mesas da Câmara dos Deputados e do Senado Federal poderão encaminhar pedidos escritos de informações a Ministros de Estado ou a qualquer das pessoas referidas no caput deste artigo, importando em crime de responsabilidade a recusa, ou o não - atendimento, no prazo de trinta dias, bem como a prestação de informações falsas.
Art. 53. Os Deputados e Senadores são invioláveis, civil e penalmente, por quaisquer de suas opiniões, palavras e votos.
§ 6º Os Deputados e Senadores não serão obrigados a testemunhar sobre informações recebidas ou prestadas em razão do exercício do mandato, nem sobre as pessoas que lhes confiaram ou deles receberam informações.
Art. 58. O Congresso Nacional e suas Casas terão comissões permanentes e temporárias, constituídas na forma e com as atribuições previstas no respectivo regimento ou no ato de que resultar sua criação.
§ 2º - às comissões, em razão da matéria de sua competência, cabe:
III - convocar Ministros de Estado para prestar informações sobre assuntos inerentes a suas atribuições;
Art. 71. O controle externo, a cargo do Congresso Nacional, será exercido com o auxílio do Tribunal de Contas da União, ao qual compete:
VII - prestar as informações solicitadas pelo Congresso Nacional, por qualquer de suas Casas, ou por qualquer das respectivas Comissões, sobre a fiscalização contábil, financeira, orçamentária, operacional e patrimonial e sobre resultados de auditorias e inspeções realizadas;
Art. 93. Lei complementar, de iniciativa do Supremo Tribunal Federal, disporá sobre o Estatuto da Magistratura, observados os seguintes princípios:
IX todos os julgamentos dos órgãos do Poder Judiciário serão públicos, e fundamentadas todas as decisões, sob pena de nulidade, podendo a lei limitar a presença, em determinados atos, às próprias partes e a seus advogados, ou somente a estes, em casos nos quais a preservação do direito à intimidade do interessado no sigilo não prejudique o interesse público à informação;
Art. 129. São funções institucionais do Ministério Público:
VI - expedir notificações nos procedimentos administrativos de sua competência, requisitando informações e documentos para instruí-los, na forma da lei complementar respectiva;
Art. 139. Na vigência do estado de sítio decretado com fundamento no art. 137, I, só poderão ser tomadas contra as pessoas as seguintes medidas:
III - restrições relativas à inviolabilidade da correspondência, ao sigilo das comunicações, à prestação de informações e à liberdade de imprensa, radiodifusão e televisão, na forma da lei;
Art. 181. O atendimento de requisição de documento ou informação de natureza comercial, feita por autoridade administrativa ou judiciária estrangeira, a pessoa física ou jurídica residente ou domiciliada no País dependerá de autorização do Poder competente.
Art. 202. O regime de previdência privada, de caráter complementar e organizado de forma autônoma em relação ao regime geral de previdência social, será facultativo, baseado na constituição de reservas que garantam o benefício contratado, e regulado por lei complementar.

construir anteparos de controle social fortes, tanto para a informação em si, quanto para esse parque tecnológico que possibilita o fluxo de informações.

Nessa esteira, no mais das vezes, em crimes de alta tecnologia, onde o bem jurídico penalmente relevante a ser protegido é a informação, estar-se-ia, segundo José Francisco de Faria Costa,

> "(...) diante de um crime de perigo abstrato. Um crime, por consequência, em que o perigo não é sequer elemento do tipo, mas apenas motivação do legislador. Uma infração que tem, apesar de tudo e quanto a nós, de se projetar – para que seja constitucionalmente válida – em uma qualquer refração que encontre eco naquilo a que apelidamos de ofensividade de cuidado de perigo."[58]

E, tendo em conta o paradigma clássico de bem juurídico material ou fisicamente detectável, tal como o patrimônio, quando se trata de proteção penal à informação,

> "(...) as incriminações definíveis ou tipicamente conformadas pela verificação de um resultado proibido tornam-se ineficazes ou tendencialmente ineficazes, na sua função protetora, quando os bens jurídicos em causa apresentam um elevado grau de imaterialidade".[59]

Discorrendo sobre esses novos bens jurídicos, Luis Reyna Alfaro assinalou que

> "os constantes avanços tecnológicos em matéria de informática têm propiciado a aparição de novos conceitos, gerando, por isso, a modificação de outros tantos,

---

§ 1° A lei complementar de que trata este artigo assegurará ao participante de planos de benefícios de entidades de previdência privada o pleno acesso às informações relativas à gestão de seus respectivos planos.

Art. 220. A manifestação do pensamento, a criação, a expressão e a informação, sob qualquer forma, processo ou veículo não sofrerão qualquer restrição, observado o disposto nesta Constituição.

§ 1º - Nenhuma lei conterá dispositivo que possa constituir embaraço à plena liberdade de informação jornalística em qualquer veículo de comunicação social, observado o disposto no art. 5º, IV, V, X, XIII e XIV.

[58] COSTA, José Francisco de Faria. *O crime de abuso de informação privilegiada (insider trading) – a informação enquanto problema jurídico – penal*. Coimbra: Editora Coimbra, 2006, p.73/74.

[59] COSTA, José Francisco de Faria. *O crime de abuso de informação privilegiada (insider trading) – a informação enquanto problema jurídico – penal.* Coimbra: Editora Coimbra, 2006, p.73/74.

> enriquecendo-os na maioria das ocasiões, assim o conteúdo do termo '*informação*', que segundo a definição da Real Academia da Língua Espanhola significa: '*inteirar, dar notícia de algo*' e que em termos leigos pode significar tão-só mera acumulação de dados, tem se ampliado, transformando-se como adverte Gutiérrez Francés: '*em um valor, um interesse social valioso, com frequência qualitativamente distinto, dotado de autonomia e objeto de tráfego*'." [60]

Ademais, segundo o autor[61], hoje em dia, de nada adianta apenas possuir informação, mas, sim, há que se deter a capacidade de armazenar, processar, tratar e transmitir a informação, pois é esse conjunto de tarefas automatizadas que confere vantagem econômica ao proprietário ou detentor de informação, no âmbito de um sistema capitalista.

Luis Reyna Alfaro afirmou ainda, que "o bem jurídico 'informação' encontrar-se-ia entre os chamados delitos sócio-econômicos e por isso suas repercussões transcenderiam às próprias bases do sistema sócio-econômico, isto é, estar-se-ia diante de um bem jurídico coletivo".[62]

Arrematando a importância da informação como bem jurídico supra-individual penalmente relevante, assinalou que

---

[60] ALFARO, Luis Reyna. *Fundamentos para la protección penal de la información como valor económico de empresa. In*: Revista de Derecho Informático, vol. 9, abril/99. Disponível em: http://www.alfaredi.org/rdi-articulo.shtml?x=259. Acesso em: 09/12/2008, às 12horas e 55 minutos. Traduziu-se, livremente, o trecho citado: "*Los constantes avances tecnológicos en matéria informática han propiciado la aparición de nuevos conceptos, gerando asimismo la modificación de otros tantos, enriqueiéndolos la mayoría de ocasiones, así el contenido del término 'información', que según la definición de la Real Academia de la Lengua Española significa: 'enterar, dar notícia de algo' y que en términos legos hubiera significado tan sólo una simple acumulación de datos, se ha ampliado, transformándose como adverte Gutiérrez Francés: 'en un valor, un interés social valioso, con fecuencia cualitativamente distinto, dotado de autonomia y objeto del tráfico*'."

[61] ALFARO, Luis Reyna. *Fundamentos para la protección penal de la información como valor económico de empresa. In*: Revista de Derecho Informático, vol. 9, abril/99. Disponível em: http://www.alfaredi.org/rdi-articulo.shtml?x=259. Acesso em: 09/12/2008, às 12horas e 55 minutos.

[62] ALFARO, Luis Reyna. *Fundamentos para la protección penal de la información como valor económico de empresa. In*: Revista de Derecho Informático, vol. 9, abril/99. Disponível em: http://www.alfaredi.org/rdi-articulo.shtml?x=259. Acesso em: 09/12/2008, às 12horas e 55 minutos. Original em espanhol: "*el bien jurídico 'informacíon'se encontraria encardinado dentro de los llamados delitos socio-economicos y por ello sus repercusiones transcenderían a las propias bases del sistema socio-económico, esto es, estamos a través de bien jurídico colectivo*".

> "a presença de um interesse social vital não credita *per si* a existência de um bem jurídico penalmente relevante, é necessário também que este reúna os requisitos de merecimento ou importância social e necessidade de proteção em sede penal, próprios de uma concepção do bem jurídico penal de índole político-criminal como a que propugnamos, devendo-se deslindar sua presença para a posterior confirmação da nossa tese.
> A respeito da valoração do merecimento de proteção ou importância social do interesse deve ter-se em conta que este se refere – como disse Rodriguez Morullo – à generalidade dos componentes do grupo social e não apenas à minoria ou um setor social determinado, não obstante a valoração daqueles interesses que, como a informação, têm um imanente caráter coletivo, deve se abordar em função de sua transcedência para os indivíduos, o que corresponderia aos lineamentos próprios do Estado Democrático de Direito, dessa maneira, como assinala Mir Puig, '*a valoração da importância de um determinado interesse coletivo exigirá a comprovação do dano que cause a cada indivíduo sua vulneração'*, isto é, não resulta suficiente para a comprovação do merecimento de proteção que o interesse social transcenda à generalidade é preciso que sua lesão ou sua colocação em perigo possua capacidade para provocar danos aos indivíduos integrantes do grupo social."[63]

Enrique Rovira del Canto, por sua vez, aduziu que o bem jurídico supra-individual a ser protegido, em primeiro lugar, seria a informação, e, em segundo lugar, os dados informáticos e os ambientes computacionais distribuídos, por conta das

[63] ALFARO, Luis Reyna. *Fundamentos para la protección penal de la información como valor económico de empresa. In*: Revista de Derecho Informático, vol. 9, abril/99. Disponível em: http://www.alfaredi.org/rdi-articulo.shtml?x=259. Acesso em: 09/12/2008, às 12horas e 55 minutos. Original em espanhol: "*La presencia de un interés social vital no acredita per se la existencia de un bien jurídico penalmente relevante, es necesario tambien que este reúna los requisitos de merecimento o importancia social y necesidad de protección en sede penal, propios de una concepción del bien jurídico penal de índole político-criminal como la que propugnamos, debiéndose deslindar su presencia para la posterior confirmación de nuestra tesis. Respecto a la valoración del merecimento de protección o importancia social del interés debe tenerse en claro que este se refiere – como dice Rodriguez Mourullo – a la generalidad de los componentes del grupo social y no sólo a la minoria o un sector social determinado, no obstante, la valoración de aquellos intereses que, como la información, tienen un inmanente carácter colectivo, debe abordarse en función a su trascendencia para los indivíduos, lo que se corresponderia a los lineamentos propios del modelo de Estado Social y Democrático de Derecho, de esta manera, como señala Mir Puig, 'la valoración de la importancia de un determinado interés colectivo exigirá la comprobación del daño que cause a cada individuo su vulnaración', es decir, no resulta suficiente para la comprobación del merecimento de protección que el interés social trascienda a la generalidad, es preciso que su lesión o puesta en peligro posean entidad para provocar daño en los indivíduos integrantes del grupo social.*"

funções de representar, armazenar, processar e transportar a informação em si. Apontou, outrossim, que

> "(...) o principal bem jurídico protegível (deveria ser) a informação e, secundariamente, os dados informáticos em si mesmos ou os sistemas e redes informáticos e de telecomunicações, pois esses dados informáticos não constituem mais que a representação eletrônica, inclusive digital, da primeira, com um valor variável, e os segundos, os mecanismos materiais de funções automáticas de armazenamento, tratamento, transferências e transmissão daquela, cuja afetação ou não, de quaisquer desses, dados ou elementos, podem servir, normalmente, mas não necessariamente, para a configuração de algumas modalidades ou tipos de delitos informáticos."[64]

É natural, portanto, que esse verdadeiro bem jurídico, supra-individual por excelência, receba a proteção estatal, na real medida de sua importância. A chancela do direito penal aqui se mostra evidente, não sendo rara, contudo, a situação em que tal chancela entremostre-se desarrazoada.

De forma diversa, um ato intencional e ilícito, tal como a destruição da base de dados de algum órgão do governo federal, por meio de atuação de cidadãos interessados em ver seus registros de débitos tributários ou criminais "limpos", faria com que o direito à informação fosse cerceado, para toda a sociedade, de tal forma que não seria possível a sua realização, a despeito do desejo insculpido na Constituição Federal.

---

[64] CANTO, Enrique Rovira del. *Delincuencia informática y fraudes informáticos.* Granada: Editorial Comares, 2002, p.72. Original em espanhol: *"(...) principal bien jurídico protegible la información, y secundariamente los datos informáticos en si mismos o los sistemas y redes informáticos y de telecomunicaciones, pues los primeros no constituyen más que la representación eletrónica, incluso digital, de la primera, com um valor variable, y los segundoslos mecanismos materiales de funciones automática de almacenamiento, tratamiento, transferencia y transmisión de aquélla, cuya afectación o no, de cualquiera de ellos, datos o elementos, puedem servir, normalmente, mas no necesariamente, para la configuración de algumas modalidades o tipos de delitos informáticos.*"

2.0- Tutela penal dos interesses difusos

Os bens de natureza difusa são uma realidade. Há uma preocupação crescente nesse campo, em razão da significação desses bens e direitos para a sociedade, pelo que, em razão da necessidade de sua preservação, em razão da efetividade que se espera do Estado para a sua proteção, imperioso se faz analisar da legitimidade de tal proteção se efetivar da tutela penal, da intervenção estatal criminalizadora.

Porém, antes de iniciarmos um raciocínio sobre a tutela penal desses bens, convém destacar o conceito desses direitos difusos.

Segundo o Código de Defesa do Consumidor, direitos difusos são "os transindividuais, de natureza indivisível, de que sejam titulares pessoas indeterminadas e ligadas por circunstâncias de fato".[65]

Assim, os direitos difusos são transindividuais, pois são interesses que depassam a esfera de atuação dos indivíduos isoladamente considerados, para surpreendê-los em sua dimensão coletiva. Optou o legislador, pelo critério da indeterminação dos titulares e da inexistência entre eles de relação jurídica-base, no aspecto subjetivo.

Os direitos difusos, ainda, têm natureza indivisível, ou seja, o bem jurídico é indivisível no sentido de que basta uma única ofensa para que todos os consumidores sejam atingidos.

Finalmente, fechando o conceito, tais direitos têm como titulares pessoas indeterminadas ligadas por circuntâncias de fato, ou seja, o critério aqui é o da indeterminabilidade dos titulares, estes ligados por uma situação fática comum.

Superada a fase conceitual, cabe agora apreciar se os bens difusos são dignos e se há necessidade de tutela criminal em relação a eles.

---

[65] art. 81, inciso I.

A intervenção penal para a proteção de bens fundamentais, revelantes, se faz necessária. E o que se pode fazer para dar validade, legitimidade ao Direito Penal, é colocar sob sua tutela as condutas de mais elevada danosidade social, as condutas que violam os valores fundamentais, mais importantes para o homem e a sociedade, inclusive, valendo-se do seu caráter fragmentário, destinar a tutela penal para a proteção das violações mais graves contra determinados bens jurídicos, isso, logicamente, se outras formas de controle não forem suficientes para essa tutela.

Portanto, num primeiro momento é necessário enfatizar que não se deve abdicar, pura e simples, das potencialidades do Direito Penal, eis que ele é instrumento estatal mais efetivo na reprovação de atos gravemente lesivos da ordem jurídica, não havendo, por ora, outra forma de reprovação que o substitua de forma suficiente e eficaz.

Ocorre, porém, que os Códigos Penais tradicionais históricos, e o nosso assim se insere, têm um posicionamento clássico, trabalham sob a ótica dicotômica dos direitos (públicos e privados), veem a sociedade como a soma de indivíduos formalmente livres e iguais, elegendo como bens jurídicos essenciais a vida, a liberdade e o patrimônio, pelo que as figuras delitivas refletem essa visão, hoje extremamente divorciada da realidade que vivemos.

Os direitos individuais passaram a ser valorados à luz dos interesses sociais, os direitos sociais preponderam sobre os direitos individuais, daí porque alargou-se o espectro de bens jurídicos a serem tutelados, compreendendo, por exemplo, a ordem econômica, o meio ambiente equilibrado e sadio, as relações de consumo e os direitos dos consumidores, todos esses bens jurídicos, a serem protegidos, derivados da inserção social do homem.

Como uma das necessidades da política criminal moderna, a qualificação, como delitivas, de certas condutas que, até agora não são, ou até bem pouco não eram, consideradas como criminosas: contaminação do meio ambiente; desfiguração do ambiente urbano; fraudes fiscais e financeiras, violações à dignidade, liberdade, segurança e higiene do trabalho.

Essas considerações, levam-nos a concluir que o Direito Penal, a par de seu caráter de indispensabilidade, tendo em conta sua função primordial, essencial e legítima de defesa dos bens jurídicos, deve ter seus olhos voltados para a realidade social presente. Deve ter em mira, os anseios e expectativas do homem moderno, inserido num contexto social extremamente complexo, competitivo e desigual, marcado por desequilíbrios, deve mensurar os interesses sociais, coletivos e difusos, que ganham corpo, inclusive devendo preponderar sobre direitos individuais, e tudo isso deve refletir no ordenamento penal básico do País, que, sem dúvida, deve abarcar os bens jurídicos difusos, expressão indiscutível do existir humano com dignidade.

A doutrina penal brasileira também já vem reconhecendo a existência de bens jurídicos difusos e a sua importância para a tutela penal.

Birbaum[66] já reconhecia que a lei penal não apenas deveria possibilitar a livre coexistência dos indivíduos, mas servir também de forma imediata a fins sociais. Classificava, portanto, os bens, e por consequência os crimes, em naturais e sociais, uma vez que, no seu pensamento, os bens, em parte, já são dados ao homem pela natureza e, por outra parte, como resultado de seu desenvolvimento social.

Não se trata de ignorar o interesse humano ou personalista na concepção do bem jurídico cujas garantias individuais estão constitucionalmente garantidas, mas, sim, reconhecer a evolução social e a importância da manutenção do sistema social, em que

[66] Über das Erfordernis einer Rechtsverletzung zum begriff des Verbrechens. *Apud* COSTA ANDRADE, Manuel da Costa. *Consentimento e acordo em Direito Penal*. Coimbra: Coimbra Editora, 1991, p. 51-53.

os indivíduos encontram sua realização e o desenvolvimento de sua personalidade, para a conceituação do bem jurídico.

Por sua vez, Liszt[67] apontava a diversidade de formas dos bens jurídicos, decorrente da complexidade da própria vida e das coisas, processos e instituições que a integram e nela se movimentam. Sustentava a existência de portadores individuais dos bens, ao lado de portadores supra-individuais, entre os quais sobressaía o Estado como portador dos interesses coletivos.

Muñoz Conde e García Arán[68] demonstram a existência de bens jurídicos individuais, que afetam diretamente as pessoas individualmente consideradas, e bens jurídicos coletivos, que afetam o sistema social. Como exemplos de bens jurídicos coletivos, contam a saúde pública, o meio ambiente, a organização política etc.

Zaffaroni[69], embora entenda que não há diferença qualitativa entre bens supra-individuais e bens individuais, reconhece a existência de "bens jurídicos de sujeito múltiplo", de forma que um não pode dispor do bem individualmente sem afetar a disponibilidade de outro.

O Professor Miguel Reale Júnior[70] aponta a existência de novas áreas no Direito Penal, como a defesa do meio ambiente, da justiça social e das divisas financeiras do País, consistindo em bens jurídicos a serem penalmente tutelados.[71]

---

[67] *Apud* ANDRADE, Manoel da Costa. *Consentimento e acordo em Direito Penal*. Coimbra: Coimbra Editora, 1991. p. 66-69.

[68] MUÑOZ CONDE, Francisco; GARCÍA ARÁN, Mercedes. *Derecho Penal*: Parte General. 3.ª ed. Valência: Tirant Lo Blanch, 1998, p. 65.

[69] ZAFFARONI, Eugenio Raúl. *Tratado de Derecho Penal*: *Parte General*. Buenos Aires: Ediar, 1981. vol. 3, p. 242.

[70] *Novos rumos do sistema criminal*. Rio de Janeiro: Forense, 1983. p. 214.

[71] No mesmo sentido, Ivete Senise Ferreira, analisando os crimes ambientais defende que "Na segunda metade do séc. XX, porém, novos problemas vieram solicitar a atenção do ordenamento jurídico pela constatação de uma progressiva degradação, e por vezes destruição, do meio ambiente, aliada à previsão das conseqüências catastróficas que isso acarreta para a vida do homem e dos outros seres da natureza, devendo ser por todos os meios obstada para garantir a sobrevivência da própria humanidade. O Direito Penal, parte integrante desse ordenamento jurídico, não pode assim deixar de oferecer a sua contribuição para essa missão salvadora, justificando-se a sua intervenção não somente pela gravidade do problema e pela sua universalidade, mas também porque o direito ao meio ambiente, na sua moderna concepção, insere-se entre os direitos fundamentais do homem, os quais incumbem

Conforme podemos perceber, a idéia de bens jurídicos penais que não afetem diretamente os indivíduos, mas a coletividade de indivíduos e, portanto, interesses de relevância social, já é conhecida e aceita pela doutrina do Direito Penal, com mudanças de enfoque, conforme o momento histórico e a perspectiva da análise de cada doutrinador.

As modificações que o capitalismo e os modelos econômicos vêm enfrentando, entre eles, o modelo de Estado, diante das relações sociais em que vivemos, vêm despertando a doutrina penal para a proteção de interesses que não são individuais, mas metaindividuais ou pluriindividuais, atingindo amplos setores da população.

Renato de Mello Jorge Silveira em sua obra "*Direito penal supra-individual – interesses difusos*" [72], analisa com profundidade o desenvolvimento do conceito de bem jurídico, no devir histórico, apontando uma inexorável tendência, em uma sociedade pós-industrial caracterizada como sociedade global do risco, de se deslocar do bem jurídico individual para um bem juídico supraindividual penalmente relevante, distinguindo-se, para fins de precisão terminológica, os interesses individuais, coletivos e difusos, metaindividuais ou supraindividuais, por excelência.

Figueiredo Dias demonstra a importância da proteção dos interesses metaindividuais para o presente e, principalmente, para o futuro do Direito Penal, segundo o autor,

> "Uma convicção que só se reforçará recusando – como se deve recusar – uma ilegítima restrição da noção de bens jurídico-penais a interesses puramente individuais e ao seu encabeçamento em pessoas singulares, e aceitando antes a

tradicionalmente ao Direito Penal defender, como *ultima ratio"*. *In*: *A tutela penal do patrimônio cultural*. São Paulo: Editora Revista dos Tribunais, 1995. p. 67-68.

[72] SILVEIRA, Renato de Mello Jorge. *Direito penal supra- individual – interesses difusos*. São Paulo: Editora Revista dos Tribunais, 2003.

> plena legitimidade da existência de bens jurídicos transpessoais, coletivos, comunitários ou sociais. É, em meu juízo, no aprofundamento e esclarecimento do estatuto desta classe de bens jurídicos – cujo reconhecimento, de resto, não afetará a natureza em última instância "antropocêntrica" da tutela penal – que reside, no futuro próximo, a tarefa primária da doutrina que continue a fazer radicar a função exclusiva do direito penal na tutela subsidiária de bens jurídicos".[73]

Reconhecida a existência dos bens jurídicos penais transindividuais ou metaindividuais, resta caracterizar a distinção entre os bens jurídicos penais coletivos e os bens jurídicos penais difusos.

A existência de uma espécie de bem jurídico de natureza coletiva é reconhecida na doutrina desde a formulação do conceito de bem jurídico, a qual vem acompanhando o desenvolvimento da Teoria do Bem Jurídico e a perspectiva social do crime, deixando de lado cada vez mais o exclusivo individualismo na concepção do Direito Penal, para reconhecer a importância do sistema social na caracterização do bem jurídico.

A distinção para o Direito Penal entre os bens jurídicos coletivos e os difusos é de enorme valor para a futura perspectiva do Direito Penal, que sofrerá modificações de forma a acolher uma eficaz proteção contra a criminalidade dos interesses difusos.

Parte da doutrina considera os interesses difusos como sinônimos dos coletivos. Entretanto, na visão de Ada Pellegrini Grinover[74] há distinção entre os interesses difusos e coletivos, sem que dessa distinção resulte antagonismos ou exclusões. Ao contrário, são interesses que, na sua visão, complementam-se para a proteção penal:

---

[73] FIGUEIREDO DIAS, Jorge de. *Questões fundamentais do direito penal revisitadas.* São Paulo: Editora Revista dos Tribunais, 1999. p. 74.

[74] GRINOVER, Ada Pellegrini (Coordenadora). *A tutela dos interesses difusos.* São Paulo: Max Limonad, 1984. p. 69-70.

> "Não obstante, porém, a existência de uma "área de *conflittualità*" característica do âmbito dos interesses difusos, as concepções em torno dos fenômenos interesses coletivos e interesses difusos não são excludentes nem antagônicas. Com efeito, existem sempre no território de qualquer um dos interesses coletivos (preservação da vida, da integridade, da saúde, do ambiente, a tutela do consumidor, etc.) maiores ou menores núcleos de conflitos e divergências".

Os bens jurídicos penais difusos são distintos dos interesses coletivos, no sentido utilizado no Direito Penal. Quando a doutrina penal cita bens jurídicos coletivos, está fazendo referência ao interesse público, ou seja, àqueles bens que decorrem de um consenso coletivo, em que há unanimidade social de proteção e forma de proteção. Os conflitos que podem gerar, portanto, ocorrem entre o indivíduo que pratica o crime e a autoridade do Estado efetuando a punição. Em relação aos bens jurídicos difusos, a conflituosidade de massa está presente em suas manifestações, contrastando interesses entre grupos sociais na sua realização. Dessa forma, o Estado realiza muitas vezes uma intermediação, ou melhor, dispõe uma diretriz para as condutas socialmente consideradas, ao tipificar tais condutas como crime, ou não tipificá-las, deixando outros ramos do Direito realizarem a solução.

Por fim, vale destacar a tríplice classificação dos bens jurídicos penais proposta por Gianpaolo Poggio Smanio:[75]

a) os bens jurídicos penais de natureza individual, referentes aos indivíduos, dos quais estes têm disponibilidade, sem afetar os demais indivíduos. São, portanto, bens jurídicos divisíveis em relação ao titular. Citamos, como exemplo, a vida, a integridade física, a propriedade, a honra etc.;

[75] SMANIO, Gianpaolo Poggio. *Tutela penal dos interesses difusos*. São Paulo: Editora Atlas, 2000.

b) os bens jurídicos penais de natureza coletiva, que se referem à coletividade, de forma que os indivíduos não têm disponibilidade sem afetar os demais titulares do bem jurídico. São, dessa forma, indivisíveis em relação aos titulares. No Direito Penal, os bens de natureza coletiva estão compreendidos dentro do interesse público. Podemos exemplificar com a tutela da incolumidade pública, da paz pública etc.;

c) os bens jurídicos penais de natureza difusa, que também se referem à sociedade como um todo, de forma que os indivíduos não têm disponibilidade sem afetar a coletividade. São, igualmente, indivisíveis em relação aos titulares. Os bens de natureza difusa trazem uma conflituosidade social que contrapõem diversos grupos dentro da sociedade, como na proteção ao meio ambiente, em que os interesses econômicos - industriais e o interesse na preservação ambiental se contrapõem, ou na proteção das relações de consumo, contrapostos os fornecedores e os consumidores, na proteção da saúde pública, no que se refere à produção alimentícia e de remédios, na proteção da economia popular, da infância e juventude, dos idosos etc.

Da analise dos efeitos das transformações sociais no Direito Penal, impossível não reconhecer a importância da proteção dos interesses difusos e coletivos. A lei deve ser vista não só como resultado social, mas também como produtora de modificações. O homem, em seu espírito associativo, e pela utilização das tecnologias, pode, pela primeira vez na história da humanidade, pôr em perigo a própria escala humana, destruir a si próprio e se destruir enquanto espécie. O Direito deve dar uma resposta a essas situações, permitindo modificações em alguns de seus dogmas tradicionais.

O interesse de proteção de direitos difusos e coletivos, e principalmente as alterações surgidas no âmbito dos crimes informáticos que conformam essa nova

realidade do Direito Penal, que excepciona determinadas regras, garantem uma certa efetividade do próprio sistema punitivo.

Marta Rodriguez de Assis Machado afirmou que

> "ao se pretender oferecer tratamento penal às ameaças criadas pelos novos riscos tecnológicos (como é o caso da criminalidade cibernética, à toda evidência), logo se verifica que tais situações transcendem a lesão a um bem individual, ligado a uma vítima bem definida" .[76]

A autora apontou ainda que a proteção a bens universais (vagos, supraindividuais etc), estimados como essenciais ao pleno desenvolvimento da vida na sociedade hodierna, torna-se viável por meio do uso de alguns instrumentos de incriminação típicos das "novas áreas de regulação penal, que partem da normatização extrapenal e a trazem para o campo do ilícito criminal, como é o caso dos tipos de mera conduta aqui abordados e, também, das incriminações de perigo abstrato e de alguns dos tipos omissivos e culposos". [77]

Portanto, tendo em conta que a Constituição brasileira expressamente determina a incriminação de condutas lesivas a direitos fundamentais encontráveis na Carta Constitucional, tendo em vista que os direitos coletivos (dentre eles os direitos difusos) são espécies dos direitos fundamentais, sem dúvida que o legislador constituinte, com tal disposição, indica a dignidade dos bens de natureza difusa.

Todavia, ainda que assim não fosse, ou seja, ainda que o legislador constituinte, de forma expressa, não tivesse determinado a incriminação de condutas lesivas a tais bens de natureza difusa, é indiscutível a dignidade que eles apresentam, pelo que mereciam, seriam dignos de tutela penal.

---

[76] MACHADO, Marta Rodriguez de Assis. *Sociedade do risco e direito penal – uma avaliação de novas tendências político – criminais*. São Paulo: IBCCRIM, 2005, p. 102.

[77] MACHADO, Marta Rodriguez de Assis. *Sociedade do risco e direito penal – uma avaliação de novas tendências político – criminais*. São Paulo: IBCCRIM, 2005, p. 118.

Isto posto, concluímos, enfim, que somente em face do caso concreto, da conduta praticada, poderemos afirmar quais dos bens jurídicos penais foram atingidos. Da mesma forma, em se tratando de criminalidade informática, existem condutas criminosas que irão ofender a mais de um bem jurídico penal, entretanto, isso só pode ser objeto de verificação diante do fato concreto.

3.0- Denominação e conceito de crimes de computador

Inicialmente importante se faz ressaltar que qualquer tentativa de definir e de conceituar o termo "crimes de computador", apresenta desvantagens. Dificilmente, pode-se elaborar uma definição sucinta e precisa sem que se deixem dúvidas quer com relação ao seu objeto, quer com respeito à própria utilização que lhe for atribuída.

A noção de crime informático envolve várias espécies de crimes e a adoção de uma definição formal, genérica, pode ensejar mais dificuldades do que soluções.

As várias possibilidades de conduta criminosa na área da informática *lato sensu*, incluindo todas as tecnologias da informação, do processamento e da transmissão de dados, originaram uma forma de criminalidade que, apesar da diversidade de suas classificações, pode ser identificada pelo seu objeto ou pelos meios de atuação, os quais lhe fornecem um ponto comum, embora com diferentes denominações em diferentes países e por diversos autores.

Aliás, as legislações de diversos países não buscam, também, uma definição específica, e acabam por se abster de definir essa modalidade de ilícito.

Delitos computacionais, crimes de informática, crimes de computador, crimes eletrônicos, delito informático, crimes virtuais, cyberdelitos, cybercrimes etc. Não há um consenso quanto ao *nomen juris* dos delitos que ofendem interesses relativos

ao uso, à propriedade, à segurança ou à funcionalidade de computadores e equipamentos periféricos (*hardwares*), redes de computadores e programas de computador (estes denominados *softwares*). Dentre essas designações, as mais comumente utilizadas para identificar infrações que atinjam redes de computadores ou a própria internet ou que sejam praticados por essas vias têm sido as de "crimes de computador", "crime informático" ou "cybercrimes".

