FACULDADE BAIANA DE DIREITO
CURSO DE GRADUAÇÃO EM DIREITO

PALOMA PADILHA

CRIMES DIGITAIS E SUA TIPICIDADE NO DIREITO PENAL

Salvador
2012

PALOMA PADILHA

CRIMES DIGITAIS E SUA TIPICIDADE NO DIREITO PENAL

Monografia apresentada ao curso de graduação em Direito, Faculdade Baiana de Direito, como requisito parcial para obtenção do grau de bacharel em Direito.

Orientador: Prof. Dr. Sebastian Mello de Albuquerque

Salvador
2012

TERMO DE APROVAÇÃO

PALOMA PADILHA

OS CRIMES DIGITAIS E SUA TIPICIDADE NO DIREITO PENAL

Monografia aprovada como requisito parcial para obtenção do grau de bacharel em Direito, Faculdade Baiana de Direito, pela seguinte banca examinadora:

Nome:_____

Titulação e instituição:_____

Nome:_____

Titulação e instituição: _____

Nome:_____

Titulação e instituição:_____

Salvador, ____/_____/ 2012

A
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxx.

AGRADECIMENTOS

A Dr. xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx.

A Dra. Xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx.

A Fulano, Fulana, etc.

“xxxxxxxxxx xxxxxx xxxxxxxxxxx xxx xxxxxxxxxxxxxxxxxxxx xxx xxxxxxxxxxx xxxx xxxxx xxxxxxxxxxxxx xxx xxx xxxxx xx xxx xxxxxxxxxx”.

Nome do autor

RESUMO

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xx

ABSTRACT

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx. (250 a 500 palavras)

Keywords: xxxxxxxxxxxxxx; xxxx xxxxxxx; xxxxxxxxxxxxx; xxxxx xxx xxxxxxx. (4 a 6 palavras e/ou expressões)

LISTA DE ABREVIATURAS E SIGLAS

art.	artigo
CC	Código Civil
CF/88	Constituição Federal da República
CPC	Código de Processo Civil
CPP	Código de Processo Penal
des.	desembargador
HC	*Habeas Corpus*
MP	Ministério Público
ONU	Organização das Nações Unidas
STF	Supremo Tribunal Federal
STJ	Superior Tribunal de Justiça
TJ	Tribunal de Justiça da Bahia

LISTA DE FIGURAS, GRÁFICOS E TABELAS

SUMÁRIO

Espaços entre as seções dos capítulos: 1,5
Espaços entre seções de capítulos distintos: duplo ou 12 pts (em caso de título com 2 linhas).

SUMÁRIO

1 INTRODUÇÃO

O presente trabalho procura, inicialmente, destacar que a globalização e a evolução tecnológica têm se expandido tanto nos últimos anos, que vem provocando revoluções na vida nos seres humanos, de uma forma positiva, mas também trazem consigo uma infinidade de delitos que podem ser praticados com o uso da tecnologia informática. Assim, o objetivo que se pretende alcançar nas seguintes páginas, é demonstrar que falta de uma legislação específica traz prejuízos à sociedade, pois favorece a ocorrência de condutas ilícitas praticadas por meios de computadores.

Como material específico utilizado para enfrentar o tema, estará o recente Projeto de Lei 35/2012, que dispõe sobre a tipificação criminal de delitos informáticos, alterando o Decreto- Lei no 2.848, de 7 de dezembro de 1940 - Código Penal.

Trata-se de um tema extremamente polêmico, e que requer regulação breve, diante do anacronismo da legislação atual ao deparar-se com avanços tecnológicos que impactam diretamente no âmbito social, e, principalmente, da insegurança sofrida pela sociedade que está sujeita à prática dos crimes digitais ainda não regulados.

Além disso, a legislação penal existente também mostra-se insuficiente para punir o uso indiscriminado dessa tecnologia informática, que produz novas condutas ilícitas. Neste sentido, pode-se afirmar que há uma infinidade de crimes que podem ser praticados com o uso de sistemas informáticos e da internet, como o furto, a pedofilia, ameaça, crimes contra a honra, e muitos outros.

A escolha do tema e o tratamento dado à questão possibilitam relevante contribuição sócio-jurídica, na medida em que versam, no âmbito do Direito Penal, sobre a adequação do ordenamento jurídico à era digital, revelando a necessidade de análise da legislação penal frente ao novo delito.

O fato é que assiste-se um aumento espantoso da delinquência informática, o que demanda um novo ordenamento jurídico ou uma alteração na legislação penal existente. A era digital traz novos desafios para os legisladores, razão pela qual o Direito deve se adequar, trazendo segurança jurídica e a paz para a sociedade.

O trabalho foi desenvolvido em 8 capítulos, e buscou responder à problemática da tipicidade dos crimes praticados por meios digitais, e demonstrar como o ordenamento jurídico de outros países lida com estas questões.

Na tentativa de cumprir o fim ora proposto, em primeiro lugar busca-se demonstrar o delineamento da era digital, desde a formação da internet, da sociedade digital até o advento da criminalidade informatizada.

Em seguida, para tentar chegar a uma definição de um crime digital, faz-se necessário definir os bens jurídicos, e a partir dai, trazer novos bens jurídicos informáticos, como também fazer a classificação dos crimes digitais e analisar os sujeitos ativos e passivos dos delitos informáticos.

Para tanto, busca-se trazer à tona o princípio da legalidade, no intuito de embasar as reflexões acerca da temática que se pretende enfrentar, qual seja: a questão da tipicidade dos crimes digitais.

A partir daí, torna-se inevitável abordar os crimes digitais e sua tipicidade ou atipicidade diante das condutas, face à Legislação Penal Brasileira existente, ignorando as transformações que a sociedade atravessa, por imposição do mundo globalizado e da revolução tecnológica.

É impossível deixar de procurar respostas a respeito de como o Direito irá promover a necessária segurança jurídica com a estrutura normativa vigente, incapaz de dar resposta às novas condutas danosas que surgem a todo momento. Neste sentido, a alteração da estrutura normativa vigente ou criação de nova legislação penal torna-se necessária.

Ainda no terceiro capítulo, busca-se trazer a lume algumas considerações quanto ao momento consumativo e a legislação penal pátria, demonstrando a dificuldade de determinação do momento do crime digital, dadas as suas características, levando o Direito Penal, muitas vezes, a ser incapaz de solucionar os novos conflitos. Junto a este traz-se a questão do tempo e o lugar nos crimes digitais.

No quarto capítulo faz-se um análise da responsabilidade penal dos provedores de acesso à internet em face dos crimes praticados por seus usuários de internet e trata da culpabilidade da vítima e das particularidades no campo do direito penal

infomático, demonstrando, algumas vezes, a dificuldade em identificar e punir o infrator.

O quinto capítulo analisa os crimes digitais e as legislações estrangeiras, demonstrando avanço ou atraso em relação a Legislação Brasileira, traçando um panorama do direito internacional onde se aborda a Convenção de Budapeste e o direito comparado.

O sexto capítulo traz alguns dos crimes digitais em espécie, dentre os mais frequentes, a título de exemplificação.

O sétimo capítulo aborda as principais propostas legislativas em trâmite no Congresso Nacional e a tipificação dos crimes digitais.

Por fim, a análise é uma tentativa de determinar a tipicidade dos crimes digitais, e tentar descobrir se estes representam apenas um meio para a prática de condutas já tipificadas no ordenamento jurídico penal, havendo possíveis lesões a bens jurídicos específicos, ou se, tais delitos, em razão do novo *modus operandi* utilizado, e facilitado pelo anonimato que a internet pode proporcionar, representam novos tipos penais ainda não identificados pela lei penal.

2 A ERA DIGITAL

A internet com suas redes virtuais proporciona hoje, uma imensurável quantidade de informações, algo que é fascinante e surpreendente. Também traz muitas facilidades de comunicação, como por exemplo, o e-mail, que funciona como uma correspondência digital, praticamente atuando em tempo real, assim como o conforto que proporciona toda essa evolução tecnológica, sem que seja preciso sair de casa para pagar uma conta no banco, para fazer uma compra do outro lado do país, e receber a mercadoria confortavelmente em casa, pelo correio.

Trata-se mesmo de uma profunda mudança cultural alavancada pelos apelos do consumismo apregoado principalmente pelas regras do mundo capitalista e que acabam por alcançar patamares variados nas relações sociais, e nesse diapasão vale a pena destacar o dito por Zygmunt Bauman (2003, p. 82):

> O advento da proximidade virtual torna as conexões humanas simultaneamente mais freqüentes e mais banais, mais intensas e mais breves. As conexões tendem a ser demasiadamente breves e banais para poderem condensar-se em laços. Centradas no negócio à mão, estão protegidas da possibilidade de extrapolar e engajar parceiros além do tempo e do tópico da mensagem digitada e lida – ao contrário daquilo que os relacionamentos humanos, notoriamente difusos e vorazes, são conhecidos por perpetrar. Os contatos exigem menos tempo e esforço para serem estabelecidos, e também para serem rompidos. *A distância não é obstáculo para se entrar em contato – mas entrar em contato não é obstáculo para se permanecer à parte.*

Sem dúvidas, essa crescente evolução tecnológica, desenhou um mundo sem fronteiras, e com isso a sociedade se modernizou, evoluiu, tecnologicamente falando, mas criou para si “laços” frágeis e traiçoeiros que, no entanto, não a impedem de firmá-los, seja no âmbito emocional ou empresarial.

O fato é que o mundo virtual seduziu por completo a sociedade moderna, que dele se tornou refém, que através dele alimenta suas idiossincrasias, e vive um novo tipo de solidão que se faz acompanhar por milhares de outras pessoas.

No entanto, a facilidade da comunicação instantânea, em razão das novidades virtuais, trouxe junto consigo a delinqüência tecnológica, ou seja, a possibilidade de se praticar delitos no meio digital.

A verdade é que a sociedade se organiza em rede como bem descrevem Maria Lúcia de Arruda Aranha e Maria Helena Pires Martins (2005, p.83) e a complexidade

das relações sociais aumenta:

> No entanto, em época alguma se atingiu tal nível de inter-relacionamento que agora nos permite falar em um mercado mundial que determina a produção, a distribuição e o consumo de bens e em uma cultura da "virtualidade real", que liga todos os pontos do globo, modelando comportamentos, como veremos na seqüência.

Todo o estudo feito até os dias de hoje pela doutrina brasileira a respeito do tema, e a resposta penal para estes, têm sido feito dentro de uma perspectiva Clássica do Direito. Ou seja, a visão que se tem sobre a criminalidade digital no Brasil é baseada em uma vinculação das máquinas aos delitos já tipificados no nosso ordenamento jurídico. Portanto, trata-se apenas de uma análise quanto ao bem jurídico já protegido pela lei penal, determinando-se, quase que de plano, a tipicidade e punibilidade, ou ao contrário, a sua atipicidade. (CRESPO, 2011).

Faz-se clara, portanto, a necessidade de uma transformação do mundo jurídico, que enfrenta o desafio de regular um sem número de condutas passíveis de reprovação praticadas através dos meios digitais.

Cristiano Chaves e Nelson Rosenvald (2008, p.1) tratando a respeito da conceituação do Direito o definem:

> Exprime o Direito a idéia de adaptação social. De interação e pacificação das relações do homem consigo próprio e com o meio em que vive. Assim, enfeixa o Direito, enquanto fenômeno integrado na sociedade, um duplo aspecto: o homem adapta-se ao direito, que organiza e disciplina a sua vida em sociedade, enquanto o direito retrata as necessidades humanas dentro da sociedade. Não há, pois, como entender o fenômeno jurídico dissociado.