Afastada a existência de definição legal específica, faz-se necessária a apresentação de alguns conceitos, criticando-se essas conceituações, e, para fins metodológicos e didáticos, fazendo-se a opção por um desses conceitos apresentados.

Adotaremos aqui a expressão "crimes de computador", por entendermos que a ferramenta básica para a produção desses crimes é o uso do computador.

Importante atentar-se para o uso da expressão "crime" ou "delito", uma vez que do ponto de vista técnico, referem-se à ação ou omissão, típica e antijurídica e, assim sendo, quando se reconhece a necessidade de tipificação para algumas condutas, consequentemente, o seu uso se torna inadequado.

No início dos estudos sobre essa questão, Aaron M. Kohn intitulou "Crimes do Computador" seu editorial publicado no *The Journal of Criminal Law, Criminology and Policy Science* em 1969, e utilizou a expressão "computer criminals" para designar os seus praticantes.

A Organização para a Cooperação Econômica e Desenvolvimento reconhece como crime informático "qualquer conduta ilegal, não ética, ou não autorizada, que envolva processamento automático de dados ou transmissão de dados".[78] Entretanto, há quem entenda que esta definição tampouco resolve a questão, apresentando vários problemas, sendo que a primeira parte da definição – "qualquer

[78] OECD. *Computer related criminality: analysis of legal policy in OECD Área*, ICCP, 84:22, 1984, *apud*, REIS, Maria Helena Junqueira. *Computer Crimes: a criminalidade na era dos computadores*. Belo Horizonte: Del Rey, 1996. p.25.

conduta ilegal, não ética ou não autorizada" -, é extremamente ampla e inclui condutas que não podem ser consideradas crimes, por mais repreensíveis que sejam, enquanto que a segunda parte – "que envolva processamento automático de dados ou transmissão de dados"-, exclui, por exemplo, o armazenamento de dados.[79]

Realmente, embora a "conduta não ética" esteja inserida nesse conceito, tal é incompatível com a cultura jurídica brasileira, mesmo porque parte-se do pressuposto que toda norma penal incriminadora é eticamente indesejável. Aliás, seria um absurdo admitir que tipos penais não tivessem por fundamento a repulsa moral da sociedade.

Quanto aos denominados crimes cibernéticos, sob uma ótica ampliativa do instituto, pode-se afirmar que "esta nova forma de criminalidade se relaciona diretamente com o uso ou a intermediação de um elemento ou dado informatizado".[80]

Um primeiro conceito genérico, à toda evidência, é o que assevera que crime cibernético seria aquele em que um ambiente computacional ou sistema de computador estivesse envolvido.

O conceito de crime cibernético, ou delito informático, na concepção de alguns doutrinadores, é equívoco, multifário e plural, não havendo consenso, esta quadra, acerca de sua delimitação, contudo, sob uma ótica restritiva, tal delito seria aquele em que os ambientes computacionais representam o meio de execução,

> "pois só nesses se apreciam as peculiaridades e as características dos sistemas informáticos ou do processamento eletrônico de dados que convertem esses fatos delituosos em algo novo, diverso, ao menos do ponto de vista criminológico. Não obstante, inclusive nessa aproximação mais restritiva a uma compreensão global

[79] Nesse sentido é o posicionamento de GAGLIARDI, Pedro Luiz Ricardo. *Crimes cometidos com uso de computador*. Tese de Doutorado, USP, p.41.

[80] ABOSO, Gustavo Eduardo, ZAPATA, Maria Florência. *Cibercriminalidad y derecho penal*. Buenos Aires: Julio César Faria Editor, 2006, p.15. Original em espanhol: "*esta nueva forma de criminalidad se relaciona directamente, con el uso o la intermediación de un elemento o dato informatizado*".

> desse gênero de delinquência, deixa-se notar a mencionada heterogeneidade e a considerável amplitude".[81]

Eduardo Augusto de Souza Rossini noticiou a conceituação ainda incipiente do instituto e disse que crime cibernético seria

> "a conduta típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, praticada por pessoa física ou jurídica, com o uso da informática, em ambiente de rede ou fora dele, e que ofenda, direta ou indiretamente, a segurança informática, que tem por elementos a integridade, a disponibilidade e a confidencialidade".[82]

O ilustre jurista Antônio Scarance Fernandes[83], apesar de considerar a expressão "delito informático" como aconselhável, prefere adotar "crimes praticados por computador" ou "crimes por computador", pois, justifica ele, se apresenta mais ajustada. Observa ainda que a diferença de adequação das expressões se encontra no enfoque a ser dado pelo penalista estudioso do tema, em que a primeira se apresenta mais adequada a situações de verificação dos tipos novos e dos tipos já existentes; a segunda mostra-se mais eficiente ao abranger a descoberta do tema e a sua persecução, englobando todo e qualquer tipo de delito, desde que cometido pelo computador.

Klaus Tiedemann[84] ensina que a expressão "criminalidade por computador" se alude a todos os atos, antijurídicos segundo a lei penal vigente (ou socialmente

---

[81] MATA Y MARTÍN, Ricardo M. *Delincuencia informática y derecho penal*. Madrid, Edisofer Libros Jurídicos, 2001, p. 22. Original em espanhol: "*pués solo en estos se aprecian las peculiaridades y características de los sistemas informáticos o del procesamiento eletrónico de datos que convierte estos hechos en algo novedoso, diverso, ao menos deste el punto de vista criminológico. Pero incluso en esta aproximación más restrictiva a una ocmpresión global de este género de delincuencia se deja notar la mencionada heterogeneidad y considerable amplitud*".

[82] ROSSINI, Augusto Eduardo de Souza. *Do necessário estudo do direito penal ante a informática e a telemática. In*: Revista Brasileira de Ciências Criminais. São Paulo, vol. 49, jul/ago 2004, p.39/47.

[83] SCARANCE FERNANDES, Antônio. *Crimes praticados pelo computador: dificuldade de apuração dos fatos*. São Paulo: Revista de Ciências Criminais, 1999.

[84] TIEDEMANN, Klaus. *Criminalidad mediante computadoras. Poder econômico y delito*. Barcelona: Editorial Ariel S.A., 1985, *apud*, LIMA, Paulo Marco Ferreira. *Crimes de computador e segurança nacional*. Campinas: Millennium Editora, 2006, p.26.

prejudiciais e, por isso, penalizáveis no futuro), realizados com o emprego de um equipamento automático de processamento de dados e aos danos patrimoniais produzidos pelo abuso de dados processados automaticamente, enquanto a denominada "criminalidade informática" engloba todas as formas de comportamento ilegal, que venham a, de qualquer forma, provocar danos sociais, por intermédio de um computador.

Luciana Boiteux, por sua vez, apresentou conceituação dogmática, ao afirmar que os crimes cibernéticos ou crimes informáticos são delitos cometidos contra a integridade, a disponibilidade e a confidencialidade dos sistemas informáticos e de redes de telecomunicação, bem como consistem no uso de redes de serviços para cometer crimes tradicionais por meio da Internet.[85]

Para Ivette Senise Ferreira, reconhece-se como crime informático "toda ação típica, antijurídica e culpável cometida contra ou pela utilização de processamento de dados ou sua transmissão" [86].

Nessa esteira, são as lições de Sérgio Marcos Roque que conceitua essa criminalidade como "a conduta definida em lei como crime em que o computador tiver sido utilizado como instrumento para a sua perpetração ou consistir em seu objeto material". [87]

Para Gustavo Testa Correa esses crimes são "todos aqueles relacionados às informações arquivadas ou em trânsito por computadores, sendo esses dados, acessados

---

[85] BOITEUX, Luciana. *Crimes informáticos: reflexões sobre política criminal inseridas no contexto internacional atual*. *In*: Revista Brasileira de Ciências Criminais, São Paulo: vol. 47, pp.146/187, março/abril 2004.

[86] FERREIRA, Ivette Senise. *A criminalidade informática*. *In*: LUCCA, Newton de, SIMÃO FILHO, Adalberto (Coordenadores) e outros. *Direito e internet – aspectos jurídicos relevantes*. 2ª edição, São Paulo: Quartier Latin, 2005, p.208.

[87] ROQUE, Sérgio Marcos. *Crimes de informática e investigação policial. Justiça penal.* São Paulo: Editora Revista dos Tribunais, 2000, p. 32

ilicitamente, usados para ameaçar ou fraudar; para tal prática é indispensável a utilização de um meio eletrônico".[88]

De outra banda, alguns conceitos não se limitam ao computador e usam o sistema informático como referencial, definindo crime informático como "aquele praticado contra o sistema informático ou através deste, compreendendo os crimes praticados contra o computador e seus acessórios e os perpetrados através do computador".[89] Nesse último caso reconhece-se os crimes praticados por meio da internet como uma subdivisão dos crimes de informática, pois "o pressuposto para acessar a rede é o computador".[90]

Nesse sentido, Rita de Cássia Lopes da Silva defende como mais adequado o uso da expressão "crime informático", pois "se refere não só ao equipamento eletrônico em si, mas também a toda a tecnologia que possa ser por ele utilizada. Abrange, ainda, condutas que possam estar ligadas à informação e à sua transmissão isolada ou em conjunto".[91] Destaca ainda a autora que "a denominação envolve o sistema informático, de fundamental importância na indefinição da conduta realizada".[92]

O Professor, João Marcello de Araújo Júnior, diz ser "uma conduta lesiva, dolosa, a qual não precisa, necessariamente, corresponder à obtenção de uma vantagem ilícita, porém praticada, sempre, com a utilização de dispositivos habitualmente empregados nas atividades de informática".[93]

---

[88] CORREA, Gustavo Testa. *Aspectos jurídicos da internet*. São Paulo: Saraiva, 2000 p. 43.
[89] CASTRO, Carla Rodrigues Araújo de. *Crimes de informática e seus aspectos processuais*. Rio de Janeiro: Lumen Juris, 2001, p.10.
[90] CASTRO, Carla Rodrigues Araújo de. *Crimes de informática e seus aspectos processuais*. Rio de Janeiro: Lumen Juris, 2001, p.10.
[91] SILVA, Rita de Cássia Lopes da. *Direito penal e sistema informático*. São Paulo: Editora Revista dos Tribunais, 2003, p.57.
[92] SILVA, Rita de Cássia Lopes da. *Direito penal e sistema informático*. São Paulo: Editora Revista dos Tribunais, 2003, p.57/58.
[93] ARAÚJO JÚNIOR, João Marcello de. *Computer-crime*. *In*: Conferência Internacional de Direito Penal, 1988. Anais. Rio de Janeiro: Procuradoria Geral da Defensoria Pública, 1988, p. 461, *apud* GOUVÊA, Sandra. *O direito na era digital: crimes praticados por meio da informática*. Rio de Janeiro: Mauad, 1997, p.57.

Para Luiz Flávio Gomes[94],

> "os crimes informáticos dividem-se em crimes contra o computador e crimes por meio do computador, em que este serve de instrumento para atingimento da *meta optata*. O uso indevido do computador ou de um sistema informático (em si um fato "tipificável") servirá de meio para a consumação do crime-fim. O crime de fraude eletrônica de cartões de crédito serve de exemplo".

Vladimir Aras[95] defende que a utilização das expressões "crimes telemáticos" ou "cybercrimes" são mais apropriadas para identificar infrações que atinjam redes de computadores ou a própria Internet ou que sejam praticados por essas vias. Estes são crimes à distância *stricto sensu*.

Ao nosso ver, a definição mais acertada é a trazida por Paulo Marco Ferreira Lima[96]que, também em busca de uma definição jurídico-penal sobre essa modalidade criminosa, separou, a princípio, aquilo que constitui a estrutura essencial de um delito e diante disso concluiu que

> "crimes de computador são qualquer conduta humana (omissiva ou comissiva) típica, antijurídica e culpável, em que a máquina computadorizada tenha sido utilizada e, de alguma forma, facilitado de sobremodo a execução ou a consumação da figura delituosa, ainda que cause um prejuízo a pessoas sem que necessariamente se beneficie o

[94] GOMES, Luiz Flávio. *Atualidades criminais.* Acesso: em:www.direitocriminal.com.br, 21.05.2008, às 16h25min.

[95] ARAS, Vladimir. *Crimes de informática – uma nova criminalidade*. Acesso em: http://jus2.uol.com.br/doutrina/texto.asp?id=2250, em 21/03/2008, às 15h39min.

[96] LIMA, Paulo Marco Ferreira. *Crimes de computador e segurança nacional*. Campinas: Millennium Editora, 2006, p.31.

> autor ou que, pelo contrário, produza um benefício ilícito a seu autor, embora não prejudique a vítima de forma direta ou indireta".

Independente dos conceitos acima expostos, concluímos que ao tipificar-se o crime de computador, não se deve esquecer que é preciso evitar termos técnicos em demasia, lançando-se mão apenas dos que se fizerem estritamente necessários, já que eles podem tornar-se obsoletos dentro de pouco tempo, em função das variadas e rápidas modificações às quais a tecnologia da informação é submetida.

Tem-se de levar em consideração novos padrões de comportamento, que podem ser sistematizados na medida em que se analisem os interesses jurídicos colocados em risco. Uma sociedade democrática não pode correr o risco de permitir que, com base na analogia *in malem partem*, se determine o que pode e o que não pode ser objeto de sanção penal em sede de criminalidade informática.

Por fim, relevante também se torna analisar o objetivo da conduta criminosa, ou seja, se o agente visa atingir elementos do sistema informático, ou usa elementos desse sistema. Dessa análise, resultam três possíveis tipos de ações: I) aquelas em que o sistema informático é o objeto material da ação. Neste caso, temos o delito de informática propriamente dito, aparecendo o computador como meio e meta, podendo ser objetos de tais condutas o computador, seus periféricos, os dados ou o suporte lógico da máquina e as informações que guardar; II) aquelas que podem ser praticadas tendo o sistema informático como mais um meio de perpetração de ilícitos. Aqui o computador é apenas o meio de execução, para a consumação do crime-fim, sendo mais comuns nesta espécie as práticas ilícitas de natureza patrimonial, as que atentam contra a liberdade individual e contra o direito de autor e; III) aquelas que somente podem ser realizadas por meio dele.

4.0- Classificação

A classificação dos crimes cometidos através ou contra o computador é de grande importância para melhor visualização e compreensão do assunto.

Na análise das ações lesivas a bem jurídico-penal e o sistema informático, tem-se, de forma geral, que apresentam alguns aspectos bastante peculiares. Constata-se a referência a uma nova versão de delitos tradicionais e outros que podem ser considerados novos.

A análise dos dispositivos que integram o sistema informático levando em conta o prejuízo causado, o papel que o equipamento desempenha, ora como objeto, ora como meio de atuação, e o tipo penal em que se enquadra, levou a várias classificações.

Contudo, ao se tratar de criminalidade informática deve -se atentar inicialmente para a tecnologia utilizada pelo agente na prática da conduta criminosa. Na maioria das vezes, os sistema informático não passou de um instrumento para a prática delitiva e, portanto, perfeitamente dispensável na realização da conduta; em outras se percebe que, sem ele, a conduta não poderia ser realizada.

A doutrina nacional tem trazido à discussão, fundamentando a classificação das ações lesivas relativamente ao sistema informático, posições de vários juristas como: Martine Briat[97], Ulrich Sieber[98], Marc Jaeger[99], C.M. Romeo Casabona[100], Hervé Croze e Yves Bismuth[101], dentre outros.

---

[97] Classifica em: a) manipulação de dados e/ou programas a fim de cometer uma infração já prevista pelas incriminações tradicionais; b) falsificação de dados ou programas; c) deterioração de dados e de programas e entrave à sua utilização; d) divulgação, utilização ou reprodução ilícitas de dados e de programas; e) uso não autorizado de sistemas de informática; e) acesso não autorizado de sistema de informática. *La fraude informatique: une approche de Droit Comparé*. *In*: Revue de Droit Pénal et de Criminologie, n. 4, Bruxelas, p. 287, *apud* FERREIRA, Ivette Senise. *A criminalidade informática*. *In*: LUCCA, Newton de, SIMÃO FILHO, Adalberto (Coordenadores) e outros. *Direito e internet – aspectos jurídicos relevantes*. 2ª edição, São Paulo: Quartier Latin, 2005, p.213.

[98] Classificam-se os crimes informáticos segundo o autor em: a) fraude por manipulação de um computador contra um sistema de processamento de dados; b) espionagem informática e furto de *softwar*e; c) sabotagem informática; d) furto de tempo; e) acesso não autorizado a sistemas; f) ofensas tradicionais. *The international handbook on computer crime*. New York: Editado por John Wiley Sons,

Martine Briat[102] declara ter preferido em sua classificação não fazer menção aos computadores nem aos seus elementos técnicos, por entender que estes podem sofrer modificações muito rápidas pelo avanço da tecnologia nesse setor. Diversamente é o posicionamento de Marc Jaeger[103] que, além de preferir o termo "fraude informática" para designar todos os ilícitos penais ou ações repreensíveis ligadas à informática, distingue nelas apenas duas categorias.

De outra banda, destaca-se a classificação dos crimes em puros (próprios), impuros (impróprios) e comuns. Os puros referem-se aos tipos novos surgidos com o uso da informática, em que o sistema informático serve como meio e fim almejado pelo agente; os impuros, são os tipos que não dependem dela, mas servem somente como meio para a prática de um delito, claramente já definido na legislação penal; e os comuns situam-se na esfera das ações, cujo sistema informático é mera ferramenta para a prática de crimes comuns, ou seja, ações já tipificadas na legislação penal brasileira.

1986, *apud* FERREIRA, Ivette Senise. *A criminalidade informática*. *In*: LUCCA, Newton de, SIMÃO FILHO, Adalberto (Coordenadores) e outros. *Direito e internet – aspectos jurídicos relevantes*. 2ª edição, São Paulo: Quartier Latin, 2005, p.213; REIS, Maria Helena Junqueira. *Computer Crimes: a criminalidade na era dos computadores*. Belo Horizonte: Del Rey, 1996, p.29-30; LIMA, Paulo Marco Ferreira. *Crimes de computador e segurança nacional.* Campinas: Millennium Editora, 2006, p.36-38.

[99] Classifica em das categorias: a) fraudes propriamente ditas, estas subdivididas em: a1)fraudes no nível da matéria corporal, ou *hardware*; a2) fraude no nível do *imput*; a3) fraudes no nível do tratamento; e a4) fraudes no nível do *output*; e b) atentados à vida privada. *La fraude informatique*. *In*: Revue de Droit Pénal et de Criminologie, n. 4, Bruxelas, p. 323, *apud* FERREIRA, Ivette Senise. *A criminalidade informática*. *In*: LUCCA, Newton de, SIMÃO FILHO, Adalberto (Coordenadores) e outros. *Direito e internet – aspectos jurídicos relevantes*. 2ª edição, São Paulo: Quartier Latin, 2005, p.214.

[100] Classifica em: a) manipulação de entrada de dados (*imput*); b) manipulações de programas; c) manipulações na saída de dados; d) maipulação a distância, *apud* REIS, Maria Helena Junqueira. *Computer Crimes: a criminalidade na era dos computadores.* Belo Horizonte: Del Rey, 1996, p.31-32.

[101] Classificam em: a) os atos dirigidos contra um sistema de informática, por qualquer motivo; e b) os atos que atentam contra outros valores sociais ou outros bens jurídicos cometidos por meio de um sistema de informática, *apud* FERREIRA, Ivette Senise. *A criminalidade informática*. *In*: LUCCA, Newton de, SIMÃO FILHO, Adalberto (Coordenadores) e outros. *Direito e internet – aspectos jurídicos relevantes*. 2ª edição, São Paulo: Quartier Latin, 2005, p.215.

[102] *La fraude informatique: une approche de Droit Comparé*. *In*: Revue de Droit Pénal et de Criminologie, n. 4, Bruxelas, p. 287, *apud* FERREIRA, Ivette Senise. *A criminalidade informática*. *In*: LUCCA, Newton de, SIMÃO FILHO, Adalberto (Coordenadores) e outros. *Direito e internet – aspectos jurídicos relevantes*. 2ª edição, São Paulo: Quartier Latin, 2005, p.213.

[103] . *La fraude informatique*. *In*: Revue de Droit Pénal et de Criminologie, n. 4, Bruxelas, p. 323, *apud* FERREIRA, Ivette Senise. *A criminalidade informática*. *In*: LUCCA, Newton de, SIMÃO FILHO, Adalberto (Coordenadores) e outros. *Direito e internet – aspectos jurídicos relevantes*. 2ª edição, São Paulo: Quartier Latin, 2005, p.214.

Serão puros ou próprios, no dizer de Damásio E. de Jesus[104], aqueles que sejam praticados por computador e se realizem ou se consumem também em meio eletrônico. Neles, a informática (segurança dos sistemas, titularidade das informações e integridade dos dados, da máquina e periféricos) é o objeto jurídico tutelado. As ações delituosas se manifestam por atentados destrutivos da integridade física do sistema ou pelo acesso não autorizado ao computador e seus dados armazenados eletronicamente. Já os crimes eletrônicos impuros ou impróprios são aqueles em que o agente se vale do computador como meio para produzir resultado naturalístico, que ofenda o mundo físico ou o espaço "real", ameaçando ou lesando outros bens, não-computacionais ou diversos da informática.

Há quem ignore a existência da terceira classificação supra mencionada, por outro lado, os que a defendem, a distinguem da segunda uma vez que esta volta-se para lesionar um bem jurídico protegido pelo Direito Penal, mas que está armazenado em suporte virtual, enquanto na terceira, a ação encontra adequação típica e o meio informático é só um instrumento a mais.[105]

Os crimes informáticos impuros[106] seriam todos aqueles crimes que possam ser considerados tradicionais e que tenham sido realizados, opcionalmente, com a utilização do computador, como meio para a sua prática, ao passo que, nos crimes

---

[104] Palestra proferida pelo professor Damásio Evangelista de Jesus no I Congresso Internacional do Direito na era da Tecnologia da Informação, realizado pelo Instituto Brasileiro de Política e Direito da Informática — IBDI, em novembro de 2000, no auditório do TRF da 5ª Região, em Recipe-PE.

[105] SCARANCE FERNANDES, Antônio. *Crimes praticados pelo computador: dificuldade de apuração dos fatos*. São Paulo: Revista de Ciências Criminais, 1999, p.8.

[106] ROSSINI, Augusto Eduardo de Souza. *In: Brevíssimas considerações sobre delitos informáticos*. Caderno Jurídico da Escola Superior do Ministério Público do Estado de São Paulo, ano 2, vol. 1, nº4, julho de 2002, p.141, cita como exemplo desses crimes: o estelionato, a ameaça e os crimes contra a honra, podendo imaginar-se, inclusive, homicídio por meio da internet (mudança à distância de rotas de aviões, alterações à distância de medicamentos com o desautorizado uso do sistema informático de um hospital).

informáticos puros[107], as ações lesivas têm o sistema informático como objeto material da conduta criminosa.

Há ainda na doutrina, uma classificação baseada na ação do agente, por meio do uso da informática. Primeiro consideram-se as ações dirigidas contra o sistema informático e, segundo, condutas em que se tem o uso dos recursos da informática como um instrumento a mais para a prática de ações que já estejam previstas, sendo utilizado de acordo com a capacidade intelectual do agente.

Defensora dessa corrente, Sandra Gouvêa[108] inclui na primeira classificação condutas como aquelas que visam atingir a informação arquivada nos inúmeros bancos de dados existentes, através de inserção, alteração, supressão ou, ainda, furto de informação e, na segunda categoria as condutas praticadas com o recurso da informática a fim de cometer crimes previstos na Lei, como, por exemplo, homicídio, sedução, tráfico de entorpecentes etc.

Nesse sentido, Ivette Senise Ferreira apresenta duas categorias de crimes informáticos, quais sejam, atos dirigidos contra o sistema de informática, subdivididos em atos contra o computador e atos contra os dados ou programas de computador, e atos cometidos por intermédio do sistema de informática, subdivididos em crimes contra o

---

[107] ROSSINI, Augusto Eduardo de Souza. *In: Brevíssimas considerações sobre delitos informáticos*. Caderno Jurídico da Escola Superior do Ministério Público do Estado de São Paulo, ano 2, vol. 1, nº4, julho de 2002, p.141, cita como exemplo desses crimes: atos de vandalismo contra a integridade física do sistema em razão do acesso desautorizado – as condutas dos *hackers* e *crackers* – ainda não tipificadas no Brasil, além de algumas já previstas, como as hipóteses preconizadas naLei n. 9.609/78 (Lei de Proteção de Software).

[108] A autora cita alguns exemplos dessas condutas, tais como: "Inserção- Uma instituição financeira mantém as informações relativas aos créditos de conta corrente de seus clientes em um sistema de informática. Uma pessoa pode, violando os sistemas de segurança, inserir um valor relativo a um falso depósito em dinheiro; Alteração- Uma pessoa pode alterar dados relativos à contagem de voto de eleição de certo município, a fim de eleger um candidato. A conduta é simples, bastando imputar a um candidato os votos relativos a outro candidato; Supressão- As informações relativas aos antecedentes criminais das pessoas são arquivadas em bancos de dados. Imagine-se a hipótese de alguém apagar as informações relativas a determinada pessoa condenada, fazendo com que deixem de aparecer os registros e; Furto- O furto de informação apresenta uma peculiaridade: o bem não deixa de estar à disposição do legítimo proprietário. Um exemplo é o furto de lista de consumidores de determinada loja por outro concorrente". GOUVÊA, Sandra. *O direito na era digital: crimes praticados por meio da informática*. Rio de Janeiro: Mauad, 1997, p. 67-68.

patrimônio, liberdade individual e propriedade material.[109]Segundo essa classificação, na primeira categoria situam-se as variadas ações que atentam contra o próprio material informático, seja contra os suportes lógicos, seja contra os dados do computador. Na segunda categoria, caberiam todas as espécies de infrações previstas nas leis penais, pois a informatização da sociedade moderna e pós-moderna produzirá cada vez mais a informatização da delinquência.

Essa divisão também é aceita por Vicente Greco Filho[110] que entende que

> "focalizando-se a *Internet*, há dois pontos de vista a considerar: crimes ou ações que merecem incriminação praticados por meio da *Internet* e crimes ou ações que merecem incriminação praticados contra a *Internet*, enquanto bem jurídico autônomo. Quanto ao primeiro, cabe observar que os tipos penais, no que concerne à sua estrutura, podem ser crimes de resultado de conduta livre, crimes de resultado de conduta vinculada, crimes de mera conduta ou formais (sem querer discutir se existe distinção ente estes) e crimes de conduta com fim específico, sem prejuízo da inclusão eventual de elementos normativos. Nos crimes de resultado de conduta livre, à lei importa apenas o evento modificador da natureza, como, por exemplo, o homicídio. O crime, no caso, é provocar o resultado morte, qualquer que tenha sido o meio ou a ação que o causou".

Pedro Luiz Ricardo Gagliardi[111] prefere uma classificação mais análoga, entendendo também existir duas espécies de crimes informáticos, os crimes informáticos comuns e os crimes informáticos específicos. Nos crimes informáticos comuns, a informática é utilizada como meio para a prática de condutas que já são

---

[109] FERREIRA, Ivette Senise. *A criminalidade informática*. *In*: LUCCA, Newton de, SIMÃO FILHO, Adalberto (Coordenadores) e outros. *Direito e internet – aspectos jurídicos relevantes*. 2ª edição, São Paulo: Quartier Latin, 2005, p.215-225. Tal classificação é a preferida pela autora, vez que entende ser essa mais compatível com os problemas concretos que se apresentam.

[110] GRECO FILHO, Vicente. *Algumas observações sobre o direito penal e a Internet*. Boletim IBCCRIM, edição especial, ano 8, n. 95, outubro de 2000.

[111] GAGLIARDI, Pedro Luiz Ricardo. *Crimes cometidos com uso de computador*. Tese de Doutorado, USP, p.42.

consideradas crime pelo direito penal vigente. A conduta ilícita já é objeto de punição. Já no que toca aos crimes infomáticos específicos a situação não é a mesma, uma vez que se praticam condutas contra bens jurídicos que ainda não são objeto de tutela penal. Ainda segundo o autor, no caso dos crimes informáticos comuns, o fato de a informática ser utilizada como meio para a prática do crime não desvirtua o tipo penal, não impede, necessariamente, que ele incida. O instrumento informático não pode ser essencial para que se cometa o crime, que poderia ser praticado por meio de outra ferramenta, como por exemplo os crimes contra a honra. Com os crimes informáticos específicos, a situação é diferente. Como se praticam condutas contra bens jurídicos que ainda não são objeto de tutela, o dieito penal não pode incidir, por atipicidade.

Sob a égide das condutas ilícitas praticadas por intermédio de um sistema informático, restam as mais diversas figuras penais em razão da enorme influência que alcançou a informática na vida diária das pessoas e organizações, fazendo com que surjam novos meios para o cometimento de quase todos os crimes. De outro lado, está a categoria cujas ações delituosas são perpetradas contra os sistemas informáticos, seja contra os dados de computador ou contra a estrutura informatizada.

Como se nota, o sistema informático deve ser reconhecido como um elemento diferenciador na classificação dos delitos. Se utilizado como mero instrumento, pode levar ao reconhecimento da prática de crimes comuns, já a sua utilização como meio indispensável à execução de ilícitos pode levar ao reconhecimento de crimes previstos na legislação penal ou da prática de condutas ilícitas que ferem bens jurídicos, mas que não encontram previsão (puros ou impuros).

5.0- Sujeitos

Em uma sociedade global de risco, os crescentes avanços tecnológicos, como é o caso daqueles oriundos da ciência cibernética, fazem com que, a cada dia, para a realização do que antes era uma simples transação bancária, o cidadão comun enfrente novos gravames que foram admitidos por essa mesma sociedade pós-industrial, pautada, em verdade, pelos denominados riscos permitidos.

Esses novos riscos imprevisíveis engendraram uma inflação de leis penais e uma notável expansão do direito penal, que, de forma, muitas vezes simbólica, foi e é utilizado como verdadeira panacéia para toda sorte de problemas, em vez de se manter como baluarte de um Estado Democrático de Direito, como *ultima ratio*, no combate a fatos típicos e antijurídicos que causem lesões a determinados bens jurídicos penalmente relevantes.

O cidadão, vez por outra, acabou figurando como vítima dessas novas realidades tecnológicas.

Nos dias atuais, o cidadão comum, quase que deixou de ir ao banco, evitando perda de tempo e dissabores como filas e possibilidades concretas de assaltos. Entretanto, o preço dessa comodidade é o risco potencial de utilizar, em sua residência ou em seu local de trabalho, um sistema computacional comprometido, algo que pode levar à obtenção, por terceiros, de dados sensíveis desse usuário e dos próprios valores de sua conta bancária.

De posse desses dados sensíveis, os criminosos poderão realizar o encaminhamento dessas informações por intermédio de e-mails, que, então, poderão fazer uso ilícito de tais dados e senhas, para fins de obtenção de vantagem patrimonial indevida. Tudo sem qualquer violência ou grave ameaça à pessoa.

Naturalmente, o crime organizado já percebeu, há tempos, esse filão, cujos sistemas de segurança da informação são praticamente insuperáveis, haja vista o astronômico valor investido nessa seara.[112]

Ademais, é cada vez mais comum a cooptação, por parte de quadrilhas especializadas, antigamente, em assalto a bancos, de técnicos e de pessoas com profundo conhecimento de ambientes de redes de computadores, de segurança da informação, de programação de computadores e, também, de criação de sistemas operacionais de ambientes computacionais, para fins de cometimento de grandes golpes no ambiente virtual.

Inúmeras são as condutas delituosas na área da informática, e a primeira indagação que se faz ao investigar tais ações é: Quem são seus sujeitos ativos?

Inicialmente importante se faz destacar que não pode ser vista de forma absoluta, a idéia de que os crimes de computador somente podem ser praticados por pessoas com grandes conhecimentos da linguagem informática.

Com a evolução dos meios de comunicação e o fácil acesso aos equipamentos de informática, qualquer pessoa pode ser sujeito ativo de um crime de computador, bastando, para tanto, que tenha noções mínimas de como manuseá-lo.