É nítido que, o "mundo do ser" quando se trata da seara tecnológica, encerra características de mudanças extremamente rápidas, renovações constantes, aspectos técnicos muito próprios da área de informática, que acabam por dificultar que o "mundo do dever-ser", o mundo jurídico, as compreenda normativamente.

Essa nova era, a era tecnológica, a era digital, na qual a nova sociedade da informação se depara com uma explosão da comunicação, como conseqüência da revolução tecnológica, e universalização dos hábitos, culturas e consumo, é uma era de rompimento das fronteiras culturais, políticas, religiosas e econômicas. Além disso, vive-se a era da internacionalização da informação, que reduziu também as barreiras de tempo e distância entre as pessoas, trazendo tanto efeitos positivos quanto negativos.

Frisam Maria Lúcia de Arruda Aranha e Maria Helena Pires Martins (2005, p.82) que na sociedade contemporânea, as notícias não chegam como antigamente, no “lombo dos burros”; ao contrário, podem se disseminar instantaneamente por todo o globo, pelas infovias. Do mesmo modo, as crenças solidificadas perdem a força que davam segurança às decisões importantes, enquanto a diversidade das culturas oferece a possibilidade de adesão a ideias mais díspares, colocando em xeque a visão de mundo com aspirações à “verdade absoluta”.

Para o estudo dos crimes digitais, será preciso compreender a era digital desde p surgimento da internet, da sociedade digital, para chegar à criminalidade informática e compreender que esta nova era necessita de limites estabelecidos em prol da segurança de dados e da reputação daqueles que utilizam o mundo virtual.

2.1 SURGIMENTO DA INTERNET

É nesse contexto da era digital, retratado por mudanças constantes, que se forma uma sociedade informatizada e aí também é que se dão os crimes digitais. Portanto, o âmbito de atuação daqueles que cometem os referidos crimes rompe fronteiras.

Tem-se uma ilustração do que foi dito nas palavras de Fabio Jânio Lima Ferreira, com relação à dimensão das dificuldades que a era digital ofereceria com relação à prática dos delitos ora analisados:

> O acesso à informação sempre foi muito valorizado, constituindo verdadeira forma e fonte de poder, sendo seu controle verdadeiro patrimônio econômico, político e cultural. Entretanto, esses benefícios não aparecem sozinhos, trazem consigo os crimes e criminosos digitais, os quais estão aumentando proporcionalmente por todo o mundo, sendo que as mais otimistas previsões apontam para um epidêmico e exponencial crescimento. Os crimes praticados, também chamados de crimes digitais ou transnacionais, podem afetar dezenas de países, sem que o agressor saia de sua casa. É uma preocupação que está chamando a atenção da polícia de todo o mundo, especialmente no que diz respeito à coleta de evidências e materialidade; há também de se considerar o princípio de territorialidade, pois, se o computador está num determinado país, e o crime é cometido em outro, como processá-lo se nunca entrou naquele país? Policiais do mundo inteiro, tais como FBI, Scotland Yard, e Real Polícia Montada do Canadá, já há alguns anos, vêm formando os chamados "Cybercops", policiais especialmente treinados para combater esses delitos - o desafio criminal do próximo século - sendo a tônica, a maximização da cooperação entre os Países, alertando para o potencial das perdas econômicas, ameaças a privacidade e outros valores fundamentais. (FERREIRA, 2011)

Chega-se com essa ilustração à abordagem sobre o surgimento da internet, frisando que ela surgiu como um meio poderoso, capaz de interligar computadores entre si e possibilitar a comunicação entre estes computadores. Sua origem se deu na década de 60, sendo a princípio, de uso exclusivo das forças armadas norte-americana, e depois se mostrando um importante meio de comunicação entre estudantes e professores universitários, e, só posteriormente, passando a ser acessível a todos, alcançando a população mundial na década de 90.

A internet baseia-se na ideia de haver comandos centrais, o que faz com que todos os pontos sejam equivalentes, não importando onde estejam os computadores, se no Brasil, EUA, China, etc., sendo um pressuposto da internet, que ela seja aberta a qualquer computador ou rede que deseje se conectar, mesmo de sistemas diferentes ou de línguas diferentes (CORRÊA, 2002).

Na compreensão de Silva (SILVA, 2000), a Internet, denominada pela mídia de Superestrada da Informação, nada mais é do que a interligação simultânea de computadores de todo o planeta, algo que os futuristas em seus exercícios de suposição jamais imaginaram” (SILVA, 2000).

É válido ressaltar que, atualmente, a sociedade tornou-se dependente dessa tecnologia da informação, assim como, também as relações comerciais, as escolas, faculdades, empresas e até a administração pública, e, recentemente, passou a assumir uma postura bastante comercial através da sua utilização.

Segundo Schoueri (2000, p. 157):

> A internet é uma gigantesca rede mundial de computadores que interliga entre si desde grandes computadores até micros pessoais ou notebooks através de linhas comuns de telefone, linhas de comunicação privada, cabos submarinos, canais de satélite e diversos outros meios de comunicação.

Portanto, essa imensa rede de computadores foi concebida, inicialmente, para fins bélicos, mas seu grande trunfo foi ser acessível a toda a população, principalmente diante da ausência de um proprietário que a explore financeiramente. (RECUERO, 2011).

Como diz Paesani, com seu conhecimento: “a internet não pertence a ninguém, não é financiada por instituições, governos ou organizações internacionais, e também não é um serviço comercial” (2003, p. 36).

A internet pode ser utilizada para as mais diversas finalidades, até mesmo para produzir campanhas eleitorais e outros fins políticos, influenciando massas. A interatividade, portanto, traz facilidades para partidos e candidatos em disputas eleitorais, podendo ampliar o diálogo entre os eleitores através do ambiente virtual. Afinal, os eleitores modernos também querem ser ouvidos e participar dos processos eleitorais e a tecnologia da informação serve a este fim.

Ademais, com o surgimento das redes sociais, iniciou-se uma nova era da internet, sendo o orkut o pioneiro, e em seguida os prediletos dos brasileiros, o facebook e o twitter, ampliando a gama de opções a serviço da interatividade.

Mais recente ainda é o surgimento dos sites de compras coletivas, que fazem uma espécie de intermediação entre os clientes e os fornecedores, oferecendo preços de diversos produtos e serviços bastante atrativos, tornando-se verdadeiros fenômenos de vendas da internet.

O fato é que, a internet atingiu milhões de pessoas espalhadas pelo mundo, devido às características da sua tecnologia de baixo custo e aberta a todos os sistemas operacionais, transformando-se em um fenômeno mundial em muito pouco tempo.

2.2 SOCIEDADE DIGITAL

Paralelamente à revolução tecnológica, pode-se verificar o surgimento de uma nova sociedade, a sociedade digital, que são os cidadãos tendo contato com o mundo informatizado, o que se dá nas mais diversas classes sociais. Através dessa revolução tecnológica, ocorrendo nos meios de comunicação e nos meios de transporte, as distâncias se encurtaram, ainda que as distâncias físicas continuem as mesmas. Ou seja, o progresso tecnológico reduziu distancias, aproximou o mundo, através da possibilidade de comunicação instantânea com qualquer pessoa que esteja conectada a essa rede mundial interligada.

É facilmente perceptível que a sociedade digital está se tornando cada vez mais interligada com o mundo, e tornando estreitas as relações comerciais, econômicas, políticas e sociais, fruto dessa evolução tecnológica. Hoje é perfeitamente possível para uma pessoa comum se intercomunicar diretamente com qualquer pessoa do

planeta, graças ao desenvolvimento tecnológico e toda a parafernália de comunicação digital. Entretanto, apesar desta sensação de proximidade entre as sociedades, entre as pessoas, entre os mercados, percebe-se uma grande tendência da sociedade de ficar mais solitária, uma vez que pode-se pagar as contas sem ir ao banco, fazer supermercado sem sair de casa.

Na verdade, o mundo está em evolução desde os tempos mais remotos, porém, só recentemente é que pudemos verificar esse fenômeno chamado de “globalização”, cujo marco inicial é algo de difícil identificação.

2.3 A CRIMINALIDADE INFORMATIZADA

As inovações trazidas pela internet são, sem dúvida, de extrema importância para o cidadão comum, entretanto, há quem enxergue o computador e a internet de outra forma, de forma traiçoeira, de forma inadequada, buscando a informática para a cometer práticas ilícitas, e com isso, trazendo novas formas de criminalidade.

Com o progresso dos meios informatizados em todas as áreas (especialmente a partir da década de 70), como em bancos, supermercados e indústrias, houve uma generalização do acesso à informática, aos meios eletrônicos, especialmente através da internet, e com isto, veio junto a diversificação da criminalidade, através da prática de delitos facilitados por este acesso às informações. Ou seja, a criminalidade encontrou novas formas de concepção, por meio da prática de delitos através do acesso ao meio informatizado. E para facilitar ainda mais a prática de determinados crimes, em alguns casos, há lacunas da lei penal, diante de condutas que são prejudiciais, mas que ainda não estão tipificadas como delito. E além dos bens jurídicos afetados quando a criminalidade ainda não era informatizada, com o surgimento de uma sociedade digital, outros bens jurídicos passaram a ser afetados (PAESANI, 2003).

Vladmir Aras, um estudioso dos assuntos informáticos, já chama a atenção para o surgimento de um novo ramo do direito a ser estudado e para a sua sistematização, no momento em que os computadores se configuraram como um instrumento

indispensável presente no dia-a-dia das pessoas, do mundo empresarial, e do próprio Estado.

Prosseguindo em sua reflexão, o mesmo autor assevera que:

> A importância da informática na sociedade tecnológica é incontestável. É quase inconcebível imaginar, hoje, um mundo sem computadores. Como funcionariam os grandes aeroportos do mundo sem essas máquinas facilitando o controle do tráfego aéreo? Como seria possível levar ônibus espaciais tripulados à órbita terrestre? Como poder-se-ia projetar e fazer funcionar gigantes como a hidrelétrica de Itaipu? Como decifraríamos o código genético humano, num programa do quilate do Projeto Genoma? Como?
>
> As implicações dessa poderosa máquina no dia-a-dia dos indivíduos são marcantes. Situam-se no campo das relações pessoais, volteiam na seara da Sociologia e da Filosofia, avançam na interação do indivíduo com o Estado (a chamada cidadania digital, e-gov ou governo eletrônico), refletem no Direito Civil (ameaças a direitos da personalidade) e no Direito do Consumidor (responsabilidade do provedor de acesso à internet) e acabam por interessar ao Direito Penal.
>
> Naturalmente, conhecendo as dimensões do país e as suas carências, já é imenso o caldo de cultura para a prática de atos ilícitos em detrimento de bens informáticos ou destinados à violação de interesses e de dados armazenados ou protegidos em meio digital. (ARAS, 2011).

Portanto, o avanço tecnológico traz consigo imensas vulnerabilidade, ou seja, a evolução tecnológica gerou novas formas de práticas ilícitas, de forma que assistimos hoje a um crescimento espantoso da delinquência informática, onde tudo é muito novo, muito recente, não havendo ainda uma prática ética relacionada à tecnologia. Aliado a isto, há a possibilidade de exploração das lacunas legais por parte dos agentes, para se eximirem de sanções penais pela prática de tais atos ilícitos.

3 CRIMES DIGITAIS

Crime digital é um assunto que têm atraido a atenção dos doutrinadores que buscam refletir e lançar bases de fundamentação para a construção de um entendimento acerca de suas modalidades, regulação e adequação ou não ao teor da lei penal existente, ainda assim, é escasso o material publicado a respeito das questões que o cercam.