Em princípio, o que se verifica é que a criminalidade informática não é praticada por leigos. Não é tão simples navegar em páginas alheias sem autorização, tampouco invadir sistemas, bem como adulterar ou destruir dados.

Tais criminosos costumam ter uma formação acima da média, possuem habilidades para o manejo das ferramentas da informática e, em algumas situações, encontram-se em posições estratégicas que lhes permite o acesso a informações privilegiadas. São pessoas familiarizadas com sistemas informáticos, que usam o

[112] A Federação Brasileira de Bancos (FEBRABAN) investiu algo em torno de R$1,2 bilhão em tecnologias de segurança da informação, no ano de 2006.

conhecimento de que dispõem para tomar vantagem da tecnologia existente em seu proveito.

Da análise do perfil desses criminosos com profundo conhecimento técnico, percebe-se que alguns entraram para essa modalidade de crime por ganância, outros foram, de fato, cooptados sob ameaças a eles infligidas ou a seus familiares.

De um modo geral, ainda são os especialistas em informática os mais freqüentes criminosos dessa área.

Entretanto, com o passar do tempo se pode comprovar que os autores dos crimes de computador têm diversos perfis e o que os diferencia entre si é a natureza do delito cometido.

Sempre que se procede uma classificação ou denominação referente a determinado assunto, importa ressaltar as diferenças encontradas dependendo da doutrina adotada. Com os crimes de computador não é diferente. Deste modo, embora alguns autores denominem seu sujeito ativo como criminosos informáticos, a denominação mais conhecida até pelo seu uso corriqueiro é a de *hacker*.

A ausência de uniformidade na conceituação das expressões informáticas permite interpretações variadas.

A palavra *hacker* surgiu no Massachusetts Institute of Technology para designar os estudantes de computação que cruzavam as noites pesquisando dentro do laboratório; referia-se ao especialista em computador.[113]

Hacker, no jargão da informática, pode ser traduzido livremente por "fuçador". É o indivíduo que se dedica a explorar os detalhes de sistemas programáveis. Profundo conhecedor de computadores, o *hacker* em geral domina muito bem o uso de sistemas operacionais como o Linux e o Windows e programa em linguagens como C e

[113] SILVA, Rita de Cássia Lopes da. *Direito penal e sistema informático*. São Paulo: Editora Revista dos Tribunais, 2003, p.78.

Assembly, entre outras. A especialidade dos *hackers*, no entanto, são as redes de computadores, em especial, a internet.

Atualmente, com a popularização dos microcomputadores, o termo *hacker* acabou servindo para designar o intruso virtual que tenta obter acesso a informações confidenciais através de espionagem por meio de quebra de segurança nas redes. Não se deve, porém, usar a palavra nesse sentido, pois os intrusos virtuais são, na verdade, denominados *crackers*.

Hacker, no sentido ético da palavra, refere-se àquele habilidoso programador, ou seja, o sujeito que usa seus conhecimentos buscando solucionar situações criadas pelos *crackers*. São capazes de entrar e de sair de um computador sem que se perceba; mostrando-se verdadeiros especialistas, "invadem sistemas, corrigem falhas de segurança e instalam uma porta única e controlada, com o propósito de garantir exclusividade no acesso".[114]

É o indivíduo hábil em enganar os mecanismos de segurança de sistemas de computação e conseguir acesso não autorizado aos recursos destes, geralmente a partir de uma conexão remota em uma rede de computadores; violador de um sistema de computação.[115]

Cracker, diferentemente do *hacker*, "é o invasor destrutivo que tenta invadir sem que se perceba as portas de entrada dos servidores de internet, que são a melhor forma de disseminar informações"[116]. Além da invasão de sistemas, adulteram programas e dados, furtam informações, valores e praticam atos de destruição

[114] PAESANI, Liliana Minardi. *Direito e internet: liberdade de locomoção, privacidade e responsabilidade civil.* Coleção Temas Jurídicos. São Paulo: Editora Atlas, 2000, p. 37.
[115] FERREIRA, Aurélio Buarque de Holanda. *Novo Dicionário Aurélio – Século XXI*. Editora Nova Fronteira, 1999.
[116] PAESANI, Liliana Minardi. *Direito e internet: liberdade de locomoção, privacidade e responsabilidade civil.* Coleção Temas Jurídicos. São Paulo: Editora Atlas, 2000, p. 37.

deliberada. “É o *hacker* malicioso, ou seja, dotado de ‘mente criminosa’ mais avançada e voltada para o cometimento de crimes, destruindo e causando danos aos usuários” [117].

Cracker é o indivíduo que se utiliza de seus conhecimentos técnicos para "quebrar" todo e qualquer tipo de barreira de segurança. Numa definição mais didática poderíamos dizer que é o *hacker* "do mal". Os *crackers* podem ter como objeto de seus crimes a quebra do sistema de segurança de programas ou o acesso ilícito a informações armazenadas em computadores.

O *hacker* não pode ser confundido com o usuário comum, uma vez que este último opta por aprender o mínimo necessário para usufruir do programa informático, enquanto o primeiro desfruta da exploração de maiores detalhes.

Por outro lado, atualmente existem cerca de trinta mil páginas na internet direcionadas aos *hackers*, nas quais é possível o acesso a todos os programas necessários para que o usuário se torne um *hacker*.

Há quem defenda que a conduta dos *hackers* é inofensiva, vez que há *hackers* que acessam sistemas apenas pelo desafio sem, contudo, causar dano algum. Entretanto, esse “simples” acesso não autorizado pode caracterizar uma violação a um bem juridicamente tutelado, como a correspondência, por exemplo.

Na concepção dos defensores dessa corrente, os *hackers* não causam ou não procuram causar danos ou prejuízos a terceiros ao tentar invadir seus computadores ou sistema de rede de computadores, mas, tão-somente, demonstrar a vulnerabilidade de seus sistemas de proteção, conhecidos como *firewall*. Tal corrente condena, apenas, os *hackers* que desenvolvem vírus com a intenção de sabotar sistemas de redes de computadores. Argumentam, ainda, seus defensores, que seria injusto criminalizar os

[117] OPICE BLUM, Renato M. S. e DAOUN, Alexandre Jean. *Cybercrimes*. *In* LUCCA, Newton de, SIMÃO FILHO, Adalberto (Coordenadores) e outros. *Direito e internet – aspectos jurídicos relevantes*. 2ª edição, São Paulo: Quartier Latin, 2005, p. 122.

hackers, pois, a chancela penal deveria ser utilizada somente para reprimir os atos perpetrados pelos *crackers*.[118]

Diversamente disso, uma segunda corrente se pauta no entendimento de que tal conduta é realmente desviada e, via de conseqüência, deve ser criminalizada, assim como as outras práticas que dela derivam. Tal assertiva é defendida sob o argumento de que não há remédios civis para dissuadir tais práticas, de maneira que seria preciso utilizar a sanção penal para garantir a tutela das garantias constitucionais gerais violadas, tais como, o direito à privacidade, à propriedade, à informação etc.

As motivações que fazem um *hacker* ou um *cracker* atuar podem ser múltiplas e variadas, mas concentram-se especialmente na esfera social, técnica, política e econômica.

Quem pratica crimes informáticos também costuma ser identificado, dentre inúmeras outras denominações, como *phreackers*, *carders e cyberterrorists.*

Os *phreakers* são especialistas em fraudar sistemas de telecomunicação, principalmente linhas telefônicas convencionais e celulares, fazendo uso desses meios gratuitamente ou às custas de terceiros. Facilitam o ataque aos sistemas a partir de acesso externo, tornando impossível sua identificação e prejudicando o rastreamento de ataques informáticos.[119]

Já os *carders* são criminosos que se apropriam do número de cartões de créditos, obtidos através de invasão de listas eletrônicas constantes nos sites de compras

---

[118] São defensores dessa corrente: DUFF; LIZ; GARDINER, Simon. *Computer crime in the global village: strategies for control and regulation – in Defense of the hacker*. *In*: The International Journal of the Sociology of law, 1996, v. 24; THOMAS, Douglas. *Criminality in the electronic frontier*. *In*: THOMAS, Douglas & LOADER, Brian D. (eds.). *Cybercrime – Law enforcement, security and surveillance in the information age*. Nova Iorque: Routledge, 2000; *apud* FRAGA, Antônio Celso Galdino. *Crimes de informática: a ameaça na era da informação digital. In*: SCHOUERI, Luís Eduardo (Organizador). *Internet: o direito na era virtual*. Rio de Janeiro: Forense, 2001, p.369.

[119] LIMA, Paulo Marco Ferreira. *Crimes de computador e segurança nacional*. Campinas: Millennium Editora, 2006, p. 76.

efetivadas pela internet, ou de outros meios ilícitos para realizar toda a espécie de compras.[120]

Por fim, os *cyberterrorists* são aqueles que desenvolvem vírus, como o famoso Cavalo de Tróia (*Trojan horses*) ou as Bombas Lógicas (*Logic bombs*), criados com o intuito de sabotar as redes de computadores e provocar a queda dos sistemas de grandes provedores (*DDoS – Denial of Service*).

No tocante aos crimes previstos nos artigos 313-A[121] e 313-B[122] do Código Penal, o sujeito ativo da conduta é o funcionário público. Segundo Luiz Regis Prado[123], no primeiro tipo há uma restrição ao sujeito ativo, identificado somente como funcionário autorizado, uma vez que em sistemas de banco de dados poucos têm acesso irrestrito, já no segundo tipo admite-se a prática por qualquer funcionário público que se utilize do computador para o exercício funcional.

Independente da denominação, a verdade é que todos esses criminosos possuem grandes conhecimentos em sistemas operacionais e em linguagem informática, pesquisando falhas e invadindo-os, causando expressivos prejuízos a vários usuários, instituições e à coletividade.

Diversamente dos sujeitos ativos, os sujeitos passivos das ações aqui mencionadas não guardam, para a sua identificação, nenhum tratamento especial.

Sujeito passivo ou vítima dos crimes de computador, por seu turno, é o ente sobre o qual recai a conduta omissiva ou comissiva realizada pelo sujeito ativo.

---

[120] LIMA, Paulo Marco Ferreira. *Crimes de computador e segurança nacional.* Campinas: Millennium Editora, 2006, p. 77.

[121] "Art. 313 –A. Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou banco de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano: Pena – reclusão, de 2 (dois) a 12 (doze) anos, e multa".

[122] "Art. 313 –B. Modificar ou alterar, o funcionário, sistema de informação ou programa de informática sem autorização ou solicitação de autoridade competente: Pena – detenção, de 3 (três) meses a 2 (dois) anos, e multa".

[123] *Curso de direito penal brasileiro*. Parte especial, vol. 04, São Paulo: Editora Revista dos Tribunais, 2005, p. 376.

Na verdade, a maioria das vítimas desses crimes sequer sabe que está sendo atingida.

Em certas situações, contudo, é fácil constatar que a potencial vítima exerce papel na consecução do delito, a despeito do seu grau de instrução formal, que é normalmente alto, no âmbito dos crimes cibernéticos de cariz patrimonial.

Nesse sentido, Alessandra Orcesi Pedro Greco asseverou que,

> "por meio do estudo da evolução do conceito de vítima, percebemos que hoje ela não mais pode ser entendida como um ser inerte face ao crime; observamos que não só ela interage com o autor do crime, como, em alguns casos, pode até criar o risco para si própria, colocando-se em uma situação que a levará ao resultado danoso."[124]

Isso, é claro, não atenua a conduta do criminoso cibernético, não afasta, em grau algum, a elevada lesividade da conduta dos sujeitos ativos de tais delitos, muitos deles componentes de verdadeiras quadrilhas ou de organizações criminosas.

Nada mais verdadeiro, mormente em uma nova tônica de direito penal supra-individual, onde os bens jurídicos a serem protegidos não estão relacionados com sujeitos passivos facilmente individualizáveis, mas, sim, por número indeterminado de pretensas e potenciais vítimas.

Independente disso, podem ser sujeito passivo dos crimes de computador a vítima ofendida, a pessoa física ou jurídica, o Estado, a coletividade etc., dependendo, para sua identificação, da natureza do delito.

---

[124] GRECO, Alessandra Orcesi Pedro. *A autocolocação da vítima em risco*. São Paulo, Editora Revista do Tribunais, 2004, p. 103.

Hoje em dia, assim como qualquer pessoa pode praticar crimes por meio da informática, qualquer um pode ser vítima.

Possuem, contudo, uma característica comum: a vítima desse tipo de crime muitas vezes prefere permanecer em silêncio a denunciar a conduta criminosa, o que prejudica o conhecimento real das possíveis ações lesivas e dificulta uma regulamentação eficiente das práticas que possam ser consideradas criminosas.

A maioria das empresas atingidas por tais condutas criminosas raramente divulga seus problemas de segurança ao público, em especial, temem que seus clientes percam a confiança em seus serviços e que a imagem da entidade pública ou privada fique desmoralizada.

É por isso, a real necessidade de investimento maciço em educação formal do usuário de ambientes computacionais, como política pública de redução de números de crimes desse jaez.

Tanto as instituições bancárias, quanto o Estado e seus Órgãos competentes, devem investir nesse espectro de verdadeira inclusão digital, pois, entre outros fatores, a prevenção é, certamente, menos onerosa e menos traumática que a repressão, esta, nem sempre eficaz.

Não é, portanto, sempre verdadeiro que há necessidade de endurecimento de penas, de novas criminalizações e penalizações para fatos que são, estatisticamente, numerosos na sociedade atual. A ação preventiva é, sempre, muito mais eficaz.

Com medidas preventivas eficazes[125] afasta-se a figura do sujeito passivo do delito, tão tradicional do direito penal.

[125] Roberto Chacon de Albuquerque, em sua obra *A criminalidade informática*, Tese de Doutorado, USP, 2003, p. 06, defende que "um dos meios mais efetivos para o combate à criminalidade informática é a adoção de medidas preventivas, de medidas de segurança, tanto no setor privado, quanto no setor público, o que é uma tarefa para técnicos em computação, gerentes, revisores e consultores em segurança. Não apenas medidas de seguranças pessoais, com o esclarecimento sobre as possibilidades

No que tange ao Estado, este pode ser identificado como sujeito passivo em figuras como a dos artigos 313-A e 313-B do Código Penal, bem como no crime previsto no artigo 2º, inciso V, da Lei 8.137, de 1990.[126]

Nos projetos de lei existentes sobre o assunto, pode-se, de forma geral, identificar qualquer pessoa como sujeito passivo das condutas, bem como situações em que o sujeito passivo será a pessoa jurídica de direito público interno, autarquias, empresas públicas, sociedades de economia mista, fundações instituídas ou mantidas pelo Poder Público e serviços sociais autônomos, quando então a pena poderá ser agravada em um terço.

6.0- Tipicidade

Decisões sobre política criminal, com relação à utilização do direito penal como um dos meios mais incisivos de controle social pelo Estado, pressupõem, em primeiro lugar, que se analisem os interesses individuais e sociais que são colocados em risco.

Os ataques dos *cyberpiratas* tornaram-se um desafio não só para os técnicos em computação, como também para os profissionais da área jurídica.

O que se vive, hoje, é a realidade de inúmeras ações serem praticadas com o uso do computador e a indagação no sentido de se saber se essas ações prejudiciais ao convívio social, encontram ou não correspondência típica em nossa legislação penal. A preocupação primeira está na obediência ao princípio constitucional da legalidade.

---

de prática de conduta criminosa junto aos usuários de sistemas informáticos e à comunidade em geral, mas, também, medidas de segurança técnicas."

[126] A Lei nº8. 137 de 27 de dezembro de 1990 define crimes contra a ordem tributária, econômica e contra as relações de consumo, e dá outras providências. O texto do inciso V do art. 2º da referida lei é o seguinte: "Art. 2º - Constitui crime da mesma natureza: (...) V- utilizar ou divulgar programa de processamento de dados que permita ao sujeito passivo da obrigação tributária possuir informação contábil diversa daquela que é, por lei, fornecida à Fazenda Pública".

Decorre daí a impossibilidade de se punirem ações que não estejam previstas como fato típico, o que equivale dizer que só podem punir crimes que estejam previamente descritos em lei, em obediência ao referido princípio.

A grande discussão aqui é verificar a possibilidade de serem sanados quaisquer eventuais problemas, atinentes à criminalidade nessa àrea, por meio das leis que já existem em nosso ordenamento.

O direito penal oferece apenas um proteção fragmentária, para certos bens jurídicos. Na maioria dos casos, ele protege apenas objetos tangíveis. Alguns bens jurídicos não são protegidos adequadamente contra novas formas de interferência que se tornam possíveis com a tecnologia da informação. Se o bem jurídico já for protegido, a tipificação do crime informático, do novo *modus operandi* para a pática da conduta que já constitui crime, pode tornar-se uma tarefa até menos difícil, mas eventualmente desnecessária. As variadas manifestações da criminalidade informática compreendem novas formas de violações de bens jurídicos que merecem proteção, o que, dependendo do caso, pode ser alcançado sem a adoção de novos tipos penais. Por outro lado, em algumas instâncias, a informática levou a situações em que novas espécies de bens jurídicos estão emergindo, exigindo proteção específica.

Os bens jurídicos a serem protegidos não são realmente novos num sentido qualitativo, mas derivam de um conjunto tradicional de valores.

Os cidadãos têm interesse na segurança jurídica. Eles têm o direito de saber que condutas são objeto de sanção penal, e quais não o são. Há um crescente interesse social na tipificação dos crimes informáticos, o que, indiretamente, pode auxiliar o desenvolvimento da própria tecnologia da informação.

O cerne da questão se prende ao fato de que é princípio penal básico que *nullun crimen, nulla poena sine lege*, ou seja, não há crime sem lei anterior que assim o

defina.Tal princípio econtra-se esculpido no art. 5, inciso XXXXIX da Constituição Federal de 1988[127] e também se encontra encartado infra-constitucionalmente no art. 1 do Código Penal.[128]

Por esse princípio, qualquer indivíduo só pratica uma conduta tida como crime, se a mesma, assim estiver expressamente tipificada como tal em nosso ordenamento penal vigente. Tem como finalidade, a imposição de limites para a discricionariedade punitiva estatal, sendo um verdadeiro corolário da reserva legal.[129]

Nesse sentido, já corroborava Nélson Hungria para quem o referido princípio "antes de ser um critério jurídico-penal, é um princípio (político-liberal), pois representa um anteparo da liberdade individual em face da expansiva autoridade do Estado."[130]

Diante disso, denota-se que para a sua caracterização, o crime necessita de: a) uma tipificação expressa como crime por lei; b) conduta (comissiva ou omissiva); c) que sendo expressa como tal, esteja válida ou apta a surtir efeitos perante todos (*erga omnes*). Diz-se, assim, que é o tipo penal, ou seja, a conduta considerada como atentatória à norma.

Por seu turno, o eminente jurista pátrio Miguel Reali Júnior, sobre o tema em comento acrescenta que "a tipicidade diferencia e especifica as condutas criminais

---

[127] "Art. 5. Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no Pais a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança, à propriedade, nos termos seguintes: XXXIX- não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal;"

[128] "Art. 1. Não há crime sem lei anterior que o defina. Não há pena sem prévia cominação legal."

[129] Como bem salienta o mestre penalista Cezar Roberto Bitencourt em seu Código Penal Comentado. 4. ed. São Paulo: Editora Saraiva, 2007, p. 02: "o princípio da legalidade ou da reserva legal constitui efetiva limitação ao poder punitivo estatal. Feuerbach, no início do século XIX, consagrou o princípio da reserva legal por meio da fórmula latina nullun crimen, nulla poena sine lege. O princípio da reserva legal é um imperativo que não admite desvios nem exceções e representa uma conquista da consciência jurídica que obedece a exigências de justiça; somente os regimes totalitários o têm negado."

[130] HUNGRIA, Nelson. *Comentários ao código penal*, v. I, t.I, 5 ed., Rio de Janeiro: Forense, 1978, p. 22.

em seu aspecto objetivo. O tipo constitui apenas e tão-somente a descrição objetiva, não encerrando elementos subjetivos, nem possuindo conteúdo valorativo."[131]

Ainda sobre o princípio da legalidade, ensina Francisco de Assis Toledo que

> "(...) nenhum fato pode ser considerado crime e nenhuma pena criminal pode ser aplicada, sem que antes desse mesmo fato tenham sido instituídos por lei, o tipo delitivo e a pena respectiva, constitui uma real limitação ao poder estatal de interferir na esfera das liberdades individuais (...)."[132]

A teoria da tipicidade visa classificar as condutas humanas em normas penais proibitivas, ou, como preferem alguns doutrinadores, em normas negativas, incriminando todos os fatos que possam estar desviados de uma conduta aceita socialmente, tendo com paradigma principal, os critérios de censurabilidade da sociedade, formalizando essas ações na legislação criminal. Para os transgressores dessas normas, impõe-se uma sanção penal.

Como já dito e é também sabido no meio jurídico, pelo princípio da legalidade não se pode reconhecer como crime uma conduta que não encontre plena consonância com a descrição abstrata legal, vedando-se, em nosso sistema, a analogia para incriminar condutas.

O cerne da questão respousa justamente aqui. Em muitos casos devido à ausência de norma que tipifique tais crimes, têm, os Tribunais, se socorrido da analogia para o ajustamento da conduta atípica à norma penal, o que, pelo princípio em estudo, onde se assenta o nosso Direito punitivo, é terminantemente proibido.

Em que pesem as considerações de que a lei material penal deve ser interpretada restritivamente, proibida a extensão analógica, o revés de tal interpretação,

---

[131] REALI JUNIOR, Miguel. *Teoria do delito*. São Paulo: Editora Revista dos Tribunais, 1998, p. 42.
[132] TOLEDO, Francisco de Assis. *Princípios básicos do direito penal*. 4ª edição, São Paulo: Saraiva, 1991, p.21.

para o Direito da Informática, o dinheiro desviado de uma conta corrente via internet é furto como outro qualquer, diferenciando-se apenas quanto a maneira e quanto ao agente que pratica o delito, no caso o *hacker*.

Assim, tipos penais não podem, mediante uma interpretação analógica, abranger situações para as quais eles não foram previstos. Todavia, eles podem ser interpretados de uma maneira extensiva. A interpretação extensiva, por sua vez, não deve servir de ensejo para que um novo tipo penal seja concebido. Deve haver um limite para a interpretação extensiva, que deve ser aplicada apenas quando o desenvolvimento técnico criar equivalentes contemporâneos idênticos sob o ponto de vista funcional, o que nem sempre ocorre em sede de criminalidade informática.

É impossível que o Poder Legislativo formule todas as normas necessárias para regular a vida social; limita-se então a formular normas genéricas, que contêm somente diretrizes, e confia aos órgãos executivos, que são nuito mais numerosos, o encargo de torná-las exequíveis.

Por isso, é de extrema necessidade dar ao estudioso do Direito condições de conhecer peculiaridades da informática que possam auxiliar na aplicação da legislação já existente, bem como criar, se necessário, tipos novos.

Há o entendimento de que o Código Penal de 1940 não se presta a solucionar a criminalidade surgida com o sistema informático. Ainda que se tentasse aplicar o crime de estelionato ao acesso de extrato bancário de terceiros, apropriação indébita, invasão de domicílio, ou crime de furto, a dificuldade de punição aos infratores ainda existiria.

Três são os pontos de destaque: a necessidade de cuidado no tentar adaptar as leis já existente aos delitos que tenham sido praticados por intermédio do computador; a existência de casos, cujo uso do computador poderia ser circunstância a

provocar aumento de pena; e outros casos em que se vislumbrariam situações novas, nascendo a necessidade de se criar tipo novo.[133]

Óbvio que a lei deve acompanhar as inovações criadas e experimentadas pela sociedade. Mas no Brasil, como na maioria dos sistemas jurídicos que têm a lei como fonte principal, o processo legislativo é bem mais lento do que os avanços tecnológicos e as consequencias destes. No entanto, nem por isso os operadores jurídicos devem cruzar os braços, ficando no aguardo de providências legislativas compatíveis com a modernidade das técnicas criminosas. Se é possível o encaixe da conduta anti-social a um dispositivo legal em vigor, não deve o aplicador do Direito quedar-se em omissão.

Afirmar que alguém cometeu um fato definido como crime, sem que tal seja verdade, configura delito de calúnia (Código Penal, art. 138), tanto quanto a difusão é feita oralmente ou pelos caminhos da internet. Atacar, a pedradas, o carro de um desafeto constitui crime de dano (Código Penal, art. 183), assim como pratica o mesmo delito o *hacker* que invade perniciosamente um equipamento de informática alheio, danificando-lhe a base de dados. Diferente não é com o estelionatário que falsifica a assinatura e o valor de um cheque de terceiro para levantar fundos junto a agência bancária, assim como também é estelionatário quem captura, na internet, os dados de um cartão de crédito titularizado por outra pessoa e a partir destes faz compras em lojas virtuais, causando grandes prejuízos à primeira.

Assim, não há que ser dito que o Judiciário nada pode fazer só pelo fato de determinado crime ter sido perpetrado via internet.

Ao ser utilizado como instrumento para a prática de uma conduta criminosa, podem ocorrer duas situações distintas. Primeiro, o sistema informático pode constituir

[133] SILVA, Rita de Cássia Lopes da. *Direito penal e sistema informático*. São Paulo: Editora Revista dos Tribunais, 2003, p.51.

apenas um novo *modus operandi* para a prática do crime. O direito penal vigente pode enquadrar tais condutas, que poderiam ser particadas de maneira comparável sem o sistema. Ele já tem uma resposta para esta espécie de crime informático. Segundo, os recursos técnicos de um sistema podem ser utilizados de uma maneira tal que o crime não poderia ser praticado de uma maneira comparável. Para este tipo de conduta, para a sua punição, requer a adoção de novos tipos penais.

O mesmo pode ser dito quando o sistema informático, bem como os dados por ele armazenados, processados ou transmitidos, constituir o objeto do crime.

Em inúmeros casos, chega-se à conclusão de que a ação lesiva somente poderia ocorrer com a utilização da tecnologia informática, em outros pode servir tão-somente como meio mais fácil e rápido para a obtenção do resultado, sem contudo ser o único.

Nesse sentido, foi a decisão proferida pelo relator, o eminente ministro do Supremo Tribunal Federal, Sepúlveda Pertence, no julgamento do *habeas corpus* 76689/PB:

> "Publicação de cena de sexo infanto-juvenil (E.C.A., art.241), mediante a inserção em rede BBS/Internet de computadores, atribuída a menores: tipicidade: prova pericial necessária à demosntração da autoria: HC deferido em parte. (...) 2. Não se trata no caso, pois, de colmatar lacuna da lei incriminadora por analogia: uma vez que se compreenda na decisão típica da conduta criminada, o meio técnico empregado para realizá-la pode até ser de invenção posterior à edição da lei penal: a invenção da pólvora não reclamou redefinição do homicídio para tornar explícito que nela se compreendia a morte dada a outrem mediante arma de fogo. 3. Se a solução da controvérsia de fato sobre a autoria da inserção incriminada pende de informações técnicas de telemática que ainda pairam acima do conhecimento do homem comum, impõe-se a realização de prova pericial."

A certeza que se tem nesses casos é que a ação necessita de um meio de execução adequado, que é o sistema informático. A indagação que se faz é no sentido de qual o grau de inportância dessa tecnologia para a prática da ação.

Em verdade, os crimes de computador são, na maior parte das vezes, os crimes comuns cometidos com o auxílio de um computador, conectado ou não à internet, podendo os crimes de furto, apropriação indébita, estelionato ou dano, ser cometidos por esse meio com consideráveis prejuízos patrimoniais. Entretanto, há algo além de uma nova ferramenta, de um novo *modus operandi* para o cometimento de crimes. Estamos também diante de novas condutas não tipificadas.

Vislumbra-se que uma série de bens jurídicos penalmente tutelados parece ser objeto de criminalidade informática sem que haja a previsão de uma figura típica específica, são ações efetivadas contra a liberdade individual, o direito à intimidade ou ao sigilo das comunicações etc. Por outro lado, os dados constantes em um documento eletrônico restam mais desprotegidos que os mesmos dados constantes em um pedaço de papel.

São também objeto de lacuna as fraudes cometidas com a manipulação de dados e programas computadorizados, mediante a adulteração em documentos eletrônicos, provocando danos financeiros.

Alguns bens jurídicos, os objetos tangíveis, já são protegidos pelo direito penal contra qualquer forma de violação. O direito penal vigente já tem uma resposta para a destruição física de um sistema informático[134] ou para a subtração de um *compact disc* (cd) sem nenhum dado nele armazenado[135].

[134] Crime de Dano, Código Penal, art. 163.
[135] Crime de Furto, Código Penal, art. 155.

A situação é diferente para o acesso não autorizado ao sistema informático ou para a paralisação do funcionamento de um sistema mediante o apagamento dos seus dados, objetos intangíveis.

Evidencia-se que ações delituosas podem ser praticadas contra o funcionamento de um ou mais computadores, sem que exista uma figura típica para tal conduta, como por exemplo, a dissiminação de vírus de computador, que tem, quase sempre, como objeto único a destruição de programas e dados de uma máquina ou rede, podendo trazer consequências absurdas em razão do uso dos e-mails e do acesso à internet.

É adequado aceitar que o novo meio informático traz novos contornos a diversos crimes, que mereciam uma nova proteção penal. Todavia, difícil é vencer essa barreira, definindo de um lado o que seriam os crimes novos, merecedores de uma nova tipificação, colocando de um outro lado a reforma das figuras penais atualmente existentes, incluindo, nessas, eventuais qualificadoras e agravamentos decorrentes do uso da informática.[136]

Pedro Luiz Ricardo Gagliardi,[137] sugere algumas diretrizes para a tipificação dessas condutas criminosas, quais sejam: Em um primeiro plano, sugere que aos novos tipos penais que venham a ser adotados não se deve emprestar um definição muito rígida, sob pena de qualquer modificação social ou técnica torná-la ultrapassada, devem ser agrupados juntos aos já existentes, com os quais guardem semelhanças. O referido autor alerta ainda que não se trata de criar tipos penais em paralelo com os já existentes, mas de conferir uma orientação distinta ao direito penal, em benefício dos bens intangíveis; Sugere também que a adoção de tipos penais que enquadrassem apenas

[136] LIMA, Paulo Marco Ferreira. *Crimes de computador e segurança nacional.* Campinas: Millennium Editora, 2006, p.30.
[137] GAGLIARDI, Pedro Luiz Ricardo. *Crimes cometidos com uso de computador*. Tese de Doutorado, USP, p.30-32.

crimes praticados por determinadas espécies de pessoas, que tenham conhecimento técnico, pudesse ser uma alternativa, mas a dissiminação do conhecimento informático não aconselha que se adote essa teoria; Outro critério, segundo o autor, para a criminalização relacionar-se-ia à distinção entre crimes cometidos contra sistemas informáticos por pessoas autorizadas e por pessoas não autorizadas, por terceiros, abrangendo ou não infrações a obrigações contratuais, tais como a existente entre empregado e empregador; A adoção de medidas de segurança contra o acesso não autorizado é outro critério objetivo para a tipificação sugerido pelo autor. Segundo ele, este critério restritivo vai ao encontro do princípio da subsidiariedade, servindo de estímulo para que os titulares de sistemas informáticos adotem todas as medidas preventivas necessárias, de acordo com as circunstâncias e a situação pessoal, não se exigindo, porém, o estabelecimento de medidas de segurança com tal ou qual nível de excelência; Para o autor, o elemento subjetivo é o fator importante para a distinção da gravidade do crime informático. Ele indaga se as codutas culposas, a par das dolosas, também deveriam ser objeto de sanção,[138] defendendo que apenas as condutas dolosas devem ser enquadradas pelo direito penal em sede de crime informático. Sugere, ainda, que para alguns casos, deve-se exigir o dolo específico, como o enriquecimento ilícito ou o bloqueio de um sistema informático, dependendo das características e dos interesse jurídicos a serem protegidos. Por fim, o autor conclui dizendo que os tipos penais informáticos devem ser concebidos em termos genéricos, bem como serem suficientemente precisos e descritivos para não criar incertezas com relação aos limites fixados, defendendo ainda a permissão ao usuário da informática, com a ajuda da auto-regulação, com códigos de conduta, adaptem seu comportamento às novas exigências.

[138] Ao fazer tal indagação, o autor se baseia na Convenção sobre a Criminalidade Informática do Conselho da Europa, concluída em Budapeste, aos 23 de novembro de 2001, que entende que os crimes informáticos são praticados com dolo.

Ainda segundo Pedro Luiz Ricardo Gagliardi[139], existe uma relação mínima de tipos penais que devem ser adotados. Esta lista ilustra o consenso internacional alcançado com relação à avaliação do risco específico apresentado por um núcleo duro de condutas ilícitas. Ela diz respeito à adoção dos seguintes tipos penais: estelionato informático, dano informático, atentado contra a segurança de sistema informático e falsificação informática. Isso, segundo o autor, representa um consenso mínimo nas mais diversas legislações. A par dessa relação mínima, há uma relação opcional de condutas cuja a tipificação não constitui um consenso internacional: utilização não autorizada de sistemas informáticos ou programas de computador, quando tal alteração não implicar nenhuma espécie de prejuízo; espionagem informática, com a violação de segredos comerciais ou industriais. A primeira e a segunda hipótese são submetidas a sanção penal em vários países. Opiniões variam de país para país com relação à questão de enquadrar a utilização não autorizada de sistemas informáticos ou de programas de computador, dependendo da avaliação se o furto de uso deve ser punido.

Dessa forma, conclui-se que não é fácil buscar proteção contra criminalidade informática com o direito penal existente, que foi concebido tendo em vista a proteção de objetos tangíveis. O ponto de partida deve ser uma variedade de condutas específicas, que permitam avaliar em que medida interesses jurídicos, com projeção social ou individual, são colocados em risco. O que não se pode permitir é que a ausência de tipificação específica sirva de estímulo para a prática de crimes informáticos.

Através dos mecanismos legais existentes e dos que estão por vir, deve brotar a resistência às condutas criminosas em questão. Todavia, uma legislação adequada também não é o bastante. O aperfeiçoamento dos meios de investigação, o

[139] GAGLIARDI, Pedro Luiz Ricardo. *Crimes cometidos com uso de computador*. Tese de Doutorado, USP, p.32.

progresso técnico dos profissionais ligados à área de persecução penal, a melhor formação e treinamento dos auxiliares da Justiça e a conscientização dos internautas e usuários constituem elementos essenciais para coibir práticas desonestas no mundo virtual.

Porém, por outro lado, há quem defenda que a criação de tipos penais abertos para as condutas praticadas no âmbito da informática seria a solução para esse tipo de problema.

A doutrina, com apoio no entendimento de Hanz Welzel[140], indica a existência de tipos fechados e de tipos abertos na legislação penal. Os primeiros apresentam descrição completa do modelo de conduta proibida, bastando ao intérprete, na adequação do dispositivo legal ao comportamento humano, verificar a simples correspondência entre ambos. Já os abertos, em razão da ausência de descrição ou de descrição incompleta, transferem ao intérprete a tarefa de tipificar cada conduta, valendo-se, para tanto, de elementos não integrantes do tipo. Nele, o mandamento proibitivo inobservado pelo sujeito não surge de forma clara, necessitando ser pesquisado pelo julgador no caso concreto.

São hipóteses de crimes de tipo aberto: *a*) delitos culposos: neles, é preciso estabelecer qual o cuidado objetivo necessário descumprido pelo autor; *b*) crimes omissivos impróprios: dependem do descumprimento do dever jurídico de agir (CP, art. 13, § 2.º) e; *c*) delitos cuja descrição apresenta elementos normativos ("sem justa causa", "indevidamente", "astuciosamente", "decoro", "dignidade", "documento", "funcionário público" etc.).

[140] *Apud*, MÉDICI, Sérgio de Oliveira. *Tipos penais abertos.* Boletim IBCCRIM. São Paulo, n.30, p. 02, jun. 1995.

Nesses casos, a tipicidade do fato depende da adequação legal ou social do comportamento, a ser investigada pelo julgador diante das normas de conduta que se encontram fora da definição da figura penal.

Assim, atentando-se para o fato de que a criminalidade informática evolui na mesma (ou até em maior) velocidade que a própria tecnologia, a ausência de criação de tipos penais abertos, transferindo-se ao julgador a adequação legal ou social da conduta, poderá acarretar na manutenção da impunidade atual fundamentada na carência de previsão legal específica para essa modalidade de crime.

Uma resposta, ainda que parcial, à criminalidade informática, passa pela elaboração de tipos penais de perigo abstrato ou mediante a utilização de normas penais em branco, inclusive, para que possam incluir as novas variantes ilícitas que surjam com as constantes evoluções tecnológicas, valendo-se do princípio da proporcionalidade, evitando-se desrespeitar o princípio da legalidade, afastando-se, desse modo, constantes e contínuas reformas legislativas.

O legislador deve se valer, portanto, de tipos penais de perigo abstrato e normas penais em branco – sob pena de restar o direito penal da atualidade incapaz de proteger os novos bens jurídicos penalmente relevantes.

7.0- Competência

Outra grande dificuldade enfrentada pelo operador jurídico no que tange à criminalidade praticada através da internet, diz respeito à aplicação da lei penal no espaço.

Independente da lei material a ser adotada, problemas de soberania, jurisdição e competência estarão cada dia mais presentes no cotidiano dos juristas e dos operadores do Direito que se defrontarem com questões relativas à internet.

O ponto crucial dessas questões que surgem com a internet é, exatamente, a ruptura de paradigmas dos Estados nacionais com suas fronteiras físicas que, por meio de ondas eletromagnéticas ou da alegoria ou abstração dos pacotes de dados, restam esburacadas ou ignoradas. Ignora-se, solenemente, algo que existe no mundo real e físico, pois, no ciberespaço, as fronteiras físicas não mais funcionam como postos de sinalização, informando aos indivíduos das obrigações assumidas ao se entrar em um lugar novo e legalmente significante.

A problemática não se resume aos crimes praticados por meio da informática, mas também as relações civis e comerciais.

Estudo das leis no espaço precisa ser ivocado, principalmente pela dissiminação das redes de computador, já que uma mesma conduta pode lesar o ordenamento jurídico de mais de um Estado.

No caso dos crimes praticados através da informática, em especial aqueles através da internet, a dificuldade é ainda maior. Por estar espalhada por todo o mundo, a internet constitui um novo desafio.

O fato de a internet proporcionar ao usuário se relacionar com pessoas de diversas nacionalidades, sem necessariamente saber onde estão e tampouco sob qual jurisidição estão subordinadas é a principal consequência da revolução da informação, ou seja, a criação de comunidades cibernéticas, independente das barreiras geográficas.

Surge, então, a necessidade de se buscar soluções quanto à jurisdição sob a qual os crimes praticados serão julgados.

Os crimes cibernéticos são cometidos por meio do ciberespaço e não se detêm ante as fronteiras estatais convencionais. Eles podem ser perpetrados, a princípio, a partir de qualquer lugar e contra qualquer usuário de computadores no mundo. Pelo geral, tem-se reconhecido que uma ação efetivada contra os crimes cibernéticos é necessária em ambos os níveis nacional e internacional.[141]

A autora Érica Lourenço de Lima Ferreira[142] assevera que a compreensão da dinâmica do mundo contemporâneo, em seus diversos aspectos, passou a ser um dos mais desafiadores enigmas, por conta da grande teia de inter-relações entre instituições, organizações e Estados.

Expôs a citada autora que os reflexos oriundos do processo transdiciplinar da globalização apontaram a incapacidade do atual modelo de Estado Nacional e do próprio direito em lidar com as novas situações fáticas e relações sociais surgidas.[143]

O principal reflexo disso seria a ruptura de paradigmas consagrados tal como o conceito de soberania e, por conta da ubiqüidade plena dos delitos cibernéticos, do próprio princípio da territorialidade.

Marco Aurélio Greco assinala que "além das repercussões na idéia de soberania e na eficácia das legislações, não se pode deixar de mencionar os reflexos que serão gerados em relação ao exercício da função jurisdicional".[144]

Celso Valin[145] diz que

---

[141] ABOSO, Gustavo Eduardo, ZAPATA, Maria Florência. *Cibercriminalidad y derecho penal*. Buenos Aires: Julio César Faria Editor, 2006, p.7.

[142] FERREIRA, Érica Lourenço de Lima. *Internet – macrocriminalidade e jurisdição internacional*. Curitiba: Editora Juruá, 2007, p.19.

[143] FERREIRA, Érica Lourenço de Lima. *Internet – macrocriminalidade e jurisdição internacional*. Curitiba: Editora Juruá, 2007, p.19.

[144] GRECO, Marco Aurélio. *Internet e direito.* São Paulo: Dialética, 2000, p. 15.

[145] VALIN, Celso. *A questão da jurisdição e da territorialidade nos crimes praticados pela Internet*. *In* ROVER, Aires José Rover (organizador). *Direito, sociedade e informática: limites e perspectivas da vida digital*. Florianópolis: Fundação Boiteux, 2000, p. 115.

> "o grande problema ao se trabalhar com o conceito de jurisdição e territorialidade na Internet, reside no caráter internacional da rede. Na Internet não existem fronteiras e, portanto, algo que nela esteja publicado estará em todo o mundo. Como, então, determinar o juízo competente para analisar um caso referente a um crime ocorrido na rede?".

O crimes praticados através da internet podem atingir mais de uma pessoa, em territórios diversos, com leis distintas. Ou pode, ainda, o produto do crime ser colocado à disposição de qualquer um que queira ter acesso. Afinal, uma vez divulgada a mensagem na rede, o autor não terá mais como controlá-la.

Em tese, um crime cometido na Internet ou por meio dela consuma-se em todos os locais onde a rede seja acessível. Ver, por exemplo, o crime de calúnia. Se o agente atribui a outrem um fato tido como criminoso e lança essa declaração na Internet, a ofensa à honra poderá ser lida e conhecida em qualquer parte do mundo. Qual será então o foro da culpa? O local de onde partiu a ofensa? O local onde está o provedor por meio do qual se levou a calúnia à Internet? O local de residência da vítima ou do réu? Ou o local onde a vítima tomar ciência da calúnia?

De quem será a competência para processar e julgar uma pessoa que atentar, via internet, contra a honra de um brasileiro, por exemplo, com mensagem escrita da Argentina, lida por alguém no Japão através de um servido localizado na China? A mesma indagação se faz, por exemplo, no caso de uma pessoa que faça *upload* de um arquivo contendo fotografias pornográficas de crianças nos Estados Unidos, em um computador localizado na Inglaterra, posteriormente acessado por alguém na Itália ou no Canadá. A qual legislação estará subordinado o autor da publicação dessas fotos?

Por equiparação, Vladimir Aras[146] sugere que poder-se-ia aplicar ao fato a solução dada pela Lei de Imprensa em seu art. 42[147], que considera competente para o processo e julgamento o foro do local onde for impresso o jornal.

Esse dispositivo resolve conflitos de competência entre juízos situados em comarcas diferentes, no mesmo Estado ou em Estados diversos, a partir da consideração do provedor (de acesso ou de conteúdo) como ente equiparado a empresa jornalística. Bem trabalhado, o princípio pode ser adequado aos crimes transnacionais, ainda que cometidos por meio da internet, bastando que se considere como local do fato aquele onde estiver hospedado o *site* com conteúdo ofensivo.[148]

Ives Gandra da Silva Martins e Rogério Vidal Gandra da Silva Martins dão força a esse entendimento, quando, ao cuidar da indenização por dano à vida privada causado por intermédio da internet, sugerem que "toda comunicação eletrônica pública deve ter o mesmo tratamento para efeitos ressarcitórios da comunicação clássica pela imprensa"[149] e que "a desfiguração de imagem por informações colocadas fora da soberania das leis do país ensejaria os meios ressarcitórios clássicos, se alavancada no Brasil."[150]

---

[146] ARAS, Vladimir. *Crimes de informática – uma nova criminalidade*. Acesso em: http://jus2.uol.com.br/doutrina/texto.asp?id=2250, em 050/05/08, às 16h06min.

[147] "Art. 42. Lugar do delito, para a determinação da competência territorial, será aquele e, que for impresso o jornal ou periódico, e o do local do estúdio do permissionário ou concessionário do serviço de radiodifusão, bem como o da administração principal da agência noticiosa".

[148] ARAS, Vladimir. *Crimes de informática – uma nova criminalidade*. Acesso em: http://jus2.uol.com.br/doutrina/texto.asp?id=2250, em 050/05/08, às 16h06min.

[149] GRECO, Marco Aurélio, MARTINS, Ives Gandra da Silva (Coordenadores). *Privacidade na comunicação eletrônica. In: Direito e internet: relações jurídicas na sociedade informatizada.* São Paulo: Editora Revista dos Tribunais, 2001, p.51.

[150] GRECO, Marco Aurélio, MARTINS, Ives Gandra da Silva (Coordenadores). *Privacidade na comunicação eletrônica. In: Direito e internet: relações jurídicas na sociedade informatizada.* São Paulo: Editora Revista dos Tribunais, 2001, p.52.

Como alternativa à fórmula da Lei de Imprensa, assinale -se o art. 72 do Código de Processo Penal que estabelece a competência do foro de domicílio do réu, quando não for conhecido o lugar da infração.[151]

Sandra Gouvêa[152] sugere que a voluntariedade do usuário em se relacionar com outras localidades deve ser levada em conta, e conclui que a jurisdição aplicável será a da nação de onde o usuário "entrar" no ciberespaço, subordinando-se às regras daquele país.

Na verdade, quando um internauta acessa o endereço eletrônico ele não tem conhecimento se o arquivo procurado está em um computador localizado no país de onde acessa ou do outro lado do mundo.

Com o escopo de tentar conciliar as inovações tecnológicas com as normas limitadoras da jurisdição, torna-se necessário analisar os princípios e teorias que norteiam o assunto. O conflito de jurisdição, de acordo com a doutrina tradicional, expõe quatro princípios sobre a aplicação da lei no espaço.

O primeiro deles é o Princípio da Territorialidade e para a aplicação do referido princípio é necessário conceituar-se, inicialmente, o que se define como território e o lugar onde o crime é praticado.

A delimitação do território brasileiro não está contida no ordenamento penal e sim nas normas de Direito Público, vez que não está se tratando de espaço territorial e sim de um conceito jurídico. Assim, território, em sentifo jurídico, seria todo o espaço onde se exerce a soberania do Estado.[153]

---

[151] "Art. 72- - Não sendo conhecido o lugar da infração, a competência regular-se-á pelo domicílio ou residência do réu. § 1º - Se o réu tiver mais de uma residência, a competência firmar-se-á pela prevenção; § 2º - Se o réu não tiver residência certa ou for ignorado o seu paradeiro, será competente o juiz que primeiro tomar conhecimento do fato."

[152] GOUVÊA, Sandra. *O direito na era digital: crimes praticados por meio da informática.* Rio de Janeiro: Mauad, 1997, p.92.

[153] GOUVÊA, Sandra. *O direito na era digital: crimes praticados por meio da informática.* Rio de Janeiro: Mauad, 1997, p. 96.

O Princípio da Territorialidade, em razão da soberania dos Estados, exclui a aplicação da lei penal de um país fora de seu território. Dessa forma, a lei penal é aplicada somente no território onde se exerce a soberania do Estado. Vale ressaltar que tal princípio é aplicado a crimes ocorridos no território, independente da nacionalidade do sujeito ativo ou passivo.

O Código Penal brasileiro consagra o referido princípio, ou seja, a eficácia da lei penal, em seu artigo 5º, determinando que a lei brasileira será aplicada ao crime cometido no território nacional.[154] Mas há casos de extraterritorialidade, em que se aplicam as leis brasileiras aos crimes cometidos no estrangeiro.[155]

O segundo princípio sobre conflitos de jurisdição é o Princípio da Personalidade ou da Nacionalidade, em que considera para aplicação da lei penal a nacionalidade do agente. A lei penal de sua nacionalidade é aplicada ao cidadão em qualquer lugar que se encontre, vinculando o agente ao seu país e sob domínio de suas leis. Subdividido em Princípio da Nacionalidade Ativa e Princípio da Nacionalidade Passiva, este princípio justifica a não concessão pelo Brasil da extradição de nacionais. No caso da nacionalidade ativa, a lei é aplicada ao agente independente da nacionalidade do sujeito passivo. Já no caso da nacionalidade passiva, é preciso para

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

[155] Art. 7º - Ficam sujeitos à lei brasileira, embora cometidos no estrangeiro: I - os crimes: a) contra a vida ou a liberdade do Presidente da República; b) contra o patrimônio ou a fé pública da União, do Distrito Federal, de Estado, de Território, de Município, de empresa pública, sociedade de economia mista, autarquia ou fundação instituída pelo Poder Público; c) contra a administração pública, por quem está a seu serviço; d) de genocídio, quando o agente for brasileiro ou domiciliado no Brasil; II - os crimes: a) que, por tratado ou convenção, o Brasil se obrigou a reprimir; b) praticados por brasileiro; c) praticados em aeronaves ou embarcações brasileiras, mercantes ou de propriedade privada, quando em território estrangeiro e aí não sejam julgados. § 1º - Nos casos do inciso I, o agente é punido segundo a lei brasileira, ainda que absolvido ou condenado no estrangeiro. § 2º - Nos casos do inciso II, a aplicação da lei brasileira depende do concurso das seguintes condições: a) entrar o agente no território nacional; b) ser o fato punível também no país em que foi praticado; c) estar o crime incluído entre aqueles pelos quais a lei brasileira autoriza a extradição; d) não ter sido o agente absolvido no estrangeiro ou não ter aí cumprido a pena; e) não ter sido o agente perdoado no estrangeiro ou, por outro motivo, não estar extinta a punibilidade, segundo a lei mais favorável. § 3º - A lei brasileira aplica-se também ao crime cometido por estrangeiro contra brasileiro fora do Brasil, se, reunidas as condições previstas no parágrafo anterior: a) não foi pedida ou foi negada a extradição; b) houve requisição do Ministro da Justiça.

aplicação da lei penal que o bem atingido seja do seu próprio Estado. Na nossa legislação penal, o princípo da Nacionalidade Ativa está previsto no art. 7º, inciso II, alínea "b".[156]

Outro princípio utlizado para a resolução do conflito é o Princípio da Defesa ou Real, que determina a lei aplicável de acordo com a nacionalidade do bem atingido pela conduta. Por esse princípio, garante-se proteção de bens, mesmo que fora do território, suprimindo lacunas deixadas pelos dois princípios supracitados. Tal princípio rege o art. 7º, inciso I, alíneas "a", "b" e "c" do Código Penal brasileiro. [157]

Por fim, temos o Princípio da Justiça Universal, considerado o mais amplo e avançado, pois se fundamenta na missão dos Estados de colaborarem entre si, unindo esforços na luta contra a criminalidade. A aplicação da lei penal ocorre onde quer que o agente seja detido, independente de sua nacionalidade ou do bem juridicamente protegido. No Código Penal pátrio o referido princípio está previsto no art. 7º, inciso II, alínea "a".[158]

Tais preceitos vinculam-se ao disposto no art. 88 do Código de Processo Penal, que estipula que "No processo por crimes praticados fora do território brasileiro, será competente o juízo da Capital do Estado onde houver por último residido o acusado. Se este nunca tiver residido no Brasil, será competente o juízo da Capital da República".

Vinculam-se também ao art. 109, inciso V, da Constituição Federal, que atribui aos juízes federais a competência para processar e julgar "os crimes previstos em

---

[156] Art. 7º - Ficam sujeitos à lei brasileira, embora cometidos no estrangeiro: II - os crimes: b) praticados por brasileiro.

[157] Art. 7º - Ficam sujeitos à lei brasileira, embora cometidos no estrangeiro: I - os crimes: a) contra a vida ou a liberdade do Presidente da República; b) contra o patrimônio ou a fé pública da União, do Distrito Federal, de Estado, de Território, de Município, de empresa pública, sociedade de economia mista, autarquia ou fundação instituída pelo Poder Público; c) contra a administração pública, por quem está a seu serviço.

[158] Art. 7º - Ficam sujeitos à lei brasileira, embora cometidos no estrangeiro: II - os crimes: : a) que, por tratado ou convenção, o Brasil se obrigou a reprimir.

tratado ou convenção internacional, quando, iniciada a execução no País, o resultado tenha ou devesse ter ocorrido no estrangeiro, ou reciprocamente".

O Código Penal Brasileiro adota a teoria da ubiquidade, prevendo em seu artigo 6º[159], que se considera praticado o crime no lugar em que foi desenvolvida a conduta delinquencial, assim como o lugar onde se produziu ou deveria produzir-se o resultado.[160]

Nessa esteira, fazendo uso novamente dos ensinamentos do Procurador da República, Vladimir Aras, "no tocante aos crimes à distância, deve-se aplicar a teoria da ubiquidade, que foi acolhida no art. 6º do Código Penal. Ação e consumação do crime ocorrem em lugares distintos, uma delas fora do território nacional."[161]

Desta forma, mesmo que processado e responsabilizado em outro Estado, o autor que praticar a infração no Brasil, ainda que ali não se consume, também será julgado perante as leis nacionais.

A etimologia da palavra "ciberespaço" remete à cibernética, que é a ciência do controle à distância.[162]

Posicionando-se sobre o assunto, Lessig[163] pontua que não há liberdade absoluta na Internet e que não se pode falar no afastamento total do Estado. Para ele, o ideal seria haver uma "constituição" para a internet, não no sentido de documento jurídico escrito — como entenderia um publicista —, mas com o significado de "arquitetura" ou "moldura", que estruture, comporte, coordene e harmonize os poderes

---

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

[160] A doutrina expões três teorias sobre o local do crime: 1- Teoria da Ação ou da Atividade: de acordo com ela, é considerado lugar do crime aquele em que o agente desenvolveu a atividade criminosa, onde praticou os atos executórios; 2- Teoria do Resultado*: locus delicti* é o lugar da produção do resultado, ou seja, o local do crime é aquele onde ocorreu o resultado, sendo irrelevante o momento executivo; e 3- Teoria da Ubiquidade ou mista: nos termos dela, lugar do crime é aquele em que se realizou qualquer dos momentos do *iter*, seja da prática dos atos executórios, seja da consumação.

[161] ARAS, Vladimir. *Crimes de informática – uma nova criminalidade*. Acesso em: http://jus2.uol.com.br/doutrina/texto.asp?id=2250, em 050/05/08, às 16h37min.

[162] LESSIG, Lawrence. *Code and other laws of cyberspace*. Nova Iorque: Basic Books, 1999, p.04.

[163] LESSIG, Lawrence. *Code and other laws of cyberspace*. Nova Iorque: Basic Books, 1999, p.05.

jurídicos e sociais, a fim de proteger os valores fundamentais da sociedade e da cibercultura. Essa moldura deve ser um produto consciente e fruto do esforço de cientistas, usuários, empresas e Estado.

O mesmo autor arrola suas perplexidades diante das implicações do ciberespaço sobre o Direito, indagando como será possível enfrentar o problema do conflito real de diferentes ordens jurídicas nacionais, em decorrência de fatos ocorridos no ciberespaço ou na Internet? [164]

Corroborando com esse entendimento, Alexandre Daoun e Renato Opice Blum[165] atestam que

> "A reprimenda à criminalidade praticada com o emprego de meios eletrônicos, notadamente os que avançam na rede mundial de computadores, terá de ser acionada por todos os povos civilizados e essa perspectiva deriva, com certeza, do próprio fenômeno da globalização".

Diante disso, há ou não a necessidade de legislação sobre o ciberespaço? Inúmeros são os motivos para manter o ciberespaço desprovido de qualquer interferência legislativa, mas a melhor solução para o problema, talvez seja aquela que introduz normas protetivas dos novos valores jurídicos, sem fazer disso uma barreira para o avanço tecnológico e a troca de informações.

Para a referida unificação, três métodos poderiam ser utilizados: a adoção de regras espontâneas por parte dos Estados através de imposição ou por parte de uma autoridade supranacional em favor da qual os Estados deleguem parte de seus poderes

---

[164]"Behavior was once governed ordinarily within one jurisdiction, or within two coordinating jurisdictions. Now it will sistematically be governed within multiple, non-coordinating jurisdictions. How can law handle this?" LESSIG, Lawrence. Code and other laws of cyberspace. Nova Iorque: Basic Books, 1999, p.193.

[165]OPICE BLUM, Renato M. S., DAOUN, Alexandre Jean. *Cybercrimes. In* LUCCA, Newton de, SIMÃO FILHO, Adalberto (Coordenadores) e outros. *Direito e internet – aspectos jurídicos relevantes*. 2ª edição, São Paulo: Quartier Latin, 2005, p. 117.

legislativos, ou, ainda, por recepção no ordenamento jurídico de um Estado de legislação de outro Estado.

Na primeira fase há de se fazer a delimitação da matéria a ser unificada e uma avaliação por especialistas sobre a possibilidade de harmonização. Em um segundo momento, a realização de um estudo, através do direito comparado, visando a identificação de soluções já encontradas nos diversos sistemas. E, por fim, na terceira fase, a realização do Tratado de Direito Unificado, aceito por vários Estados através de um acordo internacional, onde se comprometem a introduzir regras uniformes ou se obrigam a editar legislação interna, respeitando certos princípios convencionados.

Na doutrina internacional há quem defenda que a elaboração de leis internacionais regulamentando a internet, como um possível tratado internacional, esbarra na dificuldade de o legislador compreender o funcionamento das redes de computadores e a globalização.[166]

Além desse fator, outro problema ocorrerá no que tange à tipificação de condutas, uma vez que cada país tem sua própria cultura, valores e sistemas diferentes. No Oriente, por exemplo, o que pode ser considerado como pornografia pode não ser em um país do Ocidente. Nos países pertencentes ao sistema da *Common Law*, a fonte direta do direito é a jurisprudência e não a lei, como ocorre nos países pertencentes à família Romano-Germânica, como é o caso do Brasil, e que tem o Princípio da Reserva Legal como fundamental.

A criação de Cortes Criminais Internacionais, segundo sugestão de Henry Perritt[167], também poderá ser uma solução para os conflitos de competência, desde que

[166] PERRIT JR, Henry H. *Jurisdiction in Cyberspace*. Pensilvania: Villanova University School of law, 1995, *apud*, GOUVÊA, Sandra. *O direito na era digital: crimes praticados por meio da informática*. Rio de Janeiro: Mauad, 1997, p. 97.

[167] PERRIT JR, Henry H. *Jurisdiction in Cyberspace*. Pensilvania: Villanova University School of law, 1995, *apud*, GOUVÊA, Sandra. *O direito na era digital: crimes praticados por meio da informática*. Rio de Janeiro: Mauad, 1997, p. 103.

os crimes praticados por meio da informática sejam amplamente debatidos por todos os países. O próprio autor comenta que a experiência tem mostrado a ineficácia das cortes internacionais, pois suas decisões esbarram na resistência da aplicação das sanções pelos Estados.

Enquanto isso não suge, persistem as dúvidas quanto à lei a se aplicar em cada caso concreto: se a *lex fori* ou se a *lex loci delicti comissi* e, no tocante à competência, qual a jurisdição assumirá o processo e julgamento desses crimes.

Especificamente em relação aos crimes praticados por meio da informática, as Nações Unidas, realizaram um estudo que resultou no "Manual de Prevenção e Controle de Crimes Relacionados aos Computadores das Nações Unidas". Neste documento, deu-se enfoque, principalmente, ao aspecto da proteção à privacidade nas redes de computadores, além de sugerir também diretrizes para a aplicação de sanções e uso de determiados termos, tais como: a) sanções penais só devem ser aplicadas em casos de grave ofensa à privacidade; b) o uso de termos vagos deve ser evitado, sem, contudo, usar-se de excessiva precisão, pois isso levaria a legislação ao casuísmo; c) a princípio, apenas as condutas dolosas devem ser tipificadas em mais de um tipo penal.[168]

Várias são as soluções cogitadas para o problema, mas até o momento nenhuma foi consagrada. É preciso, mais do que nunca, refletir acerca do tema para que de forma urgente, sejam criadas soluções justas e capazes de conciliar a soberania dos países com a inevitável evolução tecnológica.

De qualquer modo, como os crimes cometidos pela internet podem atingir bens jurídicos valiosos, como a vida humana ou a segurança do sistemas financeiros ou

---

[168] International Review of criminal Policy – United Nations Manual on the Prevention and control of computer-related crime, *apud*, GOUVÊA, Sandra. O direito na era digital: crimes praticados por meio da informática. Rio de Janeiro: Mauad, 1997, p. 103.

computadores de controle de tráfego aéreo, são necessárias tratativas urgentes para definir, em todo o globo, tais questões competenciais e jurisdicionais, tendo em vista que, pelo menos quanto a um fator, há unanimidade: não pode haver impunidade para autores de crimes que atinjam bens juridicamente protegidos, principalmente quando o resultado decorrente de tais condutas mereça um maior juízo de desvalor, como ocorre com certos tipos de delitos informáticos próprios e impróprios.

8.0- Autoria

Já assinalada a importância da legalidade também no Direito Penal da Informática, é preciso ver que na sua operacionalização quase sempre haverá uma grande dificuldade de determinar, nos crimes de computador, a autoria da conduta ilícita.

A maior dificuldade no combate à criminalidade informática no Brasil talvez não seja só legislativa, mas, também, operacional. No Brasil, essa preocupação teve início em 1996 quando a Polícia Federal começou a treinar nove agentes para a investigação destes crimes[169]. Embora fosse um número pequeno, demonstrava que o governo estava se preparando para combater os criminosos dessa nova modalidade.

A investigação de crimes praticados com os recursos da informática é considerada um dos maiores problemas deste tipo de crime. Proceder a coleta do suporte probatório demanda grandes dificuldades, já que são poucas as vezes em que existirão provas materiais e manifestas relativas ao crime.

Um dos pressupostos para a responsabilização de alguém pel os atos é a demonstração de que ele foi o autor, co-autor, ou então que a ocorrência de certo fato ou

[169] GOUVÊA, Sandra. *O direito na era digital: crimes praticados por meio da informática*. Rio de Janeiro: Mauad, 1997, p. 69.

conduta se deu por culpa *in vigilando* ou *in elegendo*, e todas as nuanças que o tema da responsabilidade jurídica tem ensejado. Todavia, não é objeto do presente estudo desenvolver uma ampla exposição sobre o tema da responsabilidade (objetiva, subjetiva, pelo risco etc.), mas, importante é que, em todas elas, em algum momento, assume relevância o tema da autoria, aspecto que pode ter perfil mais complexo quando se está num ambiente informatizado.

Dependendo do setor em que esta dificuldade surge (civil ou penal) as consequências podem ser distintas.

Apesar de os recursos de informática não serem mais novidade para ninguém, a investigação de condutas criminosas perpetradas por esse meio o são.

É exatamente nesta área que reside o maior problema destes tipos de crimes. Como proceder durante a coleta do suporte probatório, já que dificilmente existirão provas materiais e visíveis relativas ao crime?

Os crimes perpetrados na internet se caracterizam pela ausência física de agente vivo, por isso, ficaram usualmente definidos como crimes virtuais, ou seja, devido a ausência física de seus autores e seus asseclas.

Diferentemente do mundo "real", no ciberespaço o exame da identidade e a autenticação dessa identidade não podem ser feitos visualmente, ou pela verificação de documentos ou de elementos identificadores já em si evidentes, como placas de veículos ou a aparência física, por exemplo.

Patrícia Peck[170] alertou para o fato de que a criminalidade organizada transnacional vem se valendo cada vez mais dos recursos tecnológicos inerentes à sociedade digital relativos à grande rede. Há inúmeras razões para tanto, mas não se pode olvidar que apresentam tais crimes grandes dificuldades para sua comprovação,

[170] PECK, Patrícia, *Direito Digital*. 2ª ed., rev., atual., ampl., São Paulo: Saraiva, 2007, p.258, *in fine*.

pois a verificação de vestígios exige qualificação técnica específica nem sempre disponível em todos os locais em que os crimes se consumam. Às vezes, os registros magnéticos são transitórios e a menos que se realizam provas dentro de um período curto de tempo, podem ser perdidos detalhes de tudo aquilo que aconteceu, restando somente os efeitos danosos do crime.