3.1 CONCEITO

O que ocorre é que o espaço digital é um local onde se pode cometer delitos que já estão tipificados no nosso ordenamento jurídico, mas também há espaço para a prática de condutas que trazem prejuízos a outras pessoas, e apesar disso, não são consideradas incriminadoras no Brasil. A exemplo destas condutas, temos o acesso não autorizado a sistemas informáticos, interceptação de comunicações, infrações de dados, incitação ao ódio, difamação, calúnia, discriminação, terrorismo, difusão de pornografia infantil, e muitos outros. (CRESPO, 2011).

Cabe nesse momento, no intuito de analisar a necessidade de conceituar crimes digitais, mergulhar na reflexão de Copetti (apud GRECO, 2009, p.7), no sentido de compreender a dimensão que tem a tarefa do legislador:

> É nos meandros da Constituição Federal, documento onde estão plasmados os princípios fundamentais de nosso Estado, que deve transitar o legislador penal para definir legislativamente os delitos, se não quer violar a coerência de todo o sistema político-jurídico, pois é inconcebível compreender-se o direito penal, manifestação estatal mais violenta e repressora do Estado, distanciado dos pressupostos éticos, sociais, econômicos e políticos constituintes de nossa sociedade.

Dessa forma, o avanço tecnológico, que carrega consigo inúmeros benefícios já notórios, traz também diversas vulnerabilidades. Portanto, os crimes digitais são muito variados, mudam constantemente, e principalmente, adaptam-se rapidamente às novas potencialidades tecnológicas que surgem.

Como ilustração disto, temos a invasão ao celular de uma atriz americana famosa em 2011, Scarlett Johansson, que teve suas fotografias íntimas extraídas do seu

celular através da interceptação não autorizada de comunicação e dados, e sem o seu conhecimento, sendo difundida pela internet, onde o mundo todo pôde observá-la, o que trouxe danos para a atriz.

Daí se vê que esta é uma nova realidade que o direito penal terá que enfrentar, como instrumento de controle social que é, pois a prática de delitos digitais já é uma realidade. Entretanto, para definir um delito digital não basta considerar apenas a forma como ele foi praticado, mas também é preciso levar em conta o dano que ele causou a bens juridicamente protegidos.

Conforme preceitua Álvaro Mayrink da Costa (2011, p.14):

> Para a existência do delito, é necessário que o ato material causado seja um ato ofensivo a bens ou interesses protegidos (*nullum crimen sine injuria*), isto é, que possa ser valorado como contrário ao que a norma penal protege.

O termo crimes digitais é bastante amplo e abrange as mais diversas condutas, podendo também ser chamado de Crimes Informáticos, Crimes Tecnológicos, Cibercrime, Delitos Informáticos, Fraude Informática, Crimes Cibernéticos, Delinqüência Cibernética, Delitos Computacionais, Crime de Computador, e-crime, crime.com e outras muitas variações com a troca do termo “delito” por “crime” e vice-versa, sendo que esta troca apenas tem o intuito de evitar repetições em excesso nos textos escritos.

Entretanto, o termo mais utilizado é mesmo Crimes Digitais, uma vez que abrange todo o sistema de informática, e não apenas a internet. Porém, este conceito não é uniforme, pois há muitas divergências doutrinárias acerca desta denominação, justamente criticando-a por ser genérica, e por abarcar muitas condutas e muitos bens jurídicos. Independentemente da denominação que se lhe atribua, fato é que, o que se quer regular são os sistemas de informática.

“Podemos definir o crime de computador como toda conduta ilícita praticada por meio de computador ou sistema de informática, que venha a causar prejuízo material ou moral a outrem”. (MARZOCHI, 2000, p 21)”.

Para Carla Araújo Rodrigues de Castro (2003), crime de informática é aquele praticado contra o sistema de informática ou através deste, compreendendo os crimes praticados contra o computador e seus acessórios e os perpetrados através

do computador. Inclui-se neste conceito os delitos praticados através da internet, pois pressuposto para acessar a rede é a utilização de um computador.

Gustavo Correia, por sua vez, conceitua os crimes digitais como sendo: “os crimes relacionados às informações arquivadas ou em trânsito por computador, sendo esses dados acessados ilicitamente, usados para ameaçar ou fraudar; para tal prática é indispensável a utilização de um meio eletrônico.” (2000, p.43).

Portanto, os crimes digitais envolvem o uso de computadores e da rede de internet para a prática de algum delito, desde que haja um prejuízo causado a outrem. E tal prejuízo não precisa ser apenas de ordem patrimonial.

3.2 BEM JURÍDICO INFORMÁTICO

Cabe nesse momento uma reflexão acerca da conceituação de “bem jurídico” no âmbito penal no intuito de iniciar mais minuciosa reflexão acerca dos crimes digitais e sua atipicidade.

Rogério Greco (2009, p.4), preceitua que a finalidade do Direito Penal é proteger os bens mais importantes para a própria sobrevivência da sociedade, e cita Luiz Régis Prado, que diz que “o pensamento jurídico moderno reconhece que o escopo imediato e primordial do Direito Penal radica na proteção de bens jurídicos – essenciais ao indivíduo e à comunidade”.

O termo bem jurídico é entendido como uma limitação ao poder punitivo do Estado. Apesar de haver diversas definições para bem jurídico, de modo geral, vai haver sempre uma relação entre o bem jurídico e a limitação punitiva do Estado. É o que se extrai da reflexão de Francisco de Assis Toledo:

> Bem jurídico é aquele que esteja a exigir uma proteção especial, no ambito das normas de direito penal, por se revelarem insuficientes, em relação a ele, as garantias oferecidas pelo ordenamento jurídico, em outras áreas extrapenais. Não se deve, entretanto,- e esta é uma nova consequência do já referido caráter limitado do direito penal - supor que essa especial proteção penal deva ser abrangente de todos os tipos de lesão possíveis. Mesmo em relação aos bens juridico-penalmente protegidos, restringe o direito penal sua tutela a certas espécies e formas de lesão, real ou potencial. (TOLEDO, 2000, p.17).