Nesse sentido, preleciona Mata Y Martín[171] que as dificuldades para a averiguação e a persecução desses fatos delituosos são notáveis: aparecem refletidas nos sistemas um elevadíssimo número de processos simples executados, com a individualização do fato delitivo se esvanece gravemente, os processos sobre os quais se executa o delito não são diretamente visíveis e estão, normalmente, cifrados, e, inclusive, finalmente, os custos econômicos dessa tarefa de investigação podem em muitos casos não resultar rentável para a vítima. No âmbito da delinquência informática apresentam-se, sem dúvida, importantes complicadores para o descobrimento da verdade e para a investigação dos fatos em computadores e mediante esses equipamentos eletrônicos, de forma que se pode em certas ocasiões, não ser raro que muitos dos casos não cheguem sequer a ser detectados. As alterações de dados e programas e os acessos a sistemas informáticos não deixam pistas semelhantes àquelas da delinquência tradicional, de forma que as "evidências eletrônicas" introduzem uma grande novidade e uma grande complexidade.

Em verdade, um dos principais percalços que acompanham o anonimato oferecido pela internet é a capacidade de servir de suporte para organizações criminosas. A internet, do mesmo modo que outras redes informatizadas, forneceria vantagens de acesso remoto, logística e instantaneidade a serviços de grupos terrositas,

[171] MATA Y MARTÍN, Ricardo M. *Delincuencia informática y derecho penal*. Edisofer Libros Jurídicos, Madrid: 2001, p. 26/27.

mafiosos, redes de prostituição e pedofilia, bem como tráfico internacional de drogas e de armas.[172]

Em muitos casos, os criminosos são muito ágeis, pois se valem das discrepâncias legislativas existentes em diversos países, bem assim esses criminosos se locupletam das dificuldades e falhas no âmbito da coleta de provas ou evidências digitais, aproveitam-se da fragilidade na seara da cooperação internacional e na ausência de regulamentação de muitos aspectos da realidade, sob o ponto de vista da rede mundial de computadores. É exatamente por isso que as futuras soluções devem ser internacionais, amplas e especialmente na área normativa e, por óbvio, na legislação penal, tendo-se presente as específicas características da informação.

Quando um indivíduo está plugado na rede, são-lhe necessários apenas dois elementos identificadores: o endereço da máquina que envia as informações à internet e o endereço da máquina que recebe tais dados. Esses endereços são chamados de *IP — Internet Protocol*, sendo representados por números e que, segundo Lessig, não revelam nada sobre o usuário da Internet e muito pouco sobre os dados que estão sendo transmitidos.[173]

No ciberespaço, há razoáveis e fundadas preocupações quanto à autenticidade dos documentos telemáticos e quanto à sua integridade. O incômodo de ter de conviver com tal cenário pode ser afastado mediante a aplicação de técnicas de criptografia[174], em que se utiliza um sistema de chaves públicas e chaves privadas,

---

[172] PECK, Patrícia, *Direito Digital*. 2ª ed., rev., atual., ampl., São Paulo: Saraiva, 2007, p.258, *in fine*.

[173] *"Nor do the IP protocols tell us much about the data being sent. In particular, they do not tell us who sent the data, from where the data were sent, to where (geographically) the data are going, for what purpose the data are going there, or what kind of data they are. None of this is known by the system, or knowable by us simply by looking at the data. (...) Whereas in real space — and here is the important point — anonymity has to be created, in cyberspace anonymity is the given".* LESSIG, Lawrence. *Code and other laws of cyberspace*. Nova Iorque: Basic Books, 1999, p. 32-33

[174] Criptogtrafia é o estudo dos princípios e técnicas pelas quais a informação pode ser transformada da sua forma original para outra ilegível, de forma que possa ser conhecida apenas por seu destinatário, o que a torna difícil de ser lida por alguém não autorizado.

diferentes entre si, que possibilitam um elevado grau de segurança. Assim sendo, só o receptor da mensagem pode ler a informação com facilidade.

Contudo, no que pertine à atribuição da autoria do documento, mensagem ou da conduta ilícita, os problemas processuais persistem, porque, salvo quando o usuário do computador faça uso de uma assinatura digital, dificilmente se poderá determinar quem praticou determinada conduta.

A assinatura digital confere credibilidade ao documento ou mensagem, permitindo que se presuma que o indivíduo "A" foi o autor da conduta investigada. Mas o problema reside exatamente aí. Como a internet não requer auto identificação, a definição de autoria fica no campo da presunção. E, para o Direito Penal, não servem presunções, ainda mais quando se admite a possibilidade de condenação.

O único método realmente seguro de atribuição de autoria em crimes de computador é o que se funda no exame da atuação do responsável penal, quando este tenha se utilizado de elementos corporais para obter acesso a redes ou computadores. Há mecanismos que somente validam acesso mediante a verificação de dados biométricos do indivíduo. Sem isso a entrada no sistema é vedada. As formas mais comuns são a análise do fundo do olho do usuário ou a leitura eletrônica de impressão digital, ou, ainda, a análise da voz do usuário.

A questão da harmonização internacional da legislação (penal e extrapenal) seria fundamentada na ampla e irrestrita mobilidade dos criminosos cibernéticos e a impossibilidade de controle dos fluxos de dados telemáticos, por meio da dantesca teia de ambientes computacionais que estão conectados à Grande Rede (internet).[175]

[175] BOITEUX, Luciana. *Crimes informáticos: reflexões sobre política criminal inseridas no contexto internacional atual*. *In*: Revista Brasileira de Ciências Criminais, São Paulo: vol. 47, pp.146/187, março/abril 2004.

Seguindo-se o que ponderou Luciana Boiteux[176], percebeu-se que a existência de redes mundiais de telecomunicações internacionais que cruzam o território de vários países e a característica básica da internet, meio mais usado de comunicação entre computadores, que ultrapassa fronteiras nacionais, reforçam ainda mais essa conclusão.

Tais questões se inserem no âmbito da segurança digital, preocupação constante dos analistas de sistemas e cientistas da computação, que têm a missão de desenvolver rotinas que permitam conferir autenticidade, integridade, confidencialidade, irretratabilidade e disponibilidade aos dados e informações que transitam em meio telemático. Naturalmente, tais técnicas e preocupações respondem também a necessidades do Direito Penal Informático e do decorrente processo penal.

Como dito, somente os mecanismos de assinatura eletrônica e certificação digital e de análise biométrica podem conferir algum grau de certeza quanto à autoria da mensagem, da informação, ou da transmissão, se considerado o problema no prisma penal.

Denning & Baug Jr[177] informam que os *hackers* dominam várias técnicas para assegurar-lhes o anonimato, a exemplo: a) do uso de *test accounts*, que são contas fornecidas gratuita e temporariamente por alguns provedores e que podem ser obtidas a partir de dados pessoais e informações falsas; b) da utilização de *anonymous remailers*, contas que retransmitem e-mails enviados por meio de provedores de internet que garantem o anonimato; c) clonagem de celulares para acesso à internet, de modo a inviabilizar a identificação do local da chamada e de seu autor, mediante rastreamento

[176] BOITEUX, Luciana. *Crimes informáticos: reflexões sobre política criminal inseridas no contexto internacional atual. In*: Revista Brasileira de Ciências Criminais, São Paulo: vol. 47, pp.146/187, março/abril 2004.

[177] Citados por FRAGA, Antônio Celso Galdino. *Crimes de informática – a ameaça virtual na era da informação digital, in* SCHOUERI, Luís Eduardo (organizador), *Internet: o direito na era virtual*. Rio de Janeiro: Forense, 2001, p. 366.

do sinal; d) utilização de celulares pré-pagos, pois tais aparelhos podem ser adquiridos com dados pessoais falsos e são de difícil rastreamento.

Muito se comenta sobre o substitutivo ao Projeto de Lei n. 89, de 2003, da Câmara dos Deputados, que tem como objeto a regulamentação e repressão aos crimes de computador, que serviria como uma espécie de plataforma para o Brasil aderir à Convenção sobre o Cybercrime, tratado internacional assinado em Budapeste no início deste século.

A característica mais polêmica desse projeto é a previsão de identificação e cadastramento prévio dos usuários como condição para acessarem redes de computadores. Na prática, isso equivale a um formulário digital que deverá ser preenchido e validado sempre que desejarem praticar ações que envolvam interatividade, como por exemplo fóruns de discussão, e-comerce, compartilhamento de arquivos etc. Os provedores de serviço passariam a ser responsáveis pela coleta, validação e armazenamento dos dados de conexões realizadas por seus equipamentos, aptos à identificação do usuário e endereços eletrônicos de origem das conexões, pelo prazo de três anos.

Não nos parece que com o referido cadastramento estar-se-ia autorizando o provedor ou o Estado a interferir na liberdade dos usuários, mas, por outro lado, há que se ponderar os altíssimos custos e a responsabiliade criminal, que poderiam comprometer as atividades dos provedores.

A livre manifestação do pensamento é garantia constitucional fundamental do cidadão, mas só pode ser exercida mediante a identificação. A auto-identificação daquele que expõe sua opinião postando um comentário pessoal, por exemplo, em um site jornalístico é condição para o exercício desta prerrogativa. A vedação ao anonimato se justifica com clareza, na medida em que o princípio que assegura a liberdade de

expressão deve ser conjugado com outras prerrogativas constitucionais, como a da ampla defesa e a que garante o direito de resposta.

O principal objetivo da projetada regra de cadastramento parece ser a segurança da comunicação eletrônica, garantir que, no caso da prática de uma conduta criminosa na internet, a instrução processual possa ser viabilizada mediante requisição judicial ao provedor, para a identificação do usuário suspeito e garantia do direito da vítima.

No tocante à admissão da prova virtual, o Direito Francês inovou ao entrar em vigor a Lei 80.525, de 12-7-1980 que modificou profundamente a matéria sobre prova no direito, abandonando a prioridade tradicional da prova escrita e cedendo espaço ao elemento informático.

Em Direito Comparado, são numerosos os países que admitem os documentos informáticos como meio de prova. Os Estados Unidos, a Noruega, a Alemanha e outros elaboraram indicações para tornar viável a prova informática.[178]

As convenções sobre o tema tendem a multiplicar-se no mundo inteiro, e é necessário chegar-se a um consenso internacional sobre as regras relativas à sua admissão. É preciso abandonar o princípio rígido da prova por escrito e abrir espaço para os avanços da tecnologia.

Ademais, segundo o art. 5º, inciso LVI, da Constituição Federal, somente são inadimissíveis, no processo, as provas obtidas por meios ilícitos, dando, assim, ensejo a um interpretação que entende que, desde que obtida de forma legal, é totalmente possível a utilização da prova advinda do meio virtual.

É evidente que a questão não pode ser resolvida de forma simplista e que grandes diferenças separam o registro magnético de um escrito em sentido jurídico, uma

[178] PAESANI, Liliana Minardi. *Direito de informática – comercialização e desenvolvimento internacional de software*. 2ª edição, São Paulo: Editora Atlas, 1999, p.31.

vez que um estrito não pode ser concebido sem um suporte de papel, enquanto um registro magnético faz dele uma abstração.

No estágio atual, a doutrina mais prudente alega que os documentos informáticos têm valor probatório de simples presunção e, excepcionalmente, podem constituir início de prova escrita. Justificam esta postura considerando que os registros informáticos não têm dado garantias definitivas contra algumas falsificações.

A falta de uma legislação específica sobre esse tema deixa à jurisprudência um papel importante, pois as situações que se criam são confusas, conforme o valor que se dê a essa prova.

No momento, os crimes de computador parecem seguir sendo condutas ilícitas impunes, de maneira manifesta contrariando o ordenamento jurídico-penal. Enquanto não se alcança consenso quanto à forma de tratamento de tais conflitos, a criminalidade informática tem ido avante, sempre com horizontes mais largos e maior destreza do que o Estado, principalmente no tocante à ocultação de condutas eletrônicas ilícitas e ao encobrimento de suas autorias.

CAPÍTULO III - DIREITO COMPARADO

No que concerne à legislação estrangeira dos crimes de computador, merece análise no presente capítulo a situação jurídica dos crimes de computador em alguns países do mundo.

Por questões didáticas, a segmentação do tema é feita em três tópicos, quais sejam, Europa, América Latina e Estados Unidos da América, por se entender que se distinguem situações bem definidas em cada um dos grupos.

1.0- Europa

Inicialmente, considerando o que ocorre no Continente Europeu, temos que a legislação penal se mostra ali, assim como no Brasil, ainda insuficiente para dirimir todas as questões jurídico-penais existentes. Entretanto, na última década, a legislação a respeito dos crimes de computador vem sendo rapidamente ampliada, tanto em cada país, isoladamente, como quanto ao bloco comunitário.[179]

Por essa razão, passamos a traçar considerações a respeito dos principais países da comunidade européia que, mesmo diante de diferenças culturais, buscam a unificação de conceitos e tipificação dos crimes de computador.

1.1- Alemanha

[179] Nesse sentido, em 03 de setembro de 1989, o Conselho Europeu estabeleceu alterações legislativas no que tange à criminalidade informática para a Alemanha, Portugal, França e Grécia. ROSA, Frabrizio. In: *Crimes de informática.* Dissertação de Mestrado em Direito, UNIP – Universidade Paulista, Campinas, 2000, p.59.

Houve na Alemanha, logo após o advento da segunda guerra mundial, uma preocupação do Direito Penal em cuidar da repreensão da criminalidade que se desenvolvia na área econômica.

A partir dessa época, ocorreram inovações legislativas relevantes, quer estabelecendo limites entre os ilícitos penais e administrativos, quer propondo a descriminalização de várias condutas ou criando instrumentos processuais e procedimentos específicos para o chamado direito penal econômico, visando a modernização legislativa para ser essa eficaz no combate da criminalidade econômica, bem como objetivando o aperfeiçoamento daquele direito penal.

Foi nesse momento que começaram a surgir as primeiras manifestações objetivando a responsabilização das fraudes eletrônicas e outras condutas criminosas efetivadas por intermédio dos computadores.[180]

A opção Alemã em relação à luta contra a criminalidade de computador, foi a de introduzir um número relativamente alto de novos preceitos penais. O bem jurídico protegido primordialmente pela atual legislação penal alemã é o patrimônio.

Alguns autores afirmam que, desta forma, não só houve a renúncia em tipificar a mera intrusão não-autorizada em sistemas alheios de computadores, mas também tampouco castigou o uso não-autorizado de equipamentos de processamento de dados, chamado por alguns de furto de tempo.

Assinalou-se que, na hora de introduzir esses novos preceitos penais para a repressão da chamada criminalidade informática, o legislador teve que refletir a respeito de onde radicavam as verdadeiras dificuldades para a aplicação do direito penal tradicional com relação a punir comportamentos danosos praticados pelo meio da

[180] PEDRAZZI, Cesare. *La lotta contro la criminalitá economica nellòrdinamento della repubblica federale tedesca*. *In: La Criminalitá Economica- Analisi del fenomeno sotto il profilo penlistico, anche di diritto comparato, e proposte sul piano normativo ed organizativo. Apud* GAGLIARDI, Pedro Luiz Ricardo. *Crimes cometidos com uso de computador*. Tese de Doutorado, USP, p.80/84.

informática, sopesando principalmente a exposição de novos riscos dos bens jurídicos penalmente tutelados com o advento do processamento eletrônico de dados.

Em 1 de agosto de 1986 adotou-se a Segunda Lei contra a Criminalidade Econômica, de 15 de maio de 1986, em que se contemplam os seguinte delitos: a) Espionagem de dados (202 a); b) Extorsão informática (263 a); c) Falsificação de elementos probatórios (269), aí incluindo a falsificação ideológica, o uso de documentos falsos (270, 271, 273); d) Alteração de dados (303 a), considerando ilícito cancelar, inutilizar ou alterar dados, penalizando ainda a tentativa; e) Sabotagem informática (303 b), punindo a destruição de dados relevantes por qualquer meio (deteriorização, inutilização, eliminação ou alteração de um sistema de dados), punindo também a tentativa; e f) Utilização abusiva de cheques ou cartões de crédito (266 b).

Dessa forma, o Direito Penal Alemão achou por bem tipificar a fraude informática e o delito de sabotagem informática. Quanto a outras ações que atentem contra a vida pessoal e a privacidade, não quis o Código Penal punir a mera intrusão informática, excetuando as ações de manipulação dos computadores para obter informações com o intuito de lucro ilícito.[181]

1.2- Espanha

Quanto ao ordenamento jurídico-penal espanhol temos que, muito embora seja seu Código Penal um dos mais atualizados do continente[182], certas condutas de

[181] De tal modo a violação ao direito à intimidade ou outras ações que não tenham consequências patrimoniais, como por exemplo, acessos ilegítimos realizdos por hackers nos que o móvel é o desafio de acessar ilegitimamente a um sistema e bisbilhotar a informação contida nele, e interceptação de um correio eletrônico etc. não se encontram punidas pelo Direito Alemão.

[182] Em 26 de outubro de 1995 se aprovou a nova Lei Orgânca n. 107/1995 do novo Código Penal Espanhol, o qual entrou em vigor em 24 de maio de 1996. Este novo código tenta solucionar o problema de condutas delitivas que surgem com o incremento das novas tecnologias. Introduz tipos penais novos e modifica alguns dos existentes com o fim de adaptar a norma positiva ao uso delitivo do ordenamento, sistemas lógicos e tecnologias da informação.

hacking, acessos ilegítimos a sistemas informáticos e distribuição de vírus, bombas lógicas etc., permanecem não exatamente coibidas pelo ordenamento penal, acabam sendo tais ações reprimidas em face das alterações das figuras típicas tradicionais, as quais nem sempre alcançam coibir, do mesmo modo, toda a ampla gama de delitos informáticos que se apresentam.

Desse modo, assim dispõe: a) ficam equiparadas, para fins penais, as mensagens de correio eletrônico às cartas de papéis privados (art. 197); b) é responsabilizado penalmente quem, sem a devida autorização, se aproprie, utilize ou modifique, em prejuízo de terceiros, dados pessoais de outros, que se achem registrados em suportes informáticos (art. 197); c) reprime-se o delito de ameaça feito por qualquer meio de comunicação (art. 169); d) castigam-se calúnias e injúrias difundidas por qualquer meio (art. 211); e) inclui-se o uso de chaves falsas como qualificadora do delito de roubo, entendendo que são também chaves os cartões magnéticos ou perfurados, e os comandos e instrumentos de abertura a distância de sistemas (arts. 238-239); f) modifica o art. 248 que tipifica o delito de fraude, incluindo aqueles que, com ânimo de lucro e valendo-se de alguma manipulação informática ou artifício semelhante, consigam a transferência não consentida de qualquer ativo patrimonial em prejuízo de terceiro; g) penaliza a conduta de quem faça uso de qualquer equipamento ou terminal de telecomunicação sem consentimento de seu titular, ocasionando a este um prejuízo de mais de cinquenta mil pesetas; h) protege-se o *software*, ao castigar quem danifica os dados, programas ou documentos eletrônicos alheios contidos em redes, suportes, ou sistemas informáticos (art. 264), assim como a fabricação, posta em circulação e posse de qualquer meio destinado a facilitar a supressão não-autorizada de qualquer dispositivo utilizado para proteger programas de ordenador (art. 270); i) é

punida a fabricação ou posse de programas de ordenador, entre outros, especificamente destinados à falsificação de todo tipo de documento (art. 400).

O Código Penal Espanhol, em seu art. 255, prevê a responsabilização criminal da conduta delituosa consistente em atividades artificiosas que induzem a erro uma máquina computadorizada.[183]

Com isso, conclui-se que a Espanha sofreu uma revolução considerável no seu ordenamento penal, cujo Código Penal anterior (1987) só responsabilizava criminalmente a quem fizesse cópias ilícitas de *softwares*.

1.3- França

A França, com o advento da Lei n. 88/19, de 5 de janeiro de 1988, que trata sobre a fraude informática, dispõe dos seguintes delitos informáticos: a) *Acesso fraudulento a um sistema de elaboração de dados (462-2)*. Por este dispositivo são sancionados tanto o acesso ao sistema como o que se matenha nele, aumentando a pena correspondente em caso desse acesso resultar a supressão ou modificação dos dados contidos no sistema ou resultar a alteração do funcionamento do sistema; b) *Sabotagem informática (462-3)*. Neste dispositivo se sanciona quem delete ou falseie o funcionamento de um sistema de tratamento eletrônico de dados; c) *Destruição de dados (462-4)*. Tal artigo responsabiliza criminalmente quem, intencionalmente e com desrespeito aos direitos de terceiros, introduza dados em um sistema de tratamento eletrônico de dados ou, de qualquer forma, suprima ou modifique os dados que este

[183] Fabrizio Rosa elenca entre as condutas puníveis pelo art. 255 do Código Penal Espanhol: 1) tomar vantagem de mecanismos já instalados, por exemplo, abusar de sistemas de informática ou violar as regras pré-estabelecidas para o uso de linha telefônica; 2) alterar, de forma ilegal, qualquer aparato de medição, interrompendo desta maneira danosa o funcionamento do mecanismo. ROSA, Frabrizio. *Crimes de informática*. Dissertação de Mestrado em Direito, UNIP – Universidade Paulista, Campinas, 2000, p.63

contém ou os seu modos de tratamento ou de transmissão; d) *Falsificação de documentos informatizados (462-5)*. Neste artigo se sanciona quem, de qualquer modo, falsifique documentos informatizados com intenção de causar um prejuízo a outro; e) *Uso de documento informatizados falsos (462-6)*. Neste artigo se sanciona a quem conscientemente faça uso de documentos falsos fazendo referência ao artigo 462-5.

Da análise de tais dispositivos, concluímos que a França previu bem as condutas criminosas praticadas por meio de computadores, lembrando que o direito francês sempre foi um relevante referencial ao nosso direito pátrio e que as mudanças legislativas de lá se deram desde a Lei n. 78-17, de 06 de janeiro de 1978, sendo considerada a primeira lei relativa à informática, aos arquivos de dados e liberdades individuais, dos países do mundo latino.[184]

1.4- Itália

O ordenamento jurídico penal e processual penal italiano sofreu drásticas mudanças entre dezembro de 1992 e dezembro de 1993, com o advento do Decreto Legislativo n. 518/1992, que introduziu a legislação que tutela o direito do autor, criando dispositivos penais sancionando a duplicação ilícita ou a manipulação abusiva de *softwares*.

Dentre as diversas condutas tipificadas, vale destacar os seguintes delitos: a) *Sabotagem informática*: atentado contra a funcionalidade de um sistema informático. Duas são as hipóteses de ocorrência, dependendo da espécie de sistema atacado, caso seja de utilidade pública ou simplesmente de qualquer outra espécie. Na primeira figura, sob o título de atentado a instalações de utilidade pública, o crime se dá com a prática de

[184] GAGLIARDI, Pedro Luiz Ricardo. *Crimes cometidos com uso de computador*. Tese de Doutorado, USP, p. 80-84.

ato dirigido a danificar ou destruir sistemas eletrônicos de utilidade pública. A pena prevista é a de reclusão de um a quatro anos. Porém, se do ato criminoso resultar a destruição ou o dano das instalações do sistema, de seus dados, informações, programas, ou ainda a interrupção, ainda que parcial, de seu funcionamento, a pena é a de reclusão de três a oito anos. A distinção é feita para o Direito Penal Italiano considerando se o sistema é de utilidade pública ou qualquer outro, sendo causa de aumento de pena na primeira hipótese. A segunda espécie de delito de sabotagem pune o dano a sistemas informáticos e telemáticos e consiste no fato de alguém destruir, deteriorar, ou tornar, no todo ou em parte, inservíveis sistemas informáticos ou telemáticos alheios. A pena é de reclusão de três meses a três anos, salvo se o fato constituir crime mais grave (artigo 635 bis, do Código Penal, com a redação dada pelo artigo 9 da Lei n. 547, de 23 de Dezembro de 1993). É prevista, ainda, uma forma qualificada do delito em caso da ação criminosa ser perpetrada com uma ou mais das circunstâncias agravantes[185] constantes do segundo parágrafo do art. 635; b) Crimes contra a inviolabilidade de Domicílio (art. 615): punem a intrusão de um sistema informático e se apresentam em três figuras: 1- Acesso não-autorizado a um sistema de computadores ou de telecomunicações; 2- Posse e disponibilidade de códigos de acesso a sistemas de computadores ou telecomunicações; 3- Difusão de Programas que possam causar danos ou interromper sistemas de computação.

Na primeira hipótese é punida a conduta de simples acesso não-autorizado a sistemas, pouco importando a intenção do agente. Na segunda forma, a conduta punível é a de retenção das senhas e outros métodos de acesso a um sistema informático e a sua difusão visando lucro, dano ou qualquer outro fim. Na última hipótese desses crimes contra a inviolabilidade de domicílio, resta a ação criminosa da divulgação de

[185] Dentre essas circunstâncias agravantes está o uso de violência ou grave ameaça ou o fato de ter agido o criminoso valendo-se de sua atividade profissional.

programas que visem danificar ou interromper o funcionamento de um sistema informático.

C) *Crimes contra a inviolabilidade dos segredos (arts. 616/617 e 621 do Código Penal Italiano)*: punem atentados contra a comunicação informática, ampliando o conceito para incluir qualquer transmissão à distância de sons, imagens e outros dados (art. 623), trazendo a responsabilização penal para quem: 1- violar, subtrair, ou/e suprimir correspondência eletrônica; 2- realizar, ilicitamente, a escuta, interceptação, impedimento ou interrupção ilícita de comunicações informáticas (pouco importando se no ambiente da internet ou de uma rede menor de comunicações informatizadas); 3- instalar equipamento apto a interceptar, impedir, ou interromper comunicações informáticas, pouco importando o fim pretendido; 4- revelar conteúdo de documentos sigilosos obtidos em acesso autorizado a um sistema.[186]

D) *Crimes contra o patrimônio*: punem danos de sistema de informática que tragam prejuízo financeiro, qualificando o fato de ter sido o crime praticado pelo operador do sistema (artigo 635 do Código Penal Italiano); e) *Fraude informática*: é punida a conduta de quem alterar dados em sistema alheio para obter vantagem ilícita (art. 640 do Código Penal Italiano).

Salvatore Ardizzone[187] traça algumas considerações acerca da legislação penal italiana:

[186] Fabrizio Rosa explica essa regra citando o exemplo do "técnico que tem acesso ao HD do usuário e pode tomar conhecimento de todo o seu conteúdo. Para o autor, esse tipo traz uma definição de documento como sendo toda e qualquer peá informática que contenha dados, informações ou programas. *In: Crimes de informática*. Dissertação de Mestrado em Direito, UNIP – Universidade Paulista, Campinas, 2000, p.65.

[187] ARDIZZONE, Salvatore. Professor Efetivo de Direito Penal na Universidade de Palermo. Revista da Faculdade de Direito das Faculdades Metropolitanas Unidas- n. 15 – janeiro de 1996- São Paulo- SP, *apud* LIMA, Paulo Marco Ferreira. *Crimes de computador e segurança nacional*. Campinas: Millennium Editora, 2006, p.90.

> "Parcialmente ligada à questão da qualidade ofensiva dos fatos, por fim, é outra questão, concernente à modalidade de técnica legislativa mais adequada para dotar o ordenamento de preceitos incriminadores relativos às agressões informáticas. Discute-se a possibilidade de ser concebido um *corpus* normativo *ad hoc*, autônomo com relação ao código ou a outras leis especiais de interseção temática, ou a de se preferir outro modelo, dito evolutivo, consistente no trazer modificações ou acréscimos a normas já existentes, de modo a aqui se incluírem os novos crimes informáticos. Não se poderia ter escolhido outro caminho que não o dos acréscimos às categorias de ilícito já considerados no Código Penal Italiano, referentes à orientação interpretativa, amadurecida na Itália, que, por sua, vez não teve coragem de se distanciar da idéia tradicional de que este tipo de ilícito corresponderia a nada mais do que novas modalidades de agressão a bens que já são objeto da tutela penal. Lastreado nas idéias tradicionais da ofensividade e da técnica legislativa de acréscimo, o direito penal italiano pode se gabar de apresentar um número considerável de ilícitos reconhecíveis no setor dos crimes informáticos. Pode-se contar quinze preceitos incriminadores, além dos aplicáveis por extensão à matéria informática, das normas relativas à puniblidade do falso".

O autor ainda destaca que, apesar do sentimento conservador do sistema penal italiano, o país deu dois grandes saltos para o combate da criminalidade por computadores. Por um lado, criou diversas figuras típicas de delinquência informática; enquanto que, de outra banda, cuidou a legislação penal italiana de reservar um capítulo particular que trata das falsidades tendo por objeto o documento informático.

No Código Penal italiano, sob o título *Documentos informáticos*, são agrupadas algumas das falsidades previstas como delitos comuns. Dessa forma, são traçados novos conceitos quanto ao denominado documento informático público ou privado, com a consequente aplicação para os atos criminosos que utilizem documentos eletrônicos públicos e também para as escriturações particulares.[188]

[188] De acordo com o art. 491 bis do Código Penal italiano, com redação dada pelo art. 3, da lei n,547, de 23 de Dezembro de 1993, documento informático é qualquer suporte informático contendo dados ou informações tendo eficácia probatória ou programas especificamente destinados a elaborá-los.

O excesso de penalização italiano não passou despercebido por Salvatore Ardizzone[189], que lamentando as desnecessárias intervenções estatais se manifestou:

> "Estamos diante de uma hiperpenalização, que vai além dos limites de uma escolha racional de política criminal. A exigência de falta de unidade deveria ter sugerido a não previsão da proteção dos bens em qualquer caso e também no que concerne às condutas, nas quais é reconhecível o dano ou uma exposição relevante ao perigo ou, em relação aos quais dever-se-ia ter ponderado sobre a intervenção da lei penal mediante um melhor juízo de oportunidade e conveniência. O cânone da extrema *ratio* deveria ter demandado a procura da possibilidade de uma tutela alternativa à penal. O efeito preventivo atribuído à maciça intervenção da lei penal poderia ser traído por um defeituoso operar dos fatores da orientação cultural e da dissuasão, levando ao ponto de partida a questão da tutela jurídica de interesses concernentes ao uso do sistema computadorizado. Temos, pois, como uma observação realmente consistente na ciência penal, e que como tal deveria ser levada em maior conta pelo legislador, o fato de que tanto um excesso de tutela penal quanto seus defeitos podem prejudicar que se atinja o objetivo teleológico do sistema".

Discordando do nobre penalista, em se tratando de crimes efetivados por meio informático, nos parece imprescindível a presença marcante do Estado.

1.5- Inglaterra

Na Inglaterra, a lei referente ao tema, *Computer Misuse Act* (Lei de Abusos Informáticos) começou a vigorar em 1991.

[189] ARDIZZONE, Salvatore. Professor Efetivo de Direito Penal na Universidade de Palermo. Revista da Faculdade de Direito das Faculdades Metropolitanas Unidas- n. 15 – janeiro de 1996- São Paulo- SP, *apud* LIMA, Paulo Marco Ferreira. *Crimes de computador e segurança nacional*. Campinas: Millennium Editora, 2006, p.91-92.

O objetivo principal do legislador era atingir penalmente a conduta ilícita de alterar dados informáticos, punindo, com até cinco anos de prisão e/ou multa, quem impedir a operação de qualquer computador; impedir ou dificultar o acesso a qualquer programa ou prejudicar a confiança da apuração de dados eletrônicos e a conduta de impedir a execução de qualquer programa de computador ou a confiança em seus dados eletrônicos.

Prevê ainda, um dispositivo que pune a modificação de dados sem autorização, incluindo nessa categoria os vírus de computador. Assim, quem dissemina um vírus na Inglaterra pode ser condenado a penas que vão de um mês a cinco anos de prisão, dependendo dos prejuízos causados.

1.6- Portugal

No ordenamento jurídico-penal português, a tipificação de crimes de computador se deu com o advento da Lei n. 109 de 17 de agosto de 1991, quando foram criadas seis novas figuras penais na área da informática, com a punição das seguintes condutas: a) *Falsidade informática (art. 4º)*: tal dispositivo penaliza a introdução, modificação ou a supressão de dados ou de programas informáticos, com o intuito de falsear a obtenção da dados eletrônicos; b) *Dano a dados ou programas informáticos (art. 5º)*: consiste a conduta típica na destruição de dados eletrônicos ou de programas de computador, objetivando tão só o dano ou a obtenção de alguma vantagem ilícita; c) *Sabotagem informática (art. 6º)*: é punida a conduta de apagar, alterar, introduzir ou suprimir dados ou programas informáticos, com o objetivo de entravar ou perturbar o funcionamento informático ou de comunicação de dados à distância; d) *Acesso ilegítimo (art. 7º)*: responsabiliza criminalmente a intrusão à sistemas informáticos; e)

Interceptação ilegítima (art. 8º): o referido dispositivo penaliza a interceptação ilegítima de comunicações informáticas, em qualquer ambiente computacional, seja na internet, em um sistema ou em qualquer outra espécie de rede computadorizada; f) Reprodução ilegítima de programa protegido (art. 9º): é punida a reprodução, divulgação ou a comunicação ao público, sem autorização, de *software*.

A preocupação da Comunidade Européia na unificação de suas normas e conceitos na área de direito da informática foi bem recebida pelo Direito Penal Português. O movimento de reforma legislativa portuguesa atingiu, inclusive, o seu atual Código Penal, com a tipificação dos seguintes comportamentos: a) Devassa por meio de informática; b) Burla informática e nas telecomunicações. Além desse fator, a Lei n. 67, de 26 de outubro de 1998, também previu a possibilidade de punição das seguintes condutas: a) Não cumprimento de obrigações relativas à proteção de dados; b) acesso indevido; c) Viciação ou destruição de dados pessoais; d) Desobediência qualificada; d) Violação do dever de sigilo.

2.0- América Latina

No tocante aos países da América Latina, há uma preocupação em reformar as legislações nacionais visando a tipificação de novas figuras delitivas. Isto se deu em razão da intensificação das relações comerciais eletrônicas, à globalização da economia, e à vulnerabilidade dos sistemas eletrônicos, facilitando, assim, a prática de condutas criminosas.

Por outro lado, nenhuma das legislações analisadas prevê integralmente figuras típicas da criminalidade informática. Não há previsão expressa quanto à fraude informática, embora todas condenem o acesso ilegítimo a dados alheios informatizados.

Há também ausência de tipificação de condutas penalmente relevantes, como a fraude na introdução, alteração ou supressão de dados; as falsificações informáticas; os danos causados a dados ou programas; a sabotagem informática; o mero acesso ilegítimo; a interceptação, reprodução não-autorizada de um programa informático etc.

Vale lembrar que a escolha dos países abaixo estudados, se deu pelo fato de seus ordenamentos apresentarem maiores mudanças nas últimas décadas.

2.1- Argentina

O ordenamento jurídico Argentino procura conjugar a regulamentação do comércio eletrônico e as condutas ilícitas que possam dele surgir. E, foi em razão de algumas legislações que cuidam de forma precípua de normatizar o comércio eletrônico, que surgiram alterações penais de grande relevância.

As leis comerciais que isoladamente tratam do uso de certa informação eletrônica importaram uma reforma ao texto do Código Penal Argentino.[190]

A título de exemplo, podemos citar a lei do *Habeas Data*, acrescentando o artigo 117, bis, no título *Dos Delitos Contra a Honra*, que pune a inserção de informação falsa em um arquivo de dados pessoais, sendo a pena agravada se do mesmo fato se derivar prejuízo a uma pessoa ou se o autor praticar a conduta através de uso abusivo de sua atividade profissional.

[190] Citamos, a seguir, algumas legislações que cuidam de normatizar o comércio e que, contudo, vieram a afetar a esfera penal: 1) Lei n. 24.766, denominada *Lei do Sigilo de Dados*, que protege criminalmente a informação que contenha a relevância de um segredo comercial; 2) Lei n.23.326, chamada de *Habeas Data*, que tutela a informação de caráter pessoal armazenada em arquivos e dados eletrônicos; e 3) A Lei n. 11.723, denominada Lei de Propriedade Intelectual (com modificação feita pela Lei 25.036) que amplia a tutela legal às obras de computação, preservando a fonte e o objeto.

Ainda no que se refere às alterações sofridas pelo Código Penal Argentino, o art. 157, bis, prevê a possibilidade de punição da conduta daquele que, de forma dolosa, acessar ilegalmente sistemas de dados confidenciais ou a um banco de dados pessoais, revelando a outrem informação privada ou sigilosa, com a agravante da conduta quando o autor é funcionário público. Prevê, também, a punição penal relativa às violações de dados e criações eletrônicas de caráter intelectual.

2.2- Chile

O Chile foi o primeiro país da América Latina a atualizar sua legislação sobre a matéria. Através da Lei n.19.223 (de 28 de maio de 1993) foram tipificadas várias figuras relativas à criminalidade informática, dentre elas: a) Destruição ou inutilização maliciosa de *hardware* e *software*, assim como alteração de seu funcionamento por qualquer meio; b) Acesso ilegítimo à informação contida em um sistema com o intuito de apoderar-se dela, usá-la ou conhecê-la indevidamente; c) Difusão maliciosa de dados confidenciais contidos em um sistema de informação.

No ordenamento jurídico chileno, assim como acontece na legislação argentina, o *software* é considerado obra intelectual e, como tal, é protegido.

3.0 - Estados Unidos

As primeiras normas sobre crimes informáticos nos Estados Unidos começaram a surgir no fim da década de 1970.

O ordenamento jurídico-penal americano tem no combate à criminalidade econômica uma prioridade[191], isto explicando a enormidade de recursos intelectuais e financeiros despendidos na luta contra os comportamentos ilícitos nessa área. Tal priorização levou a um cuidado de tutelar o direito informático. Criou-se, em virtude disso, uma respeitável estrutura legislativa que protege contra o ataque a sistemas eletrônicos, o uso ilegítimo de senhas, invasões eletrônicas na privacidade, entre outras transgressões.

A primeira e a principal legislação federal que cuidou de responsabilizar criminalmente as condutas pepertradas pelo meio informático foi a CFAA (*Computer Fraud and Abuse Act*. de 1986), que tipificou condutas como a de intrusão informática para a obtenção de segredos nacionais com a intenção de prejudicar o país, ou para obter vantagens financeiras. Embora muitas outras leis regionais possam ser aplicadas aos diferentes tipos de crimes de computador, é a CFAA, até hoje, a principal peça legislativa aplicável à maioria dos delitos informáticos.

Os Estados Unidos possuem duas leis federais mais utilizadas para a repreensão aos crimes de computador, quais sejam: 18 USC, Capítulo 47, Seção 1.029, e a Seção 1.030, de 1994 que modificou e atualizou a *Computer Fraud and Abuse Act*.[192]

Além desse fator, foram introduzidas modificações com o escopo de complementar a Lei de Privacidade das Comunicações Eletrônicas de 1986, no sentido de suprir a anterior omissão à proteção legal à interceptação de comunicações eletrônicas. A CFAA, também foi alterada com o intuito de coibir o ato de transmitir

[191] BRUNO, Assuma. *La lotta contro la criminalitá econômica nell´ordinamento degli stati uniti. Apud* GAGLIARDI, Pedro Luiz Ricardo. *Crimes cometidos com uso de computador*. Tese de Doutorado, USP, p.85.

[192] LIMA, Paulo Marco Ferreira. *Crimes de computador e segurança nacional.* Campinas: Millennium Editora, 2006, p.99.

vírus ou qualquer outra espécie de programa destrutivo maligno, punindo a transmissão de programa, informação, códigos ou comandos que causem danos ao computador, a sistemas informáticos, às redes, à informação, aos dados ou a outros programas.

Por outro lado, o legislador americano procurou não definir os vírus informáticos, mas sim descrevê-los, com o intuito de capacitar a legislação para coibir qualquer forma de ataque aos sistemas informáticos que possa advir com a diversificação tecnológica.

Os EUA, no que toca ainda à repreensão penal à disseminação de vírus de computador, dá tratamento penal diferenciado àqueles que de maneira culposa lançam ataques de vírus e àqueles que assim agem com intenção (dolo) de causar danos efetivos. São definidos dois níveis de tratamento legislativo: primeiro para aquele que cria o vírus e, dolosamente, o dissemina (estabelecendo para aqueles que intencionalmente causam um dano pela transmissão de um vírus uma pena de até 10 anos de prisão mais multa); e para aqueles que o transmitem de forma negligente a sanção para esses casos é tão somente pena de multa até um ano de prisão.

Pela estrutura legislativa americana, em geral, sã o coibidas quaisquer condutas que, de alguma forma: a) atentem contra o sigilo de informação eletrônica de defesa nacional, de assuntos exteriores, de energia atômica ou qualquer outra informação restrita de caráter estratégico; b) envolvam a um ordenador pertencente a departamentos ou agências do governo dos Estados Unidos; c) envolvam banco ou qualquer outra classe de instituição financeira; d) envolvam comunicações interestaduais ou internacionais; e) afetem pessoas ou ordenadores em outros países ou Estados.

A fraude eletrônica, através de manipulação de documentos eletrônicos, também foi objeto de preocupação do Estado americano, estando prevista na Seção

1029. Referida legislação proíbe a fraude e qualquer atividade relacionada que possa realizar-se mediante o acesso ou uso de dispositivos falsificados (como cartões de crédito, números de contas etc). São elencadas nove figuras típicas em diversas, sendo imprescindível que o delito implique em dano ao comércio interestadual ou internacional. O elemento subjetivo é o mesmo para todas as figuras, o delito deve ser cometido dolosamente, havendo o agente atuado conscientemente com o intuito de extorquir.

Dessa forma, são punidos: a) produção, uso ou tráfico de disposi tivos de acesso falsificados. A pena para tais crimes vai de multa de U$50.000,00 ou duas vezes o valor do crime cometido e/ou até 15 (quinze) anos de cárcere, ou U$100.000,00 e/ou aé 20 (vinte) anos de cárcere em caso de reincidência; b) uso ou obtenção, sem autorização, de dispositivos de acesso, que visem obter um valor de U$1.000,00 ou mais durante um período de um ano. A pena para esses casos vai desde multa de U$10.000,00 ou duas vezes o valor do crime cometido e/ou até 10 (dez) anos de cárcere, U$100.000,00 e/ou até 20 (vinte) anos de prisão na reincidência; c) posse de 15 (quinze) ou mais dispositivos de acesso não-autorizados ou falsificados. Pena: Multa de U$10.000,00 ou duaz vezes o valor do crime cometido e/ou até 10 (dez) anos de prião, U$100.000,00 e/ou até 20 (vinte) anos de cárcere se reincidir; d) fabricação, tráfico ou posse de equipamento apto para a fabricação de dispositivos de acesso ilegais. Pena: Multa de U$50.000,00 ou duas vezes o valor do crime cometido e/ou até 15 (quinze) anos de cárcere, U$1.000.000,00 e/ou 20 (vinte) anos de prisão pela reincidência; e) realização de transações com dispositivos de acesso pertencentes à outra pessoa com o objetivo de obter dinheiro totaizando U$1.000,00 ou mais durante o período de um ano. A pena será de multa de U$10.000,00 ou duas vezes o valor do crime cometido e/ou até 10 anos de cárcere, ou U$100.000,00 e/ou até 20 (vinte) anos em caso de reincidência;

f) oferecer algum dispositivo de acesso ou vender informação que possa ser usada para conseguir acesso a algum sistema sem a autorização do proprietário do sistema de acesso. Pena: Multa de U$50.000,00 ou duas vezes o valor do crime e/ou até 15 (quinze) anos de cárcere, U$100.000,00 e/ou até 20 (vinte) anos em se tratando de reincidência; g) uso, produção, tráfico ou posse de instrumentos de telecomunicações que tenham sido alterados ou modificados para obter um uso não-autorizado de um serviço de telecomunicações. Pena: Multa de U$50.000,00 ou o dobro do valor do crime cometido e/ou até 15 (quinze) anos de prisão, ou U$100.000,00 e/ou até 20 (vinte) anos de cárcere na reincidência; h) uso, fabricação, tráfico ou posse de receptores, escaneadores ou *hardware* ou *software* usado para alterar ou modificar instrumentos de telecomunicações para obter acesso não-autorizado a serviços de telecomunicações. Inclui-se aqui os *scanners* de uso muito difundido para a interceptação de chamadas de telefones celulares. Pena: Multa de U$50.000,00 ou duas vezes o valor do crime e/ou até 15 (quinze) anos de prisão, ou U$100.000,00 e/ou até 20 (vinte) anos pela reincidência; i) passar-se por membro de companhia de cartão de crédito ou seu agente para obter vantagem econômica ilícita ou passar-se pelo legítimo detentor do cartão de crédito para a companhia com objetivo de obter vantagem financeira. Pena: Multa e/ou até 1 (um) ano de cárcere, até 10 (dez) anos de prisão na reincidência.

No que toca à Lei sobre Abuso e Fraude Informática de 1986 (28 USC, Capítulo 47, Seção 1.030), cuida essa legislação federal da responsabilização criminal daqueles que acessem dolosamente, sem a devida autorização ou fraudulentamente, a sistemas governamentais, estabelecendo diversas sanções. Dentre as condutas puníveis estão: a) aquisição de informação restrita relacionada com defesa nacional, assuntos exteriores ou sobre energia nuclear com o objetivo ou possibilidade de que sejam usados contra os interesses nacionais; b) obtenção de registros de instituição fiscal,

creditícia ou financeira; c) ataque a um ordenador de uso exclusivo de departamento ou agência do governo do EUA; d) fraude mediante acesso a um sistema eletrônico de interesse federal para obtenção de vantagem econômica ilícita; e) uso de um ordenador utilizado em comércio interestadual, para a transmissão de programa, informação, sódigos ou comandos a outro sistema informático, visando provocar danos ou permitir que outrem possa acessar ou provocar danos. Nesta figura também é prevista a forma culposa, recebendo também a responsabilização penal aquele que de forma imprudente cause prejuízo aos proprietários ou operadores dos ordenadores, provocando danos econômicos superiores a U$1.000,00, ou aquele que altera ou potencialmente modifica um exame ou tratamento médico); f) efetivar fraude eletrônica utilizando *passwords* ou informação similar que possibilite acesso a um sistema sem a devida autorização, com o intuito de afetar o comércio estatal ou internacional.

Por derradeiro, nos EUA existe uma vasta legislação dentro de cada um dos seus mais de cinquenta Estados[193], que cuida de tipificar uma série de delitos informáticos e outras regras atinentes ao direito penal informático.

Do presente modo, a opção americana foi a de cercar as condutas criminosas de forma a não existirem lacunas para comportamentos desviantes na área da criminalidade informática.

[193] São exemplos dessas legislações: 1) *Arizona Computer Crimes Laws*, *Section* 13-2316; 2) *Iowa Computer Crime Law, Chapter*, 716A.9; 3) *Kansas Computer Crime Law, Kansas*, *Section* 1-3755; 4) *Lousiana evised Status* 14:73.4 (*Computer Fraud*); 5) *Michigan Compilam Laws Section 752.794* (*Acces to computer for devising or executing scheme to defraud or obtain money, property, or services*).

CAPÍTULO IV- DIREITO PENAL DO INIMIGO E OS CRIMES DE COMPUTADOR

Partindo-se de uma análise histórica do Direito Penal como hoje o conhecemos, é forçoso lembrar que diversas etapas foram ultrapassadas pela humanidade, ou seja, o Direito Penal foi conhecido em tempos remotos como de intensa vingança privada, em que a pena era aplicada de forma arbitrária, sem fundamentação e desproporcional ao delito que lhe deu ensejo, até chegar ao Direito Penal moderno, que se notabiliza por ser garantista, protetivo dos direitos individuais das pessoas frente a um possível arbítrio estatal.

Ocorre que certas modalidades de infações penais, típicas dos tempos atuais, tais como, a da área da informática, tráfico de drogas, terrorismo, crime organizado etc, vêm trazendo grande desassossego aos operadores do Direito Penal, colocando, para alguns, em risco, o Direito Penal e o Direito Processual Penal Constitucional, garantistas por excelência.

É, justamente neste contexto, que surge a denominada "Teoria do Direito Penal do Inimigo", propalada na Alemanha por Gunther Jakobs, que passou a ganhar eco com a recente onda de ataques de grupos terroristas aos países de maior influência no mundo atual.

Com o surgimento desses novos delitos decorrentes dos riscos pós-modernos, e a expansão do Direito Penal, a consequência foi o aumento de tipos penais. Porém, as penas tendem a serem mais brandas e alternativas.

Este fato decorre da implementação de acordos no âmbito do processo penal, onde as penas privativas de liberdade são substituídas por penas alternativas, como restritivas de direito e de multa.

Em decorrência da necessidade de combate aos novos e numerosos delitos, e da constatação de que o Direito Penal Clássico, com suas regras e princípios rígidos, não está preparado para tanto, surge como alternativa a "teoria dualista do sistema penal com regras de imputação e princípios de garantias processuais de dois níveis"[194]

A idéia trazida por essa teoria é a existência de dois tipos de Direito, um voltado para o cidadão e outro voltado para o inimigo.

Segundo os defensores dessa corrente, não se trata de contrapor duas esferas isoladas do Direito Penal, mas de descrever dois pólos de um só contexto jurídico-penal.

O Direito voltado para o cidadão caracteriza-se pelo fato de que, ao violar a norma, ao cidadão é dada a chance de restabelecer a vigência dessa norma, de modo coativo, mas como cidadão pela pena. Neste caso, o Estado não vê no indivíduo um inimigo, que precisa ser destruído, mas o autor de um fato normal, que, mesmo cometendo um ato ilícito, matêm seu *status* de pessoa e seu papel de cidadão dentro do Direito. Além do que, não pode despedir-se da sociedade pelo seu ato.

Porém, existem indivíduos que pelos seus comportamentos, pelos tipos de crimes que cometem, ou pela sua ocupação profissional (criminalidade econômica, tráfico de drogas), ou por participar de uma organização criminosa (terrorismo), "se afastaram, de maneira duradoura, ao menos de modo decidido, do Direito, isto é, que não proporciona a garantia cognitiva mínima necessária a um tratamento como pessoa"[195] e, portanto, devem ser tratados como inimigos, sendo que para estes se volta o Direito Penal do Inimigo.

---

[194] SILVA SANCHEZ, Jesus-Maria. *A expansão do direito penal. Aspectos da política criminal nas sociedades pós-industriais.* Tradução de Luiz Otávio de Oliveira Rocha. São Paulo: Revista dos Tribunais, 2002, p.142.

[195] JAKOBS, Gunther, MELIA, Manuel Cancio. *Direito Penal do Inimigo, noções e críticas*. Tradução de: André Luis Callegari e Nereu José Giacomolli. 2 ed. Porto Alegre: Livraria do Advogado Editora, 2007, p.36.

Argumenta Silva Sanchez[196] que o Direito Penal leva em conta que aos delitos socioeconômicos são imputadas penas privativas de liberdade, sendo que para estas devem ser respeitadas todas as garantias e princípios processuais.

Ainda segundo o referido autor, essa teoria tem duas consequências:

> "Por um lado, naturalmente, admitir as penas não privativas de liberdade, como um mal menor, dadas as circunstâncias, para as infrações nas quais têm se flexibilizado os pressupostos de atribuição de responsabilidade. Mas, sobretudo, exigir que ali onde se impõem penas de prisão e, especialmente, penas de prisão de larga duração, se mantenha todo o rigor dos pressupostos clássicos de imputação de responsabilidade".[197]

Preconiza ainda um Direito Penal ao mesmo tempo funcional e garantista, onde sejam preservadas as garantias individuais para o núcleo dos delitos individuais clássicos, para os quais é prevista a pena de prisão. Mas, para as novas modalidades de delitos, os quais não colocam um perigo real a bens individuais, sustenta a flexibilização controlada das regras de imputação (a saber, responsabilidade penal das pessoas jurídicas, ampliação dos critérios de autoria ou da comissão por omissão, dos requisitos de vencibilidade do erro) como também dos princípios políticos-criminais, como, por exemplo, o princípio da legalidade, o mandato de determinação ou o princípio da culpabilidade.

---

[196] SILVA SANCHEZ, Jesus-Maria. *A expansão do direito penal. Aspectos da política criminal nas sociedades pós-industriais.* Tradução de Luiz Otávio de Oliveira Rocha. São Paulo: Revista dos Tribunais, 2002, p.142.

[197] SILVA SANCHEZ, Jesus-Maria. *A expansão do direito penal. Aspectos da política criminal nas sociedades pós-industriais.* Tradução de Luiz Otávio de Oliveira Rocha. São Paulo: Revista dos Tribunais, 2002, p.143.

A teoria em questão atende um critério de proporcionalidade e razoabilidade político-jurídica, um meio termo entre o Direito Penal mínimo e rígido e um Direito Penal amplo e flexível.

Suas principais bandeiras são: a) flexibilização do princípio da legalidade (descrição vaga dos crimes e das penas); b) inobservância de princípios básicos como da ofensividade, da exteriorização do fato, da imputação objetiva, etc.; c) aumento desproporcional de penas; d) criação artificial de novos delitos (delitos sem bens jurídicos definidos; e) endurecimento sem causa da execução penal; f) exagerada antecipação da tutela penal; g) corte de direitos e garantias processuais fundamentais; h) concessão de prêmios ao inimigo que se mostra fiel ao Direito (delação premiada, colaboração premiada etc.); i) flexibilização da prisão em flagrante (ação controlada); j) infiltração de agentes policiais; k) uso e abuso de medidas preventivas ou cautelares (interceptação telefônica sem justa causa, quebra de sigilos não fundamentados ou contra a lei); l) medidas penais dirigidas contra quem exerce atividade lícita (bancos, advogados, joalheiros, leiloeiros etc.).[198]

A perda de tradições liberais, com a flexibilização das garantias individuais e das regras de imputação, é o preço pago pelo Direito Penal funcional, com o fim de atender e aplacar o sentimento de insegurança social. Porém, um Direito Penal de urgência e demasiado amplo causa insegurança jurídica e atende a fins basicamente simbólicos, carecendo de eficácia prática, e despertando um sentimento de impunidade generalizado na sociedade.

Além desse fator, o avanço acelerado da macrocriminalidade moderna, inclusive na esfera da informática, e a ânsia de contê-la é um terreno fértil para o surgimento de novas teorias funcionalistas como o Direito Penal do Inimigo.

---

[198] GOMES, Luiz Flávio. *Críticas à tese do direito penal do inimigo*. Disponível em: http://www.mundolegal.com.br/?Fuse_Action=Artigo_Detalhar&did=15528. Acesso em: 29/09/2007, às 17h20min.

A tendência do Direito Penal moderno a um aspecto simbólico cada vez maior e a necessidade de tornar-se mais efetivo frente às novas formas de criminalidade moderna, acarretaram o surgimento de novas formas de pena, mais brandas que a pena de prisão, em decorrência de uma possível flexibilização das regras de imputação e princípios e garantias processuais, como já fora demosntrado acima.

Porém, constata-se, com a tese do Direito Penal do Inimigo, uma outra tendência do Direito Penal moderno, a total exclusão dos direitos e garantias processuais dos indivíduos classificados como inimigos, caracterizando uma nova velocidade do Direito Penal.

Dessa forma, o Direito Penal do Inimigo caracteriza, segundo Silva Sanchez, uma terceira velocidade do Direito Penal. Na qual o "Direito Penal da pena de prisão concorra com uma ampla relativização de garantias político-criminais, regras de imputação e critérios processuais".[199]

Defende ainda o autor que o Direito Penal de terceira velocidade deve ser reduzido a um âmbito de pequena expressão, em caso de absoluta necessidade, subsidiariedade e eficácia. Porém, conclui que o mesmo é inevitável frente a determinados delitos como o terrorismo, delinquência sexual violenta e reiterada e criminalidade organizada. Além de considerá-lo um "mal menor" frente o contexto de emergência em que está inserido, profetizando seu crescimento e até sua estabilidade.[200]

Mas quem seriam esses inimigos? Em princípio, nem todo delinquente é um adversário do ordenamento jurídico. Por isso, a introdução de um cúmulo de linhas e

[199] SILVA SANCHEZ, Jesus-Maria. *A expansão do direito penal. Aspectos da política criminal nas sociedades pós-industriais.* Tradução de Luiz Otávio de Oliveira Rocha. São Paulo: Revista dos Tribunais, 2002, p.148.

[200] SILVA SANCHEZ, Jesus-Maria. *A expansão do direito penal. Aspectos da política criminal nas sociedades pós-industriais.* Tradução de Luiz Otávio de Oliveira Rocha. São Paulo: Revista dos Tribunais, 2002, p.148,149 e 151.

fragmentos de Direito Penal do Inimigo no Direito Penal Geral é um mal, desde a perspectiva do Estado de Direito.

Inimigos são indivíduos que se caracterizam, primeiro, por repelir o ordenamento jurídico e perseguirem a destruição dessa ordem e, segundo, a consequência disso, por sua especial periculosidade para a ordem jurídica, dado que tais indivíduos não oferecem garantias de mínima segurança cognitiva de um comportamento pessoal, é dizer, seu comportamento já não é calculado conforme as expectativas normativas vigentes na sociedade.

O Direito penal do inimigo necessita de eleição de um inimigo e caracteriza-se, ademais, pela oposição que faz ao Direito penal do cidadão onde vigoram todos os princípios limitadores do poder punitivo estatal.

O inimigo, para Jakobs[201], é uma não-pessoa, e, segundo ele, "um indivíduo que não admite ser obrigado a entrar em um estado de cidadania não pode participar dos benefícios do conceito de pessoa".

Como o inimigo é uma não-pessoa, a qual o Estado visa combater e neutralizar, a ele são previstos os direitos e grantias processuais a que os cidadãos têm direito. Dessa forma, o inimigo não pode ser tratado como sujeito processual.

Quando comete um delito, ao cidadão é previsto o devido processo legal que resultará numa pena como forma de sanção pelo ato ilícito cometido. Ao inimigo, o tratamento é diverso.

Assim, aos inimigos não são previstos, no curso do processo, vários direitos permitidos ao cidadão, como o acesso aos autos do inquérito policial, o direito de solicitar a prática de provas, de assitir aos interrogatórios, de se comunicar com seu advogado. Além de que, são admitidas contra ele provas obtidas por meios ilícitos,

[201] JAKOBS, Gunther, MELIA, Manuel Cancio. *Direito Penal do Inimigo, noções e críticas*. Tradução de: André Luis Callegari e Nereu José Giacomolli. 2 ed. Porto Alegre: Livraria do Advogado Editora, 2007, p.36.

como as escutas telefônicas, agentes infiltrados, investigações secretas, além de ter-se um avanço da prisão preventiva como regra, que é exceção num processo ordenado. Portanto, o processo contra o inimigo não pode denominar-se "processo" e sim procedimento de guerra.[202]

Jakobs utiliza a periculosidade do agente para caracterizar o inimigo, contrapondo-o ao cidadão que, apesar de seu ato, oferece garantia de que se conduzirá como cidadão, atuando com fidelidade ao ordenamento jurídico, de forma que sua personalidade tende para tanto. Já o inimigo não oferece essa garantia, devendo ser combatido pela sua periculosidade, e não punido segundo a sua culpabilidade.

No Direito Penal do Inimigo, a punibilidade avança para o âmbito interno do agente e da preparação, e a pena se dirige à segurança frente aos atos futuros, caracterizando essa teoria como um direito do autor e não do fato.

Assim, o ponto de partida ao qual se ata a regulação é a conduta não realizada, mas planejada, isto é, não o dano à vigência da norma que tenha sido realizado, mas o fato futuro. Dito de outra forma, o lugar do dano atual à vigência da norma é ocupado pelo perigo de danos futuros: uma regulação própria do Direito Penal do Inimigo.

O Direito Penal do Inimigo não repele a idéia de que as penas sejam desproporcionais, ao contrário, como se pune a periculosidade, não entra em jogo a questão da proporcionalidade aos danos causados.

Em um outro plano, deve limitar-se, previamente, que a denominação Direito Penal do Inimigo não pretende ser sempre pejorativa. Certamente, um Direito Penal o Inimigo é indicativo de uma pacificação insuficiente, entretanto esta, não

---

[202] JAKOBS, Gunther, MELIA, Manuel Cancio. *Direito Penal do Inimigo, noções e críticas*. Tradução de: André Luis Callegari e Nereu José Giacomolli. 2 ed. Porto Alegre: Livraria do Advogado Editora, 2007, p.39-41.

necessariamente deve ser atribuída aos pacificadores, mas pode referir-se aos rebeldes. Ademais, um Direito Penal do Inimigo implica, pelo menos, um comportamento desenvolvido em regras, ao invés de uma conduta espontânea e impulsiva.

Levando-se em conta que na criminalidade informática há a possibilidade de nos depararmos com sujeitos ativos de extrema periculosidade, destemidos de qualquer punição, ao Estado é dado o direito de procurar a segurança frente aos mesmos.

Dessa forma, por todo o exposto, pensamos que com a criminalidade informática não deva ser diferente, uma vez que, em alguns casos, considerar o sujeito ativo desses crimes como inimigos, bem como flexibilizar as garantias processuais, será a única forma de combater tais condutas.

CAPÍTULO V-LEGISLAÇÃO EXISTENTE E PROPOSTAS LEGISLATIVAS

1.0- Figuras típicas da informática existentes na legislação brasileira

Trata-se de característica fundamental do ordenamento jurídico, o dinamismo de seus preceitos, que permite a adequação das normas jurídicas às constantes evoluções nos diversos campos da atividade humana. Seria temerário se o Poder Legislativo restasse inerte aos relevantes fenômenos sociais; por não editar os ditames legais a reger as novas situações de fato.

Ressalva-se que, evidentemente, seria impossível abranger no texto legal todos casos que se possam verificar em concreto. Por este motivo, nos casos de lacunas na legislação, o próprio ordenamento dita os meios a supri-lo; uma vez que o judiciário não pode escusar-se de apreciar a questão sob a alegação de falta de disposição legal quanto à matéria. Não se demonstra coerente, porém, que os operadores do direito vejam-se obrigados a utilizarem, por longo lapso temporal, as fontes subsidiárias para a resolução das celeumas. A necessidade de criação da norma pode ser indicada por diversos fatores, dentre estes, a conjectura econômica, política ou social do país.

Se a estrutura normativa vigente se demonstra incapaz de dar resposta aos novos desafios, faz-se necessária a incorporação dos elementos indispensáveis de informática e cibernética para que nos seja permitido obter a devida segurança jurídica das relações sociais.

Porém, a necessidade de incorporação dos conceitos de informática à legislação vigente não significa que devamos esquecer todo o nosso sistema e criar um novo ordenamento jurídico. Mas, sim, o contrário, nosso sistema legal se encontra

atualmente desenhado para suportar sem maiores contratempos as modificações referidas.

A tipicidade das condutas antijurídicas obriga-nos a definir com precisão os novos delitos associados a esta revolução tecnológica. Aqui, duas situações devem ser analisadas.

A primeira delas tem a ver com a utilização dos meios informáticos para o cometimento de delitos já previstos em nossa legislação, cuja periculosidade se potencializa em virtude do elemento empregado.

A segunda espécie, de igual importância, diz respeito a novas condutas que, justamente pela impossibilidade de ser previstas pelos legisladores do passado com a tecnologia então existente, não restam contempladas em nosso ordenamento jurídico penal atual e constituem um sério risco para a segurança dos sistemas informáticos e as relações estabelecidas por meio deles.

Para responder a essas questões, os projetos legislativos devem observar a criação de novas figuras delitivas que tipifiquem condutas que agridem a sociedade e que violem novos bens jurídicos.

Não se pode olvidar também, da previsão de responsabilização dos servidores de internet que, por negligência ou dolo, facilitem o cometimento de delitos, assim como para o envio dos *spams*, que saturam a rede, provocando grave perturbação à tranqüilidade de seus usuários.

Somente com a devida regulamentação será obtida a segurança jurídica das relações eletrônicas naturalmente, podendo, quiçá, servir como base para futura regulamentação internacional.

Porém, a verdade é que o nosso atual Direito Penal da Informática é quase inexistente, sendo certo afirmar que muito pouco existe no âmbito legislativo quando se

trata do campo da informática. Diversamente não ocorre no que tange às condutas criminais que de qualquer forma mantenham relação ao meio informático, pouco se tem em termos de norma legal repressora de condutas atentatórias a bens jurídicos penalmente relevantes.