Luiz Regis Prado (2007, p. 257) destaca que todo delito deve lesar ou expor a perigo de lesão certo bem jurídico e se refere a este último como um ente (dado ou valor social) material ou imaterial haurido do contexto social, de titularidade individual ou metaindividual reputado como essencial para a coexistência e o desenvolvimento do homem, e, por isso, juridico-penalmente protegido.

Como visto, entende-se que a função do Direito Penal, sob uma perspectiva individual, é a proteção de bens jurídicos e os bens jurídicos são aqueles valores que devem receber maior proteção estatal.

É importante entender o que são bens jurídicos e a função do Direito Penal, para que se possa aplicar e distinguí-los às condutas, e assim, defendê-las como criminosas ou não-criminosas no meio informatizado, uma vez que, a evolução digital trouxe novas idéias quanto a bens jurídicos e isso influencia em uma possível classificação sobre o que sejam crimes digitais.

Sendo assim, cabe questionar se há novos bens jurídicos referentes ao avanço tecnológico, porque se houver novos bens jurídicos, os crimes digitais não se limitarão somente aos bens jurídicos tradicionalmente tutelados. Haverá a possibilidade de lesão a outros bens jurídicos, que surgem de condutas ilícitas praticadas por meio da informática. Isso quer dizer que as condutas não serão restritas aos valores que são juridicamente protegidos, como a vida, a integridade física, o patrimônio, a fé pública, mas também, a outros valores como segurança de sistemas, informações armazenadas, redes de telecomunicações, etc.

A informação, que antes era comercializada apenas em papel (jornal, revistas, etc), hoje, já recebe tratamento de “mercadoria” propriamente dita, pois já é comercializada com facilidade, e é valorizada como se mercadoria fosse, em meio digital e composta por dados. (GOMES, REIS, 2011)

Diante dessa questão, quais seriam os novos bens jurídicos afetados pela criminalidade informática, seria a informação ou os dados, ou ainda os sistemas informáticos?

Além disso, se a informação for considerada como bem jurídico novo a ser tutelado, ainda resta analisar o grau do prejuízo causado para que se possa tipificar as condutas.

Essas questões ainda são complexas e ainda há muito o que discutir, para se chegar a um consenso doutrinário.

3.3 CLASSIFICAÇÃO DOS CRIMES DIGITAIS

Atualmente os crimes digitais são classificados em crimes digitais próprios e crimes digitais impróprios. A diferença entre os crimes digitais próprios e impróprios é quanto ao *modus operandi.* Os crimes digitais próprios são aqueles praticados exclusivamente através de sistemas informáticos, pois somente através desta, é que torna-se possível a execução e consequentemente a consumação do delito. Entretanto, tais crimes são tipos novos, que agridem sistemas de informática como bem juridicamente protegido, e, diante da escassez de legislação existente neste âmbito, alguns fatos não podem ser punidos por serem atípicos. (CASTRO, 2003).

Os crimes digitais impróprios, diferentemente da classificação anterior, podem ser praticados de todo modo, e também através de sistemas de informática. Desta forma, o agente que comete o delito, utiliza, esporadicamente, a informática. O computador funciona como um instrumento para a execução do crime. Estes, são delitos que violam bens já protegidos por nossa legislação, como o patrimônio, a honra, a ameaça, estelionato, calúnia, pedofilia. Para tanto, utiliza-se a legislação existente.

Ou seja, nos crimes digitais próprios o que muda é o modo como se pratica a ação delitiva, pois só podem ser praticados através da informática, sendo que não é necessário conhecimentos técnicos específicos. Já os ilícitos digitais impróprios são aqueles que dependem de conhecimento técnico próprio do âmbito da computação. Enquadram-se nestes, os *hackers*, os crackers, justamente por deterem maior conhecimento informático. (CRESPO, 2011).

Portanto, nos crimes digitais próprios, a informática funciona como meio e fim desejado pelo praticante do delito, de forma que, não havendo legislação específica, não será possível punir o responsável pelas condutas ilícitas praticadas pelo computador. (COSTA, 2011).

Essa classificação de crime digital em próprio e impróprio, nos diz que os crimes são próprios porque foram produzidos e praticados pela informática, e são impróprios porque o meio utilizado para a prática do crime é o computador.

Essa distinção entre crimes próprios e impróprios é muito importante, porque através desta análise é que será possível concluir se a conduta ilícita é realmente criminosa ou mesmo discutir acerca da questão, com a finalidade de tipificar e punir tais condutas.

Quanto aos crimes digitais impróprios, a semelhança entre este e o crime comum encontra-se no bem jurídico tutelado. Uma injúria, por exemplo, sempre atingirá a honra subjetiva da vítima, mesmo que praticada por meio do computador. (COSTA, 2011).

Sendo assim, podemos afirmar que o crime comum que for praticado por meio informático, não requer legislação nova para tipificação da conduta. Entretanto, existem questões que necessitam ser revistas, como a coleta e análise das provas, questões de cooperação internacional entre países, e muitos outros.

Outra questão a ser analisada, é que quando se diz que o crime foi praticado por meio da informática e contra o computador, não é a máquina que foi atingida, mas um certo banco de dados do computador é que sofreu danos. E a análise desta conduta, perante a nossa legislação vigente nos deixa em dúvida, se é uma conduta atípica ou um delito de dano. Isso ocorre porque o mundo digital é muito novo, e sujeito a muitas indefinições, principalmente a ausência de normas regulamentadoras.