As primeiras iniciativas legislativas ocorreram com o Advento do Plano Nacional de Informática e Automação (CONIN), através da Lei n. 7.232/84, que veio a delimitar as principais diretrizes no âmbito da informática, e também com a Lei n. 7.646, de 1987 (revogada pela Lei n. 9.609, de 19 de Fevereiro de 1998), que foi o primeiro mecanismo legal a descrever condutas ou infrações de informática. A principal crítica feita a essa lei era o fato de que essa somente cuidou de proteger a propriedade intelectual dos programas de computador e sua comercialização.

Com o advento da Lei n. 9.609, de 19 de Fevereiro de 1998, foram revogados os dispositivos penais da Lei n. 7.646, de 1987, permanecendo, contudo, a imperfeição anterior, atualmente restando tipificadas as seguintes condutas:

> "Art. 12. Violar direitos do autor de programa de computador:
> Pena – Detenção de seis meses a dois anos ou multa.
> § 1º Se a violação consistir na reprodução, por qualquer meio, de programa de computador, no todo ou em parte, para fins de comércio, sem autorização expressa do autor ou de quem o represente:
> Pena - Reclusão de um a quatro anos e multa.
> § 2º Na mesma pena do parágrafo anterior incorre quem vende, expõe à venda, introduz no País, adquire, oculta ou tem em depósito, para fins de comércio, original ou cópia de programa de computador, produzido com violação de direito autoral.
> § 3º Nos crimes previstos neste artigo, somente se procede mediante queixa, salvo:
> I - quando praticados em prejuízo de entidade de direito público, autarquia, empresa pública, sociedade de economia mista ou fundação instituída pelo poder público;
> II - quando, em decorrência de ato delituoso, resultar sonegação fiscal, perda de arrecadação tributária ou prática de quaisquer dos crimes contra a ordem tributária ou contra as relações de consumo.

> § 4º No caso do inciso II do parágrafo anterior, a exigibilidade do tributo, ou contribuição social e qualquer acessório, processar-se-á independentemente de representação."

Outra norma incriminadora se encontra no Código de Defesa do Consumidor, que sanciona condutas ilícitas relacionadas à proteção das informações correlacionadas aos consumidores, armazenadas em banco de dados, nos seguintes termos:

> "Art. 72. Impedir ou dificultar o acesso do consumidor às informações que sobre ele constem em cadastros, banco de dados, fichas e registros:
> Pena - Detenção de seis meses a um ano ou multa."

> "Art. 73. Deixar de corrigir imediatamente informação sobre consumidor constante de cadastro, banco de dados, fichas ou registros que sabe ou deveria saber ser inexata:
> Pena - Detenção de um a seis meses ou multa."

Na esfera das interceptações telefônicas ilícitas, outra forma de repressão penal ligada à informática é a que garante o direito à inviolabilidade das comunicações telefônicas assegurada constitucionalmente pelo inciso XII do art. 5º da Constituição Federal de 1988 e pela Lei n. 9.296, de 24 de julho de 1996, que regulamente o referido dispositivo.

A norma constitucional estabelece que:

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

Ainda nessa esteira, o art. 10 da Lei Federal n. 9.296/96 considera crime, punível com reclusão de 2 a 4 anos e multa, "realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo de Justiça, sem autorização judicial ou com objetivos não autorizados em lei".[203]Nos termos em que foi estabelecido este tipo penal, a conduta criminosa fica limitada aos fins visados pela lei em que se insere, ou seja, a obtenção de provas para fins policiais ou processuais, o que limita bastante a incriminação, pois se a interceptação informática não adequar-se ao modelo proposto o autor incidirá apenas no delito de violação de comunicação, previsto no artigo 155, §1º do Código Penal, punido mais brandamente. Percebe-se claramente a inadequação desse modelo para abranger todas as situações de interceptação, que hoje são usuais, que perturbam a normalidade das transmissões informáticas e telemáticas, cuja proteção já encontrou formulações mais precisas em outros países.[204]

Além dos já mencionados, outros tipos penais que descrevem crimes de informática, já existem na legislação pátria. Podemos citar os seguintes artigos:

> a) “Art. 153, §1º-A, do Código Penal, com a redação dada pela Lei Federal n. 9.983/2000, que tipifica o crime de divulgação de segredo: "Divulgar, sem justa causa, informações sigilosas ou reservadas, assim definidas em lei, contidas ou não nos sistemas de informações ou banco de dados da Administração Pública", punindo-o com detenção de 1 a 4 anos, e multa”;

[203] Regulamenta o art. 5º, inciso XII, da CF: "É inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal".

[204] Assim ocorreu em Portugal, onde existe o crime de interceptação legítima, inserido na Lei da Criminalidade Informática, Lei nº109/91, cujo artigo 8º dispõe: “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 destinados ou deles provenientes, será punido com pena de prisão de até três anos ou com pena de multa”.

O artigo 313-A, do Código Penal, introduzido pela Lei n. 9.983/2000, que tipificou o crime de inserção de dados falsos em sistema de informações, com a seguinte redação:

> "Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano", punindo-o com pena de reclusão, de 2 (dois) a 12 (doze) anos, e multa."

O artigo 313-B, do Código Penal, introduzido pela Lei n. 9.983/2000, que tipificou o crime de modificação ou alteração não autorizada de sistema de informações, com a seguinte redação:

> "Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente", cominando-lhe pena de detenção, de 3 (três) meses a 2 (dois) anos, e multa."

O artigo 325, §1º, incisos I e II, introduzidos pela Lei n. 9.983/2000, tipificando novas formas de violação de sigilo funcional, nas condutas de quem,

> "I – permite ou facilita, mediante atribuição, fornecimento e empréstimo de senha ou qualquer outra forma, o acesso de pessoas não autorizadas a sistemas de informações ou banco de dados da Administração Pública";

E de quem,

> "II – se utiliza, indevidamente, do acesso restrito", ambos sancionados com penas de detenção de 6 meses a 2 anos, ou multa."

O artigo 2º, inciso V, da Lei Federal n. 8.137/90, que considera crime,

> "utilizar ou divulgar programa de processamento de dados que permita ao sujeito passivo da obrigação tributária possuir informação contábil diversa daquela que é, por lei, fornecida à Fazenda Pública."

O artigo 72 da Lei n. 9.504/97, que cuida de três tipos penais eletrônicos de natureza eleitoral:

> "Art. 72. Constituem crimes, puníveis com reclusão, de cinco a dez anos: I - obter acesso a sistema de tratamento automático de dados usado pelo serviço eleitoral, a fim de alterar a apuração ou a contagem de votos; II - desenvolver ou introduzir comando, instrução, ou programa de computador capaz de destruir, apagar, eliminar, alterar, gravar ou transmitir dado, instrução ou programa ou provocar qualquer outro resultado diverso do esperado em sistema de tratamento automático de dados usados pelo serviço eleitoral; III - causar, propositadamente, dano físico ao equipamento usado na votação ou na totalização de votos ou a suas partes."

A Lei 10.764, de 12 de novembro de 2003, aperfeiçoou a redação do art. 241 do Estatuto da Criança e do Adolescente que pune a difusão da pornografia infantil na internet para quem,

> "Apresentar, produzir, vender, fornecer, divulgar ou publicar, por qualquer meio de comunicação, inclusive rede mundial de computadores ou internet, fotografias ou imagens com pornografia ou cenas de sexo explícito envolvendo criança ou adolescente", punindo com reclusão de 2 (dois) a 6 (seis) anos, e multa."

O parágrafo 1º do referido dispositivo prevê que,

> "Incorre na mesma pena quem: I - agencia, autoriza, facilita ou, de qualquer modo, intermedeia a participação

> de criança ou adolescente em produção referida neste artigo; II - assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens produzidas na forma do *caput* deste artigo; III - assegura, por qualquer meio, o acesso, na rede mundial de computadores ou internet, das fotografias, cenas ou imagens produzidas na forma do *caput* deste artigo."

Já o parágrafo 2º do mesmo artigo prevê pena de reclusão de 3 (três) a 8 (oito) anos:

> "I - se o agente comete o crime prevalecendo-se do exercício de cargo ou função; II - se o agente comete o crime com o fim de obter para si ou para outrem vantagem patrimonial."

Tais tipificações esparsas não resolvem o problema da criminalidade na internet, do ponto de vista do direito objetivo, mas revelam a preocupação do legislador infraconstitucional de proteger os bens informáticos e de assegurar, na esfera penal, a proteção a dados de interesse da Administração Pública e do Estado democrático, bem como à privacidade "telemática" do indivíduo.

Para Ivette Senise Ferreira essas leis estão

> "longe de esgotarem o assunto, deixaram mais patente a necessidade do 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".[205]

Concordamos com a autora. A legislação penal existente no ordenamento jurídico brasileiro atual, no que se refere às infrações cometidas no âmbito informático e

[205] *A criminalidade informática*. In: LUCCA, Newton de e SIMÃO FILHO, Adalberto (Coordenadores) e outros. *Direito e internet – aspectos jurídicos relevantes*. 2ª edição, São Paulo: Quartier Latin, 2005, p. 208.

através de computadores, suas redes ou sistemas, não é eficaz para reprimir de forma adequada todas as condutas ilícitas praticadas nessa área.

Isso se dá, em parte, por serem tais ações efetivadas com a utilização de tecnologia muito específica, com características próprias e com evolução e desenvolvimento extremamente céleres, fazendo com que o conhecimento técnico dos legisladores seja insuficiente para antever toda a problemática possível de ocorrer.

Além desse fator, inúmeras são as críticas à Parte Especial do Código Penal, para a qual tais infrações soam demasiadamente modernas, e somente com um esforço incomum podem ser adaptadas às normas ali existentes.

Com certa dificuldade, alguns dispositivos penais poderiam ser aplicados para a incriminação de certas condutas praticadas pelo ou contra o meio informático, dentre eles podemos citar, a violação de correspondência (art. 151 e 152), divulgação de segredo (art. 153 e 154), furto mediante fraude (art.155, parágrafo 4, II, segunda figura) e falsificação documental (art. 297 a 299). Tais figuras criminosas foram criadas sob a ótica de outra realidade, sendo que as atuais condutas praticadas através e com a tecnologia dos computadores lhes são, evidentemente, estranhas.

Sem uma codificação ou legislação única, alguns crimes de computador podem acabar, pela própria velocidade da tecnologia da área, sem qualquer aplicabilidade prática. A evolução tecnológica quase que diária na área da informática pode dificultar a aplicação do nosso atual Código Penal para questões relacionadas ao tema, ou seja, o enquadramento dos crimes comuns às condutas típicas do delito de informática.

Dessa forma, concluímos que o ordenamento jurídico penal brasileiro não oferece solução para condutas lesivas ou potencialmente lesivas que possam ser praticadas através da internet e que não encontrem adequação típica no reduzido rol de

delitos novos existentes no Código Penal e nas leis especiais brasileiras que tratam da matéria ou nos inexistentes tratados internacionais.

O esforço interpretativo para adequar alguns crimes informáticos à nossa legislação penal evidencia, justamente, a atipicidade dessas condutas. Inegável, também, é a existência de dificuldades na punição das ações cometidas mediante e contra o meio computacional pela atual legislação, Ademais, não se pode olvidar da exigência constitucional de lei anterior para definição de crime e aplicação de pena, sendo, pois, vedado, o uso da analogia e ampliações para a incriminação dessas condutas. Necessária se faz a criação de novas leis, determinando novas condutas típicas, reconhecendo-se que um tratamento específico da questão acabará por facilitar a punição dos agentes criminosos.

Com o escopo de examinar a questão de forma mais global, passemos ao exame dos projetos e substitutivos legislativos em trâmite no Congresso Nacional quanto aos crimes de computador.

2.0- Propostas legislativas

À vista da necessidade crescente em nosso meio de uma resposta penal para o problema da criminalidade informática, têm-se visto inúmeros projetos de leis que visam à regulamentação jurídica do assunto.

Existem algumas propostas tramitando nas casas legislativas. Embora não seja possível afirmar quando ou qual proposta será aprovada, vale citar e tecer comentários sobre alguns dos projetos de lei.

Dentre os projetos mais significativos, e que têm merecido destaque por parte da doutrina, apontam-se: Projeto de Lei nº. 76/2000, Projeto de Lei nº. 137/2000,

Projeto de Lei nº. 89/2003, Projeto de Lei nº. 279/2003 e Projeto de Lei nº. 508/2003. Além desses, existem quase duzentos outros projetos tramitando no Congresso Nacional.

O Projeto de Lei do Senado nº76/2000, de autoria do Senador Renan Calheiros, apresenta tipificação dos delitos cometidos com o uso do TIC e atribuiu-lhes as respectivas penas em sete categorias, quais sejam: 1) contra a inviolabilidade de dados e sua comunicação; 2) contra a propriedade e o patrimônio; 3) contra a honra e a vida privada; 4) contra a vida e a integridade física das pessoas; 5) contra o patrimônio fiscal; 6) contra a moral pública e a opção sexual e 7) contra a segurança nacional.

O Projeto de Lei do Senado nº. 137/2000, de autoria do Senador Leomar Quintanilha atribuiu o triplo das penas dos crimes já tipificados no Código Penal se forem cometidos usando ferramentas de TIC.

O Projeto de Lei do Senado nº. 279/2003, de autoria do Senador Delcídio Amaral, visa a obrigar os prestadores de serviços de correio eletrônico (e-mail) a manter cadastro detalhado dos titulares de suas respectivas contas. Desse cadastro constarão: 1) se pessoa física: número do cadastro de pessoa física (CPF), nome completo, endereço residencial, número da carteira de identidade (RG), data e órgão de expedição; 2) se pessoa jurídica: a razão social, o endereço completo e o número de Cadastro de Pessoa Jurídica (CNPJ).

O Projeto de Lei do Senado nº. 508/2003 veda a divulgação de informações privadas. Seu longo artigo 11 veda a divulgação de “informações privadas referentes, direta e indiretamente, a dados econômicos de pessoas físicas ou jurídicas, a origem racial, opinião política, filosófica ou religiosa, crenças, ideologia, saúde física ou mental, vida sexual, registros policiais, assuntos familiares ou profissionais, e outras que

a lei definir como sigilosas, salvo por ordem judicial ou com anuência expressa da pessoa a que se refere ou do seu representante legal".

Originário da Câmara como Projeto de Lei nº. 84/99, de autoria do Deputado Luiz Piauhylino, o Projeto de Lei da Câmara nº. 89/2003 altera o Código Penal (Decreto-Lei n. 2.848, de 07 de dezembro de 1940) e a Lei nº. 9.296 de 24 de julho de 1996, que cuida da interceptação das comunicações telefônicas, de qualquer natureza, para prova em investigação criminal e instrução processual penal. Para tanto, dispõe sobre os crimes cometidos na área da informática, e suas penalidades. Dispõe que o acesso de terceiros não autorizados pelos respectivos interessados, a informações privadas mantidas em redes de computadores, dependerá de autorização judicial.

O projeto tem a virtude de pretender se tornar a primeira lei brasileira que trata de uma maneira ampla e sistematizada dos crimes cometidos através dos meios informáticos[206]. Não apenas cria tipos penais novos, mas estende o campo de incidência de algumas figuras já previstas no Código Penal para novos fenômenos ocorrentes nos meios desmaterializados - impossíveis de terem sido previstos pelo legislador de 1940.

O projeto, na versão aprovada pelo Plenário da Câmara em novembro de 2003, criava os seguintes tipos penais, cometidos contra sistemas informáticos ou por

[206] Antes dele, apenas a Lei 9.983, de 14.07.2000, havia introduzido no Código Penal Brasileiro a figura qualificada do crime de divulgação de segredo (art. 153, §1º-A), cujo tipo prevê pena de detenção de um a quatro anos e multa para aquele que divulgar, sem justa causa, informações sigilosas ou reservadas, assim definidas em lei, contidas ou não nos sistemas de informações ou banco de dados da Administração Pública. Essa Lei introduziu, ainda, o chamado "peculato eletrônico", ao acrescentar no Código Penal os artigos 313-A e 313-B, os quais contêm a previsão de punição para o funcionário público que praticar a inserção de dados falsos em sistemas de informações (art. 313-A) - a pena prevista é de reclusão de dois a doze anos e multa -, bem como para aquele que modificar ou alterar sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente (art. 313-B), sendo a pena neste caso de detenção de três meses a dois anos e multa. Também a Lei nº 10.764 de 12.11.2003, alterou a redação do artigo 241 do Estatuto da Criança e do Adolescente, ampliando o descritor normativo do crime de pornografia infantil, para proibir a divulgação e publicação na Internet de fotografias e imagens contendo cenas de sexo explícito envolvendo criança ou adolescente, com pena de reclusão de dois a seis anos, além de multa. Essas duas leis anteriores, como se vê, trataram de definir de forma isolada tipos específicos de "crimes informáticos", possuindo ambas outros dispositivos que tratam de figuras delitivas que não se incluem nessa denominação. Não foram elaboradas, portanto, com a finalidade de criar um texto sistematizado e geral sobre delitos no campo da informática, objetivo a que se propõe o projeto de lei ora em comento.

meio deles: a) *acesso indevido a meio eletrônico* (art. 154-A); b) *manipulação indevida de informação eletrônica* (art. 154-B); c) *pornografia infantil* (art. 218-A); d) *difusão de vírus eletrônico* (art. 163, par. 3º.); e e) *falsificação de telefone celular ou meio de acesso a sistema informático* (art. 298-A). O projeto também elaborava os conceitos legais de "meio eletrônico" e "sistema informatizado", para efeitos penais (art. 154-C). Além disso, produzia as seguintes alterações em figuras penais já existentes: a) acrescentava a "telecomunicação" no tipo penal de *atentado contra a segurança de serviço de utilidade pública* (art. 265 do Código Penal) e no de *interrupção ou perturbação de serviço telegráfico ou telefônico* (art. 266 do Código Penal); b) estendia a definição de *dano* do art. 163 do Código Penal (crime de dano), por meio da equiparação à noção de "coisa" de elementos de informática como "dados", "informação" e "senha", sob a nova rubrica do dano eletrônico (acrescentando o parágrafo 2º, incisos. I e II); c) equiparava o cartão de crédito a documento particular no tipo *falsificação de documento particular*, acrescentando um parágrafo único ao art. 298 do Código Penal, sob a rubrica de falsificação de cartão de crédito; e d) permitia a interceptação do fluxo de comunicações em sistema de informática ou telemática, mesmo para crimes punidos apenas com detenção, por meio do acréscimo de um parágrafo 2º ao art. 2º da Lei 9.296, de 24 de julho de 1996.

À época, o Senador Marcelo Crivella[207], muito apropriadamente, entendeu que o projeto necessitava de alguns aperfeiçoamentos. É claro que isso se deve ao longo tempo de maturação que o projeto ficou na Câmara, mas também é fato de que o projeto original não contemplava algumas condutas já previstas em legislações de outros países, como bem lembrou o Senador. Nesse sentido, apresentou algumas emendas criando novas figuras delituais, tais como os crimes de falsidade informática (art. 154-C) e de

[207] O Senador Marcelo Crivella apresentou seu relatório quanto ao PLC 89/2003, na condição de membro da Comissão de Constituição, Justiça e Cidadania do Senado Federal.

sabotagem informática (art. 154-D), com a emenda relativa a eles assim redigida: a) *Falsidade Informática*: Art. 154-C. Introduzir, modificar, apagar ou suprimir dado ou sistema informatizado, ou, de qualquer forma, interferir no tratamento informático de dados, com o fim de obter, para si ou para outrem, vantagem indevida de qualquer natureza, induzindo a erro os usuários ou destinatários. Pena - detenção, de um a dois anos, e multa. Parágrafo único. Nas mesmas incorre quem, com a mesma finalidade, cria, disponibiliza ou divulga comunicação eletrônica falsa; b) *Sabotagem Informática*: Art. 154-D. Introduzir, modificar, apagar ou suprimir dado ou sistema informatizado, ou, de qualquer forma, interferir em sistema informatizado, com o fim de desorientar, embaraçar, dificultar ou obstar o funcionamento de um sistema informatizado ou de comunicação de dados à distância. Pena - detenção, de um a dois anos, e multa.

O acréscimo dessas duas figuras[208] traz inegáveis avanços ao projeto e o atualiza em relação às novas espécies de crimes informáticos cometidos por meio de redes eletrônicas.

A definição do crime de *falsidade informática*, e em especial a subespécie da *comunicação eletrônica falsa* (encapsulada no parágrafo único do art. 154-C), vem em boa hora diante do fenômeno que se tornou a marca cada vez mais comum dos crimes cometidos nos ambientes das redes informáticas: a associação entre fraudadores e *spammers*. A nova faceta de um problema que cada vez mais assola os usuários, o recebimento de mensagens não solicitadas (*spams*), agora vem adicionado às tentativas de fraudes eletrônicas (*scams*). Não se trata somente das tradicionais mensagens eletrônicas enganosas, contendo texto com as famosas "correntes" ou promessas de recompensa. Agora, elas costumam vir adicionadas de "programas maléficos" anexados

[208] O parecer do Senador Marcelo Crivella modifica o artigo 2º do PLC, que aborda os crimes contra a inviolabilidade dos sistemas informatizados e acrescenta outros na "Seção V do Capítulo VI do Título I do Código Penal". Assim, o atual artigo 154-C do PLC é transformado em 154-E, para que sejam acrescidos os dois novos artigos (o do crime de *falsidade informática* e o do crime de *sabotagem informática*).

à própria mensagem de e-mail. Uma vez abertos esses arquivos anexos, eles instalam programas espiões no computador do destinatário da mensagem, do tipo *spyware* ou *trojan* (cavalo de tróia), que permite que o agente criminoso tenha acesso remoto a todo o sistema do computador atacado. Um tipo específico desses programas espiões (o *keylogger*) tem capacidade para registrar qualquer tecla pressionada pelo usuário do computador infectado, bem como alguns movimentos do mouse, e enviar esses dados (por e-mail) para o agente criminoso que opera um computador remoto, tudo sem o conhecimento da vítima. Esse tipo de programa permite capturar informações críticas, como senhas e números de contas bancárias.

A redação do dispositivo em comento, a ser introduzido no Código Penal, pretende abarcar todas essas modalidades de fraudes eletrônicas, ao prever que incorre no tipo penal de *falsidade informática* todo aquele que "de qualquer forma interferir no tratamento informático de dados, com o fito de obter, para si ou para outrem, vantagem indevida de qualquer natureza, induzindo a erro os usuários ou destinatários" (*caput*). As fraudes eletrônicas perpetradas por e-mail, ainda que sem a utilização de programas espiões, também não escapam da regulamentação, na medida em que o parágrafo único esclarece que "nas mesmas penas incorre quem, com a mesma finalidade, cria, disponibiliza ou divulga comunicação eletrônica falsa". Na verdade o parágrafo único estabelece a figura do crime de *comunicação eletrônica falsa*, como se já observamos acima.

É suficiente, portanto, o simples envio de uma mensagem eletrônica falsa, com a finalidade de obter vantagem indevida, mediante a indução do operador ou usuário de um sistema informático a erro. O artifício ou meio fraudulento necessário à caracterização do crime pode ser exclusivamente a mensagem eletrônica falsa, desde que daí surta um duplo resultado: a vantagem indevida (ilícita) e o prejuízo alheio (da

vítima). A consumação propriamente dita exige esses dois elementos (vantagem ilícita e dano patrimonial), mas a figura do crime de *falsidade informática* admite a tentativa, da mesma forma como o estelionato tradicional (do art. 171 do Código Penal). Em outras palavras, aquele que envia mensagem eletrônica falsa, com essa finalidade (a obtenção de vantagem indevida), ainda que não se concretize o prejuízo do destinatário, responde pelo crime na modalidade tentada, até porque, nessa hipótese, a fraude já estaria caracterizada.

É importante também destacar que a regra do art. 154-C, que se pretende introduzir no Código Penal por meio do projeto, não objetiva e nem tampouco resolveria o problema específico do *spam* – o envio de mensagens não solicitadas. A questão do *spam* deve ser tratada em uma lei específica, contendo uma regulamentação completa e exaustiva sobre o problema, que estabeleça os tipos penais, as exceções (os casos em que se legitima o envio de mensagens comerciais não solicitadas), atribua poderes a agências governamentais para fiscalizar e aplicar multas, contenha previsão das sanções civis e penais, dos limites das penas pecuniárias, atribua recompensa a quem prestar informações que auxiliem a desvendar identidades dos criminosos, entre outras medidas[209]. Algumas leis estrangeiras editadas recentemente sobre *spam* têm mais de cem dispositivos[210]. Além do mais, a questão do *spam* é objeto de vários projetos que estão tramitando atualmente no Congresso Nacional. O futuro art. 154-C se limita, como se disse antes, ao problema das fraudes eletrônicas, quer sejam elas cometidas com ou sem a utilização de e-mail. Trata-se de uma ferramenta legal para combater os *scammers*, e não propriamente os *spammers*.

[209] Essa é a opinião de REINALDO FILHO, Demócrito. *O projeto de lei sobre crimes tecnológicos (PL nº. 84/99). Notas ao parecer do Senador Marcello Crivella*. Disponível em: <http://jus2.uol.com.br/doutrina/texto.asp?id=5447>. Acesso em: 20 julho de 2008, às 17h45min.

[210] É o caso da lei americana (o *CAN-SPAM Act*) e da lei australiana (*Spam Act 2003*).

A figura do crime de *sabotagem informática*, delineado no descritor normativo do art. 154-D, pretende por sua vez alcançar outras modalidades de crimes informáticos cometidos em rede, a exemplo do conhecido "denial-of-service attack", um tipo de delito que pode resultar em significante perda de tempo e dinheiro para as vítimas, em geral empresas que operam serviços na internet ou em outras redes de arquitetura aberta.

O principal objetivo nesse tipo de ataque é impossibilitar a vítima (um sistema informático) de ter acesso a um particular recurso ou serviço. Em geral, não somente o operador do sistema atacado fica impossibilitado de fazer uso dele, mas também seus legítimos usuários. Por exemplo, existem *hackers* que atuam inundando uma rede informática por meio do envio de massivos pacotes de informações, impedindo assim o tráfico na rede (ainda que temporariamente) de todos os seus usuários; em outros casos, atuam tentando romper a conexão entre o computador do usuário ao do seu provedor, obstaculizando o acesso a um serviço prestado por esse último. Em suma, esse tipo de ataque essencialmente visa a desabilitar o computador da vítima ou a rede informática que ela usa para prestar ou receber um serviço. O pior é que esse tipo de ataque pode ser executado com limitados equipamentos contra sofisticados *site* de sistemas informáticos. Usando um velho e simples PC e uma conexão à internet de baixa velocidade, um *hacker* consegue incapacitar máquinas e redes informáticas tecnicamente sofisticadas.

Os modos de ataque são os mais variados possíveis, atingindo a velocidade do tráfico de informações na rede, a memória ou espaço em disco do sistema informático ou sua estruturação de dados.

O parecer do Senador Crivella também estabelece a obrigação de todos os provedores de internet armazenarem os registros de movimentação de seus usuários,

pelo prazo de 03 anos[211]. Trata-se de medida inadiável e indispensável para possibilitar a investigação de delitos cometidos na rede mundial. Sem esses registros de conexão e navegação é impossível qualquer investigação criminal de delitos informáticos. O projeto, nesse sentido, segue uma tendência global, pois praticamente todos os países desenvolvidos já incluíram esse tipo de obrigação legal em seus sistemas jurídicos, sobretudo depois que o combate ao terrorismo se tornou assunto de política geral. Essa providência, aliás, já deveria ter sido implementada por via infralegal, através de alguma agência reguladora, a exemplo da Anatel[212]. O Comitê Gestor da Internet (CGI) no Brasil apenas recomenda aos provedores nacionais, dada a ausência de lei nesse sentido, que guardem por até três anos os registros de conexão dos usuários[213].

O parecer ainda faz outros ajustes ao projeto original, como, por exemplo, a eliminação da figura do art. 218-A (pornografia infantil), cuja inclusão não é mais necessária, uma vez que a Lei a Lei 10.764, de 12 de novembro de 2003, já criou esse tipo de delito (por meio do aperfeiçoamento da redação do art. 241 do Estatuto da Criança e do Adolescente, que agora já pune a difusão desse tipo de material ilícito na internet). Além disso, aperfeiçoa a redação do art. 298-A (crime de falsificação de telefone celular ou meio de acesso a sistema informático), de que trata o projeto de lei da Câmara[214], e acrescenta um parágrafo único ao art. 46 do Código Penal, de modo a

---

[211] O parecer traz emenda que acrescenta um parágrafo único ao art. 11 do projeto da Câmara (PLC 89/03).

[212] Essa é a opinião de REINALDO FILHO, Demócrito. *O projeto de lei sobre crimes tecnológicos (PL nº. 84/99). Notas ao parecer do Senador Marcello Crivella*. Disponível em: http://jus2.uol.com.br/doutrina/texto.asp?id=5447>. Acesso em: 20 julho de 2008, às 17h51min.

[213] Tal recomendação está prevista no item 3.2 ("Manutenção de Dados de Conexão") do documento "Recomendações para o Desenvolvimento e Operação da Internet no Brasil", criado pelo Comitê Gestor.

[214] O art. 298-A, proposto pelo projeto, cria o crime de falsificação de telefone celular ou meio de acesso a sistema informático. O parecer sugere emenda para deixá-lo com a seguinte redação: "Art. 298-A. Criar, copiar, interceptar, usar, indevidamente ou sem autorização, ou falsificar senha, código, seqüência alfanumérica, cartão inteligente, transmissor ou receptor de radiofreqüência ou telefonia celular ou qualquer instrumento que permita o acesso a meio eletrônico ou sistema informatizado. Pena: reclusão, de um a cinco anos, e multa". A redação anterior não era clara sobre a conduta bastante comum de "quebra de senhas", o que demandava um aperfeiçoamento do art. 298-A, agora incluída pelo parecer do Senador Marcelo Crivella.

possibilitar a aplicação de penas restritivas de direito a *hackers*, aproveitando seus conhecimentos técnicos em cursos de instituições públicas ou outras atividades equivalentes[215].

De um modo geral, o parecer promove alterações importantes ao projeto originário da Câmara. É claro que o combate aos *cybercrimes* não se resolverá na sua aprovação.

Independente disso, a definição legal das práticas criminosas é realmente o primeiro passo na luta contra o problema..

Para Demócrito Reinaldo Filho[216], o que não pode ser feito é retardar ainda mais a aprovação do projeto e, a cada passo, ficar acrescentado novas figuras à sua redação original. Ainda, segundo o autor, é melhor uma lei que não preveja todos os delitos de possível ocorrência no ciberespaço do que nenhuma.

Entretanto, contrariando as idéias do mencionado autor, o Plenário do Senado aprovou recentemente[217] a proposta substitutiva a esse último projeto, que conceitua juridicamente crimes cometidos no universo da informática, seja em redes privadas ou na internet. Segundo o senador Aloizio Mercadante, com a proposta, o Brasil "busca incluir-se entre as modernas nações onde legislação específica trata de delitos cibernéticos, que incluem, entre outros, a pedofilia, o estelionato eletrônico e a difusão de vírus".[218] Mercadante[219] explica que a tipificação do crime, ou sua

---

[215] A emenda proposta tem a seguinte redação: "Dê-se ao art. 5º. do Projeto de Lei da Câmara n. 89, de 2003, a seguinte redação: Art. 5º. O art. 46 do Decreto-Lei n. 2.848, de 7 de dezembro de 1940 – Código Penal, passa a vigorar acrescido do seguinte parágrafo: "No crime praticado contra ou por meio de meio eletrônico ou sistema informatizado, o juiz poderá aproveitar as habilidades e conhecimentos do condenado para a ministração de cursos ou trabalhos de criação de sistemas informatizados em empresas ou instituições públicas, ou para qualquer tipo de prestação de serviços equivalentes" (NR)"

[216] REINALDO FILHO, Demócrito. *O projeto de lei sobre crimes tecnológicos (PL nº. 84/99). Notas ao parecer do Senador Marcello Crivella*. Disponível em: http://jus2.uol.com.br/doutrina/texto.asp?id=5447>. Acesso em: 20 julho de 2008, às 18h00min.

[217] Proposta aprovada no dia nove de julho de 2008.

[218] Disponível em: http://www2.camara.gov.br/conheca/altosestudos/noticia/entenda-o-projeto-de-lei-dos-crimes-cometidos-por/noticiasView. Acesso em: 18/07/2008, às 21h23min.

[219] O Senador foi o relator da matéria na Comissão de Assuntos Econômicos (CAE). Ali seu parecer foi aprovado com 23 subemendas ao substitutivo. Na mesma data da aprovação da proposta substitutiva

conceituação jurídica, facilita a punição de culpados, já que o Código Penal brasileiro acolhe o princípio universal de que "não há crime sem lei anterior que o defina. Não há pena sem prévia cominação legal".[220]

Para alguns operadores do Direito, o projeto de lei substitutivo sobre crimes eletrônicos é um grande avanço na definição de regras para o ambiente virtual, necessitando, entretanto, de alguns ajustes.[221]

Segundo a jurista Patrícia Peck[222], o principal defeito do substitutivo está no modo como foi estabelecida a criminalização de divulgação de vírus e demais arquivos danosos. O projeto prevê que o crime só será caracterizado quando for comprovada a intenção de repassar os dados infectados. Patrícia acredita que muitos criminosos podem alegar que não pretendiam cometer o ilícito para se livrarem de punições. Entretanto, tornar crime o repasse de vírus independentemente da intenção também geraria incoerências.[223]

Por outro lado, apesar das ressalvas, o texto do projeto recebeu elogios dos operadores do Direito, ressaltando a necessidade de normas específicas para a internet.

Embora alguns senadores defendam a tese de que o projeto de lei não embute ameaças à liberdade de informação e à democratização da rede e que trata apenas de "tipificar" os crimes, a Associação Brasileira dos Provedores de Internet

---

pelo Plenário do Senado, o parlamentar apresentou dez novas emendas, que atendem às sugestões de diversos setores da sociedade civil.

[220] Disponível em: http://www2.camara.gov.br/conheca/altosestudos/noticia/entenda-o-projeto-de-lei-dos-crimes-cometidos-por/noticiasView. Acesso em: 18/07/2008, às 21h23min.

[221] É o que afirmam os advogados Rony Vainzof, sócio do escritório Opice Blum Advogados, e Patrícia Peck, do PPP Advogados, especialistas em crimes cometidos pela internet. *In*: GAZETA MERCANTIL – DIREITO CORPORATIVO. Clipping Eletrônico da Associação dos Advogados de São Paulo, edição de 12 de junho de 2008.

[222] GAZETA MERCANTIL – DIREITO CORPORATIVO. Clipping Eletrônico da Associação dos Advogados de São Paulo, edição de 12 de junho de 2008.

[223] A autora destaca ainda que "algumas pessoas recebem esses programas em mensagens aparentemente inofensivas e enviam a seus contatos sem saber que estão espalhando um vírus". Segundo ela, "seria necessário um debate mais profundo para que se resolvesse esse impasse, garantindo que a lei não vai punir os inocentes e nem liberar a ação dos criminosos." *In*: GAZETA MERCANTIL – DIREITO CORPORATIVO. Clipping Eletrônico da Associação dos Advogados de São Paulo, edição de 12 de junho de 2008.

(Abranet) afirma que o Projeto de Lei exagera nas exigências e "cria regras que não fazem o menor sentido".[224]

Eduardo Parajo, presidente da Abranet, chega a dizer que, caso as condições impostas no projeto entrem de fato em vigor, pequenos provedores do país correm o risco de fechar as portas. Segundo do presidente da associação "o que se propõe hoje é um exagero" e que "não adianta aprovarmos uma lei que dá doses de elefante para formigas."[225]

Uma das queixas dos provedores diz respeito à exigência de guardar, pelo prazo de três anos, os chamados "logs de acesso", a identificação do instante em que o usuário entra ou sai da rede. Segundo a Abranet, a maior parte dos provedores já guarda esses dados por 90 dias.[226] Vale lembrar que o Projeto de Lei não define como os logs devem ser armazenados.

No ano passado, a Abranet chegou a elaborar um estudo em que concluía que a mudança teria um impacto de pelo menos R$ 15 milhões por ano no bolso dos provedores, um setor que hoje reúne mais de 1,7 mil empresas no país. Atualmente, cerca de 85% dos 40 milhões dos internautas do país têm seus acessos vinculados aos 10 maiores provedores da rede, empresas como Universo Online (UOL), Terra e iG. Os demais 15% estão pulverizados em uma nuvem de pequenos provedores que, na maioria das vezes, oferecem outros serviços para aumentar a receita.

Segundo o Senador Eduardo Azeredo, a queixa de aumento de custo não tem fundamento, pois o armazenamento pode ser feito até em um disquete. Destaca ainda que a aprovação do projeto permitirá ao Brasil aderir aos tratados internacionais

---

[224] VALOR ECONÔMICO – EMPRESAS: *Provedores criticam projeto que pretende coibir crimes na web*. Clipping Eletrônico da Associação dos Advogados de São Paulo, edição de 28 de julho de 2008.

[225] VALOR ECONÔMICO – EMPRESAS: *Provedores criticam projeto que pretende coibir crimes na web*. Clipping Eletrônico da Associação dos Advogados de São Paulo, edição de 28 de julho de 2008.

[226] Alega a entidade que a extensão do prazo exigiria que muitas empresas comprassem novos equipamentos e sistemas de segurança.

de cooperação para combate e punição de crimes de informática. O senador procurou harmonizar o que ele chama de futura lei de crimes cibernéticos com a Convenção sobre o Cybercrime do Conselho da Europa, assinada pelos países da Comunidade Européia, além dos Estados Unidos, Coréia do Sul, Japão, Canadá e África do Sul.[227]

De outra banda, Júlio Semeghini, deputado federal que apóia a tramitação do projeto na Câmara, diz que os pequenos provedores sempre tiveram o controle desses dados para fazer a cobrança do serviço.

Outro tema que ainda deve render muita discussão diz respeito a quem passará a ser obrigado a guardar os tais logs de acesso. Gil Torquato, diretor corporativo do UOL, afirma que o texto, da forma como foi redigido, abre espaço para a interpretação de que qualquer empresa que tenha computadores em rede terá que armazenar as informações. Segundo ele, "pelo que está definido, até o dono de uma padaria também terá que guardar seus logs, o que é, no mínimo, um absurdo."[228] O Projeto de Lei não informa, porém, como será feita a distinção entre as empresas que se encaixam e as que não se encaixam nessa regra.

Além de possíveis impactos econômicos, a Abranet reclama que o Projeto de Lei induz os provedores a assumir o papel de investigadores. Atualmente, os provedores de São Paulo mantêm um acordo com o Ministério Público para repassar denúncias de supostos crimes de pedofilia e racismo.

Azeredo, no entanto, afirma que os provedores não terão que verificar se o conteúdo da denúncia é ou não pertinente. "Não estamos pedindo que investiguem, apenas que nos transmitam essas informações."[229]

---

[227] VALOR ECONÔMICO – POLÍTICA: *Lei que pune crimes cibernéticos passa na CCJ*. Clipping Eletrônico da Associação dos Advogados de São Paulo, edição de 19 de junho de 2008.
[228] VALOR ECONÔMICO – EMPRESAS: *Provedores criticam projeto que pretende coibir crimes na web*. Clipping Eletrônico da Associação dos Advogados de São Paulo, edição de 28 de julho de 2008.
[229] VALOR ECONÔMICO – EMPRESAS: *Provedores criticam projeto que pretende coibir crimes na web*. Clipping Eletrônico da Associação dos Advogados de São Paulo, edição de 28 de julho de 2008.

Ao passar pela Câmara dos Deputados, o Projeto de Lei não poderá mais ser alterado. A única possibilidade será excluir partes do texto. Para Pedro Paranaguá, professor da escola de Direito da Fundação Getulio Vargas (FGV-Rio), entidade que participou da reformulação do projeto, a versão final do Projeto de Lei não obteve o resultado esperado. Segundo o professor, "o texto ficou melhor, mas alguns artigos estão vagos e podem dar margem a interpretações variadas."[230]

A referida proposta altera o Código Penal, o Código Penal Militar, a Lei dos Crimes Raciais (Lei nº. 7.716 de 1989) e o Estatuto da Criança e do Adolescente (Lei nº. 8.069, de 1990).

A seguir, destacamos e comentamos os principais pontos da proposta, que ainda terá que ser votada na Câmara dos Deputados:

1) *Acesso não autorizado a rede de computadores, dispositivo de comunicação ou sistema informatizado*: Art. 285-A (Código Penal). Acessar, mediante violação de segurança, rede de computadores, dispositivo de comunicação ou sistema informatizado, protegidos por expressa restrição de acesso: Pena - reclusão, de 1 (um) a 3 (três) anos, e multa. Parágrafo único - Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime, a pena é aumentada de sexta parte.

Nessa primeira hipótese, comete o crime quem acessa uma rede de computadores (que não é apenas a internet, pode ser uma rede de computadores conectados entre si, como uma rede coorporativa ou de governo) violando alguma medida de segurança, em rede ou sistema informatizado ou dispositivo de comunicação que contenha expressa restrição de acesso.

[230] VALOR ECONÔMICO – EMPRESAS: *Provedores criticam projeto que pretende coibir crimes na web*. Clipping Eletrônico da Associação dos Advogados de São Paulo, edição de 28 de julho de 2008.

Em um primeiro plano, havia dúvida se cometeria esse crime a pessoa que acessa uma página na internet, ou liga um aparelho eletrônico de outra pessoa. Temos que afirmar com clareza que não. O crime só acontece quando aquele que acessa viola alguma medida de segurança colocada para proteger as informações na rede de computadores, no dispositivo de comunicação ou no sistema informatizado que seja expressamente restrito. Por exemplo, um computador que pede uma senha tem uma restrição expressa de acesso, se essa senha for violada, ocorre o crime.

Importante lembrar que o objetivo desse novo tipo penal é proteger informações pessoais ou empresariais importantes de serem conhecidas indevidamente.

2) *Obtenção, transferência ou fornecimento não autorizado de dado ou informação*: Art. 285-B (Código Penal). Obter ou transferir, sem autorização ou em desconformidade com autorização do legítimo titular da rede de computadores, dispositivo de comunicação ou sistema informatizado, protegidos por expressa restrição de acesso, dado ou informação neles disponível: Pena - reclusão, de 1 (um) a 3 (três) anos, e multa. Parágrafo único - Se o dado ou informação obtida desautorizadamente é fornecida a terceiros, a pena é aumentada de um terço.

Esse dispositivo também busca proteger os dados eletrônicos (por exemplo, fotos pessoais, um trabalho acadêmico ou artístico, etc.) de ser obtido ou transferido sem autorização para terceiros.

Diferentemente do dispositivo anterior, esse crime acontece quando ocorre a transferência ou obtenção do dado eletrônico sem a autorização do titular da rede de computadores, ou do dispositivo de comunicação ou sistema informatizado. Notem bem, não se fala em autorização do titular (ou dono) do dado, mas sim da rede onde ele se encontra.

A redação deixa claro que o crime não é cometido quando duas ou mais pessoas trocam dados (sejam eles quais forem, como filmes, músicas mp3, jogos, etc), pois, nesse caso, os titulares (ou donos) das redes que estão trocando as informações estão de acordo.

Inicialmente houve dúvida se o crime seria cometido por quem troca arquivos "piratas" (protegidos por direito autoral), mas a redação é explícita em dizer que não. Se os dados trocados violam direito autoral de outras pessoas, isso é assunto não tratado por essa lei.

Além desse fator, vale destacar que o Art. 285-C[231] do projeto determina que os dois crimes acima só se procedem se houver representação da pessoa ofendida, isso quer dizer que a polícia ou o Ministério Público não podem processar por conta própria.

3) *Divulgação ou utilização indevida de informações e dados pessoais*: Art.154-A (Código Penal). Divulgar, utilizar, comercializar ou disponibilizar dados e informações pessoais contidas em sistema informatizado com finalidade distinta da que motivou seu registro, salvo nos casos previstos em lei ou mediante expressa anuência da pessoa a que se referem, ou de seu representante legal. Pena - detenção, de 1 (um) a 2 (dois) anos, e multa. Parágrafo único - Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime, a pena é aumentada da sexta parte.

Esse crime busca punir conduta que se tornou muito comum nos dias atuais, que é a divulgação de fotos e informações pessoais, como, por exemplo, dados da receita federal, comercializados por camelôs.

[231] Art. 285-C (Código Penal). Nos crimes definidos neste Capítulo somente se procede mediante representação, salvo se o crime é cometido contra a União, Estado, Município, empresa concessionária de serviços públicos, agências, fundações, autarquias, empresas públicas ou sociedade de economia mista e subsidiárias.

Comete o crime quem divulga as fotos ou dados sem a permissão dos donos (ou representantes legais dos donos) das fotos ou dados.

4) *Dano*: Art. 163 (Código Penal). Destruir, inutilizar ou deteriorar coisa alheia ou dado eletrônico alheio.

Esse artigo já existe no Código Penal, apenas foi acrescentado o "dado eletrônico" para protegê-lo de dano.

5) *Inserção ou difusão de código malicioso*: Art. 163-A (Código Penal). Inserir ou difundir código malicioso em dispositivo de comunicação, rede de computadores, ou sistema informatizado. Pena - reclusão, de 1 (um) a 3 (três) anos, e multa.

Pratica essa conduta quem difunde vírus ou o insere em rede de computadores. Note-se que esse crime, tal como os demais, não existe em modalidade culposa, apenas dolosa, o que quer dizer que aquele que recebe o vírus e sem perceber passa a distribuí-los, não comete crime (não existe dolo na conduta).

Parágrafo 1º - Se do crime resulta destruição, inutilização, deterioração, alteração, dificultação do funcionamento, ou funcionamento desautorizado pelo legítimo titular, de dispositivo de comunicação, de rede de computadores, ou de sistema informatizado: Pena - reclusão, de 2(dois) a 4 (quatro) anos, e multa.

Parágrafo 2º - Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime, a pena é aumentada de sexta parte.

Trata-se de um agravante caso o crime de difusão de vírus seja seguido da destruição do sistema afetado.

6) *Estelionato Eletrônico*: VII - difunde, por qualquer meio, código malicioso com intuito de facilitar ou permitir acesso indevido à rede de computadores, dispositivo de comunicação ou sistema informatizado: Parágrafo 3º - Se o agente se vale

de nome falso ou da utilização de identidade de terceiros para a prática do crime do inciso VII do § 2º deste artigo, a pena é aumentada de sexta parte.

Criou-se uma modalidade a mais de estelionato (que já existe no Código Penal). Note-se que esse crime é diferente do anterior, de difusão de vírus. Nesse caso, a difusão do código malicioso tem a intenção (ou dolo) de obter vantagem ilícita.

7) *Atentado contra a segurança de serviço de utilidade pública*: Art. 265 (Código Penal). Atentar contra a segurança ou o funcionamento de serviço de água, luz, força, calor, informação ou telecomunicação, ou qualquer outro de utilidade pública.

Comete esse crime quem ataca os sistemas de funcionamento de serviços públicos essenciais, causando prejuízo à população

8) *Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático, dispositivo de comunicação, rede de computadores ou sistema informatizado*: Art. 266 (Código Penal). Interromper ou perturbar serviço telegráfico, radiotelegráfico, telefônico, telemático, informático, de dispositivo de comunicação, de rede de computadores, de sistema informatizado ou de telecomunicação, assim como impedir ou dificultar-lhe o restabelecimento.

Semelhante ao anterior, mas não igual, esse crime é cometido por quem busca dolosamente interromper serviço telegráfico, radiotelegráfico, telefônico, telemático, informático, de dispositivo de comunicação. Muitas vezes a conduta é feita inconseqüentemente, como uma brincadeira de adolescente, mas provoca seriíssimos danos à sociedade.

9) *Falsificação de dado eletrônico ou documento público*: Art. 297 (Código Penal). Falsificar, no todo ou em parte, dado eletrônico ou documento público, ou alterar documento publico verdadeiro.

Esse crime já existe no Código Penal, mas acrescentou-se "dado eletrônico" para preservá-lo de falsificação.

10) *Falsificação de dado eletrônico ou documento particular*: Art. 298 (Código Penal). Falsificar, no todo ou em parte, dado eletrônico ou documento particular ou alterar documento particular verdadeiro.

Semelhante ao anterior, mas tratando de documento ou dado eletrônico particular.

11) Código Penal Militar - os seguintes crimes foram acrescentados ao Código Penal Militar, tal como acima comentado quanto ao Código Penal:

a) *Estelionato Eletrônico*: VI - Difunde, por qualquer meio, código malicioso com o intuito de facilitar ou permitir o acesso indevido a rede de computadores, dispositivo de comunicação ou a sistema informatizado, em prejuízo da administração militar. Parágrafo 4º - Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime, a pena é aumentada da sexta parte;

b) *Dano Simples*: Art. 259 (Código Penal Militar). Destruir, inutilizar, deteriorar ou fazer desaparecer coisa alheia ou dado eletrônico alheio, desde que este esteja sob administração militar;

c) *Dano em material ou aparelhamento de guerra ou dado eletrônico*: Art. 262 (Código Penal Militar). Praticar dano em material ou aparelhamento de guerra ou dado eletrônico de utilidade militar, ainda que em construção ou fabricação, ou em efeitos recolhidos a depósito, pertencentes ou não às forças armadas;

d) *Inserção ou difusão de código malicioso*: Art. 262-A (Código Penal Militar). Inserir ou difundir código malicioso em dispositivo de comunicação, rede de computadores, ou sistema informatizado, desde que o fato atente contra a administração militar: Pena - reclusão, de 1 (um) a 3 (três) anos, e multa;

e) *Inserção ou difusão código malicioso seguido de dano*: Parágrafo 1º - Se do crime resulta destruição, inutilização, deterioração, alteração, dificultação do funcionamento, ou funcionamento não autorizado pelo titular, de dispositivo de comunicação, de rede de computadores, ou de sistema informatizado: Pena - reclusão, de 2 (dois) a 4 (quatro) anos, e multa. Parágrafo 2º Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime, a pena é aumentada da sexta parte;

f) *Acesso não autorizado a rede de computadores, dispositivo de comunicação ou sistema informatizado*: Art. 339-A (Código Penal Militar). Acessar, mediante violação de segurança, rede de computadores, dispositivo de comunicação ou sistema informatizado, protegidos por expressa restrição de acesso, desde que o fato atente contra a administração militar: Pena - reclusão, de 1 (um) a 3 (três) anos, e multa. Parágrafo único - Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime, a pena é aumentada de sexta parte;

g) *Obtenção, transferência ou fornecimento não autorizado de dado ou informação*: Art. 339-B (Código Penal Militar). Obter ou transferir, sem autorização ou em desconformidade com autorização do legítimo titular da rede de computadores, dispositivo de comunicação ou sistema informatizado, protegidos por expressa restrição de acesso, dado ou informação neles disponível, desde que o fato atente contra a administração militar: Pena - reclusão, de 1 (um) a 3 (três) anos, e multa. Parágrafo único - Se o dado ou informação obtida desautorizadamente é fornecida a terceiros, a pena é aumentada de um terço;

h) *Divulgação ou utilização indevida de informações e dados pessoais*: Art. 339-C (Código Penal Militar). Divulgar, utilizar, comercializar ou disponibilizar dados e informações pessoais contidas em sistema informatizado sob administração militar com finalidade distinta da que motivou seu registro, salvo nos casos previstos em lei ou

mediante expressa anuência da pessoa a que se referem, ou de seu representante legal: Pena - detenção, de um a dois anos, e multa. Parágrafo único - Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática de crime, a pena é aumentada da sexta parte;

i) *Falsificação de documento*: Art. 311 (Código Penal Militar). Falsificar, no todo ou em parte, documento público ou particular, ou dado eletrônico ou alterar documento verdadeiro, desde que o fato atente contra a administração ou o serviço militar;

j) *Da traição*: Favor ao inimigo. Art. 356 (Código Penal Militar). "(...) II - entregando ao inimigo ou expondo a perigo dessa conseqüência navio, aeronave, força ou posição, engenho de guerra motomecanizado, provisões, dado eletrônico ou qualquer outro elemento de ação militar;

III - perdendo, destruindo, inutilizando, deteriorando ou expondo a perigo de perda, destruição, inutilização ou deterioração, navio, aeronave, engenho de guerra motomecanizado, provisões, dado eletrônico ou qualquer outro elemento de ação militar". O crime de traição é exclusivamente militar.

12) Definições. O projeto cria um glossário, com as seguintes definições, que auxiliam na sua interpretação:

a) *dispositivo de comunicação*: qualquer meio capaz de processar, armazenar, capturar ou transmitir dados utilizando-se de tecnologias magnéticas, óticas ou qualquer outra tecnologia;

b) *sistema informatizado*: qualquer sistema capaz de processar, capturar, armazenar ou transmitir dados eletrônica ou digitalmente ou de forma equivalente;

c) *rede de computadores*: o conjunto de computadores, dispositivos de comunicação e sistemas informatizados, que obedecem a um conjunto de regras, parâmetros, códigos,

formatos e outras informações agrupadas em protocolos, em nível topológico local, regional, nacional ou mundial através dos quais é possível trocar dados e informações;

d) *código malicioso*: o conjunto de instruções e tabelas de informações ou qualquer outro sistema desenvolvido para executar ações danosas ou obter dados ou informações de forma indevida;

e) *dados informáticos*: qualquer representação de fatos, de informações ou de conceitos sob forma suscetível de processamento numa rede de computadores ou dispositivo de comunicação ou sistema informatizado;

f) *dados de tráfego*: todos os dados informáticos relacionados com sua comunicação efetuada por meio de uma rede de computadores, sistema informatizado ou dispositivo de comunicação, gerados por eles como elemento de uma cadeia de comunicação, indicando origem da comunicação, o destino, o trajeto, a hora, a data, o tamanho, a duração ou o tipo do serviço subjacente.

13) *Permissão para cessar transmissão em caso de crime racial*: Art. 20 (Lei nº 7.716/1989). II - a cessação das respectivas transmissões radiofônicas, televisivas, eletrônicas, ou da publicação por qualquer meio.

Altera-se um inciso da lei de crimes raciais para permitir a determinação por parte do juiz de cessação de transmissão eletrônica ou publicação por qualquer meio (as demais já existiam).

14) *Alteração no crime de pedofilia*: Art. 241 (Estatuto da Criança e do Adolescente). Apresentar, produzir, vender, receptar, fornecer, divulgar, publicar ou armazenar consigo, por qualquer meio de comunicação, inclusive rede mundial de computadores ou internet, fotografias, imagens com pornografia ou cenas de sexo explícito envolvendo criança ou adolescente.

Apenas acrescentam-se dois novos verbos, para permitir a punição pelo crime de pedofilia em muitos casos hoje não previstos.

15) *Responsabilidade dos Provedores*:

I- manter em ambiente controlado e de segurança, pelo prazo de três anos, com o objetivo de provimento de investigação pública formalizada, os dados de endereçamento eletrônico da origem, hora, data e a referência GMT da conexão efetuada por meio de rede de computadores e fornecê-los exclusivamente à autoridade investigatória mediante prévia requisição judicial;

II- preservar imediatamente, após requisição judicial, outras informações requisitadas em curso de investigação, respondendo civil e penalmente pela sua absoluta confidencialidade e inviolabilidade;

III- informar, de maneira sigilosa, à autoridade competente, denúncia que tenha recebido e que contenha indícios da prática de crime sujeito a acionamento penal público incondicionado, cuja perpetração haja ocorrido no âmbito da rede de computadores sob sua responsabilidade.

Parágrafo 1º - Os dados de que cuida o inciso I deste artigo, as condições de segurança de sua guarda, a auditoria à qual serão submetidos e a autoridade competente responsável pela auditoria, serão definidos nos termos de regulamento.

Parágrafo 2º - O responsável citado no *caput* deste artigo, independentemente do ressarcimento por perdas e danos ao lesado, estará sujeito ao pagamento de multa variável de R$ 2.000,00 (dois mil reais) a R$ 100.000,00 (cem mil reais) a cada requisição, aplicada em dobro em caso de reincidência, que será imposta pela autoridade judicial desatendida, considerando-se a natureza, a gravidade e o prejuízo resultante da infração, assegurada a oportunidade de ampla defesa e contraditório.

Parágrafo 3º - Os recursos financeiros resultantes do recolhimento das multas estabelecidas neste artigo serão destinados ao Fundo Nacional de Segurança Pública, de que trata a Lei nº 10.201, de 14 de fevereiro de 2001.

O projeto estabelece ainda quais são as obrigações dos provedores de acesso:

a) Guardar por três anos os chamados "logs de acesso" que nada mais são do que a identificação da hora de conexão e desconexão à internet. Frise-se que não há qualquer armazenamento obrigatório de informações privadas, como os sites navegados ou qualquer outra.

b) Em caso de requisição judicial, aí sim podem ser armazenadas outras informações, mas apenas com requisição judicial e apenas para os fins daquela investigação.

c) Os provedores, caso recebam um e-mail com denúncia de crime possivelmente cometido no espaço sob sua responsabilidade, devem informar, de maneira sigilosa (para preservar a intimidade das pessoas, que podem não ter cometido crime algum), à autoridade competente. É bom frisar que o papel de polícia, de investigador não é do provedor, ele apenas encaminha a denúncia.

d) Se não armazenar os dados, pode ser multado de R$ 2.000,00 (dois mil reais) a R$ 100.000,00 (cem mil reais) a cada requisição. Os recursos financeiros das multas estabelecidas neste artigo serão destinados ao Fundo Nacional de Segurança Pública.

Pelo exposto, conclui-se que a demora na aprovação dos projetos supracitados, bem como o próprio constante desenvolvimento da tecnologia informática, acabam por destruir os meios de repreensão penal criados, vez que todos os dias surgem novas maneiras de transpor os dispositivos de segurança eletrônica, aumentando ainda mais os crimes e os danos nessa essencial área de conhecimento e de relações humanas e comerciais.

A existência de um vácuo na legislação penal dificulta a luta contra os *cybercrimes*. Parece-nos que o correto, no momento, reside em apressar a votação dos projetos com os crimes já incluídos e analisados nas diversas comissões (tanto na Câmara como no Senado), até porque, nos ambientes das redes de comunicação, novas modalidades de crime surgem a cada dia e é impossível se prever todas elas. A aprovação dos projetos é um primeiro passo e, no futuro, criminalizar outras condutas que forem surgindo.

CONCLUSÕES

1. O fenômeno da globalização refletiu em todas as sociedades pós-industriais, rompendo paradigmas, em especial aqueles inerentes à soberania e à territorialidade;
2. As transformações provocadas pela informática e pela internet na vida do ser humano são evidentes e se solidificam dia a dia, com a interferência em todos os campos sociais: na cultura; na economia; na educação e, por conseguinte, atinge o campo do direito;
3. A comunicação estabelecida pela internet anula os limites de espaço e tempo, fazendo nascer uma sociedade de comunicação global, em que, abatidas, hipoteticamente, as fronteiras das nações, das culturas e ideologias, têm surgido novas relações;
4. A macrocriminalidade surge como uma teia de relacionamentos ilícitos, em âmbito planetário, rompendo limites territoriais dos países envolvidos, ignorando-se quaisquer soberanias ou tratados e convenções internacionais firmados;
5. Com a difusão da tecnologia informática, o Direito Penal deve se preocupar em estabelecer valores penalmente relevantes, criando normas protetoras com o escopo de garantir a segurança dessas relações;
6. Tal proteção não deve ser limitada a bens jurídicos tradicionalmente reconhecidos e lesionados com o uso da tecnologia informática, mas, sim, deve ser estendida a outros bens e valores recentemente surgidos com a criação e proliferação dos computadores;

7. No tocante aos bens jurídicos passíveis de afetação com os delitos informáticos além dos bens jurídicos já tradicionalmente protegidos pelo Direito Penal, tais como a honra, a vida, o patrimônio, a integridade física, a fé pública, a propriedade industrial etc., estão também os objetos informáticos propriamente ditos, como o *hardware*, *software*, dados, documentos eletrônicos etc;
8. Além desse fator, os crimes de computador, no envolver histórico, avançaram de tipos penais que compreendiam a proteção a determinados bens jurídicos individuais, para tipificações penais que englobam a proteção a determinados bens jurídicos supra- individuais; Esses novos bens jurídicos supra-individuais, no que diz respeito à criminalidade informática, são, principalmente, o direito à informação, a proteção da informação e dos dados eletrônicos em si e, ainda, a confiabilidade e segurança dos sistemas de armazenamento, processamento, transferência e transmissão desses dados e dessas informações;
9. Não pode ser vista de forma absoluta, a idéia de que os crimes de computador somente podem ser praticados por pessoas com grandes conhecimentos da linguagem informática, uma vez que com a evolução dos meios de comunicação e o fácil acesso aos equipamentos de informática, qualquer pessoa pode ser sujeito ativo de um crime de computador, bastando, para tanto, que tenha noções mínimas de como manuseá-lo;
10. Muitas vezes o fenômeno da expansão do direito penal entremostrou-se desarrazoado, pois certas criminalizações de condutas não satifizeram os requisitos inerentes ao ramo da dogmática jurídica que sempre foi visto como *ultima ratio*;
11. Se a estrutura normativa vigente se demonstra incapaz de dar resposta aos novos desafios, faz-se necessária a incorporação dos elementos indispensáveis de

informática e cibernética para que nos seja permitido obter a devida segurança jurídica das relações sociais;

12. Porém, a necessidade de incorporação dos conceitos de informática à legislação vigente não significa que devamos esquecer todo o nosso sistema e criar um novo ordenamento jurídico;
13. Uma resposta, ainda que parcial, à criminalidade informática, passa pela elaboração de tipos penais de perigo abstrato ou mediante a utilização de normas penais em branco, inclusive, para que possam incluir as novas variantes ilícitas que surjam com as constantes evoluções tecnológicas, valendo-se do princípio da proporcionalidade, evitando-se desrespeitar o princípio da legalidade, afastando-se, desse modo, constantes e contínuas reformas legislativas;
14. O legislador deve se valer, portanto, de tipos penais de perigo abstrato e normas penais em branco – sob pena de restar o direito penal da atualidade incapaz de proteger os novos bens jurídicos penalmente relevantes;
15. Outra grande dificuldade enfrentada pelo operador jurídico no que tange a criminalidade praticada através da internet, diz respeito à aplicação da lei penal no espaço;
16. A criminalidade informática faz romper paradigmas até então consagrados tal como o conceito de soberania e, por conta da ubiqüidade plena dos delitos cibernéticos, do próprio princípio da territorialidade;
17. Várias são as soluções cogitadas para o problema, mas até o momento nenhuma foi consagrada. É preciso, mais do que nunca, refletir acerca do tema para que de forma urgente, sejam criadas soluções justas e capazes de conciliar a soberania dos países com a inevitável evolução tecnológica;

18. A investigação de crimes de computador é considerada um dos maiores problemas deste tipo de crime, uma vez que tais crimes apresentam grandes dificuldades para sua comprovação, pois a verificação de vestígios exige qualificação técnica específica nem sempre disponível em todos os locais em que os crimes se consumam;
19. Às vezes, os registros magnéticos são transitórios e a menos que se realizam provas dentro de um período curto de tempo, podem ser perdidos detalhes de tudo aquilo que aconteceu, restando somente os efeitos danosos do crime;
20. Em decorrência da necessidade de combate a esses novos e numerosos delitos, e da constatação de que o Direito Penal Clássico, com suas regras e princípios rígidos, não está preparado para tanto, surge como alternativa a teoria do Direito Penal do Inimigo;
21. Inúmeros são os projetos de lei existentes acerca do tema, entretanto, a demora na aprovação desses projetos, bem como o próprio constante desenvolvimento da tecnologia informática, acabam por destruir os meios de repreensão penal criados, vez que todos os dias surgem novas maneiras de transpor os dispositivos de segurança eletrônica, aumentando ainda mais os crimes e os danos nessa essencial área de conhecimento e de relações humanas e comerciais;
22. A cooperação internacional é uma tendência inafastável e inexorável, haja vista a constatação fática do caráter transnacional dos crimes de computador;
23. Há necessidade de produção legislativa homogênea, no âmbito do Estados nacionais, bem como a elaboração e vinculação de número máximo de países a tratados e convenções internacionais relacionados à matéria.