Tanto o banco de dados destruido ou danificado, quanto o equipamento que abriga a informação, são merecedores de proteção jurídica. Entretanto, a condenação da conduta causadora do dano, atualmente, só poderá ocorrer na esfera civil, obrigando ao agente reparar os danos. A responsabilização penal do agente será ineficaz, se aplicada a legislação em vigor.

A propósito, como já visto, isto ocorre em função do princípio da legalidade, em que as ações praticadas por meios informáticos, prejudiciais a terceiros, precisam necessariamente estar previstas previamente em lei para poderem ser punidas.

Então, para analisar a questão da tipicidade ou da atipicidade das condutas praticadas na informática, será preciso definir antecipadamente se os bens informáticos em questão estão na categoria dos bens já tutelados pela norma penal, para posteriormente, examinar se estes podem ser tutelados por normas já existentes ou se necessitam de novas normas. (COSTA, 2011).

Podemos citar como crimes digitais próprios, aqueles crimes ofensivos contra os dados contidos no computador, e também as ações que atentam contra a inviolabilidade de correspondência eletrônica, do software, da segurança nacional, e outros tantos semelhantes.

Existe outra classificação para os crimes digitais, denominada tripartida, em que estes são divididos em crimes digitais puros, mistos, ou comuns.

Crimes digitais puros são aqueles delitos em que o sujeito visa atingir especificamente o computador como um todo, ou seja, o sistema de informática.

Crime de informática misto não são as infrações em que o agente visa atingir o sistema de informática especificamente, mas esse sistema de informática é a ferramenta essencial para a execução e consumação do delito.

E por fim, os crimes de informática comuns são as condutas em que o agente utiliza a informática como um instrumento, entretanto, não é indispensável, sendo que o crime pode ser consumado por outros meios.

3.4 LEGALIDADE E TIPICIDADE DOS CRIMES DIGITAIS

A internet é a inovação tecnológica mais importante do nosso tempo, modificando as relações sociais e provocando impactos nos diversos ramos do direito. Essa vasta influência alia-se ao fato de que as mudanças sociais sempre estarão à frente do direito, que por sua vez, bucará acompanhar as mudanças sociais no intuito de regular as novas relações daí advindas.

Sendo assim, o surgimento de novos fenômenos jurídicos implicarão no surgimento de novas normas, para a solução dos conflitos que passam a compor a realidade social.

Sabe-se, entretanto, que uma das maneiras de diminuir o problema da falta de normas capazes de punir as condutas ilícitas informáticas, seria a analogia, que não é admitida no Direito Penal Brasileiro, salvo em benefício do réu. A analogia é uma forma de suprir lacunas na legislação existente, ou nos dizeres de Fernando Capez (2011,p. 30): “a atividade consistente em aplicar a uma hipótese não regulada por lei disposição relativa a um caso semelhante”.

> Diante do princípio da legalidade do crime e da pena, pelo qual não se pode impor sansão penal a fato não previsto em lei, é inadmissivel o emprego da analogia para criar ilícitos penais ou estabelecer sanções criminais. (MIRABETE, 2012, p. 139).

Diante das particularidades da seara penal, destacando-se dentre elas a intervenção, por meio da repressão delitiva, nos direitos mais elementares do indivíduo, e, em decorrência disso, seu caráter de *ultima ratio*, tem-se no teor do Princípio da Legalidade, uma limitação ao poder que o Estado tem de punir.

Entretanto, de acordo com o artigo 1º da Constituição Federal Brasileira, obrigatoriamente deve-se aplicar em território brasileiro, os princÍpios da legalidade e da anterioridade da lei penal, previsto no artigo 1º do Código Penal Brasileiro, e no artigo 5º, inciso XXXIX, da Constituição Federal, onde está estabelecida a garantia “Não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal.”

Dessa maneira, no Direito Penal Brasileiro, o crime deve estar previamente descrito em lei, sob pena de não ser enquadrado como crime.

Luiz Regis Prado (2007, p.133) analisa o supracitado artigo do Código Penal asseverando que ele possui dicção legal com sentido amplo e que o seu teor indica que:

> A criação dos tipos incriminadores e de suas respectivas consequências juridicas esta submetida a lei formal anterior (garantia formal) e compreende, ainda, a garantia substancial ou material que implica uma verdadeira predeterminação normativa (*lex scripta lex praevia et lex certa*).

Acerca do que foi dito, Bitencourt (2000, p.10) esclarece:

> Pelo princípio da legalidade, a elaboração de normas incriminadoras é função exclusiva da lei, isto é, nenhum fato pode ser considerado crime e nenhuma pena criminal pode ser aplicada sem que antes da ocorrência desse fato exista uma lei definindo-o como crime e cominando-lhe a sanção correspondente. A lei deve definir com precisão e de forma cristalina a conduta proibida.

Ademais, essa descrição deve ser expressa e determinada, evitando o arbítrio do julgador, e reforçando a segurança jurídica e as garantias individuais.

Assim, diante da necessidade de preenchimento das lacunas oriundas do universo da tecnologia digital, Gustavo Testa Corrêa ressalta:

> A tecnologia digital é uma realidade, e justamente por isso estamos diante da criação de lacunas objetivas, as quais o direito tem o dever de estudar, entender e, se necessário preencher. (CORRÊA, 2002, p 41).

Por esta razão, fica evidente que o Direito Penal Brasileiro não é suficiente para coibir de forma adequada todas as condutas ilícitas praticadas no âmbito informático por meio de computadores.

Nessa mesma linha, é o pensamento de Ivette Senise Ferreira:

> Essas leis, todavia, longe de esgotarem o assunto, deixaram mais patente a necessidade do aperfeiçoamento de uma legislação relativa à informática para a prevenção e a repressão de atos ilícitos específicos, não previstos ou não cabíveis nos limites da tipificação penal de uma legislação que já conta com mais de meio século de existência. O Código Penal Brasileiro, cuja Parte Especial data de 1940, e portanto elaborado numa época em que se dava primazia à proteção individual, apesar do volume da legislação especial que o acompanhou posteriormente, não se mostra suficiente e adequado para suprir as necessidades nesse setor e coibir abusos que se verificam de forma crescente e diversificada, com a constituição de novas modalidades de ofensas a interesses legítimos, no plano individual e social, que ao Estado cumpre coibir sobretudo através do direito penal, se os conflitos não puderem ser solucionados de outra forma, como dispõe a boa doutrina, segundo o princípio da subsidiariedade. (FERREIRA *apud* LIMA, 2011, p 114).

Percebe-se da análise realizada, que algumas condutas que lesam bens jurídicos não são considerados crimes pela falta de legislação que provoca lacunas jurídicas, configurando a atipicidade de determinadas práticas e fazendo com que sobre sua execução não recaia nenhuma sanção prevista que possa ser aplicada ao sujeito que as pratica. A ausência de previsão legal, portanto, é um grande óbice no combate aos crimes digitais.

Sendo assim, por mais evidente que pareça, é importante ressaltar que o Direito Penal e a Internet possuem interação, uma vez que o mundo virtual e toda sua cultura atingem de forma relevante as relações do mundo real, devendo, desta forma, o Direito regular as condutas alí praticadas.

Cabe ao Direito regulamentar as condutas que os sujeitos da sociedade informatizada praticam, controlando comportamentos que prejudiquem os bens jurídicos penalmente tutelados, como o patrimônio, a honra, entre outros.

Desta forma, pelo que já foi dito, em território brasileiro devem ser aplicados, obrigatoriamente, os princípios da legalidade e da anterioridade da lei penal. Neste

sentido, pode-se afirmar que a tipicidade é consequência direta do princípio da legalidade, pois, somente um fato previamente descrito em lei, poderá ser típico.

O instituto da tipicidade penal abarca o aspecto formal, que diz respeito à adequação da conduta do agente ao modelo abstrato previsto em lei, como também o aspecto conglobante, que vai além e busca averiguar, segundo Greco (2009, p.65), se a conduta do agente é antinormativa e se o fato é materialmente típico.

Além da necessidade de existir um modelo abstrato que preveja com perfeição a conduta praticada pelo agente, é preciso que, para que ocorra essa adequação, isto é, para que a conduta do agente se amolde com perfeição ao tipo penal, seja levada em consideração a relevância do bem que está sendo objeto de proteção. (GRECO, 2009).

No mesmo sentido Francisco de Assis Toledo (2000, p.131) ensina:

> A conduta, para ser crime, precisa ser típica, precisa ajustar-se formalmente a um tipo legal de delito (*nullum crimen sine lege*). Não obstante, não se pode falar ainda em tipicidade, sem que a conduta seja, a um só tempo, materialmente lesiva a bens jurídicos, ou ética e socialmente reprovável.

Na realidade, para se alcançar a adequação típica é necessário que o fato ocorrido, possua mais do que semelhança com a conduta penalmente descrita, sendo indispensável a combinação exata com o tipo penal.

E, portanto, com a chegada da era da informática, assistiu-se de perto a um acelerado desenvolvimento tecnológico, e junto com ele surgiram condutas reprováveis, praticadas por meios digitais, gerando a necessidade de alteração da legislação existente, diante dessa nova realidade tecnológica que impera.

É neste sentido, que a alteração da estrutura normativa vigente ou criação de nova legislação penal torna-se necessária, uma vez que esta mostra-se incapaz de dar uma resposta às novas condutas ilícitas que surgem a todo momento, decorrentes da evolução tecnológica.

Desta forma, uma mudança legislativa permitirá adquirir a segurança jurídica indispensável para continuar perseguindo a imensurável quantidade de avanços tecnológicos que a informática ainda proporcionará no futuro.

Nesse passo, a rede mundial de computadores, em função da sua vulnerabilidade, pode ser um espaço para a prática de delitos que já estão positivados no ordenamento jurídico brasileiro, mas também, é um espaço onde podem ser praticadas condutas danosas, que ainda não são punidas por serem atípicas no Brasil.

Desse modo, identificam-se duas formas delitivas dentre os crimes informáticos, a primeira delas são os delitos já existentes, porém praticados por meio da internet, ou seja, somente há a mudança do *modus operandi*, em que tais crimes são praticados através da informática, como ocorre nos delitos contra a honra, contra a liberdade individual e contra a propriedade. A segunda espécie são as novas condutas nas quais o bem jurídico atingido é o próprio sistema de informática, e portanto são necessários conhecimentos técnicos específicos em computação. Esses delitos não têm previsão ordenamento pátrio, uma vez que não podiam ser previstos pelo legislador do passado.

Não se pode deixar de observar, que através da prática de delitos virtuais, há diversas possibilidades de violação a bens jurídicos de muita importância. E, como as mudanças sociais ocorrem a todo o tempo, e de forma dinâmica, qual seria a solução para o combate a este tipo de prática criminosa que surge com a evolução tecnológica, já que o direito penal não deve ser invocado a todo tempo, mas apenas como *última ratio,* para atuar nos casos mais graves e contra os bens jurídicos mais importantes de acordo com o princípio da intervenção mínima? Ou isso poderia ser considerado como uma nova adaptação dos delitos, e os bens jurídicos seriam aqueles já tutelados pelo direito penal? (CRESPO, 2011).

Para Marzochi (2000, p.63):

> O crime de computador não é um crime novo, diferente do que já é previsto na lei. O que acontece é uma super valorização do meio de execução da conduta. A maioria dos delitos praticados pelo computador podem ser encaixados na atual lei penal. Os que não podem são os chamados de crimes de informática puros – aqueles que se utilizam da rede para execução da conduta e obtenção do resultado – como, por exemplo, o acesso não autorizado a computadores ou sistemas. Esses é que devem ser objeto de uma legislação específica que vise não apenas criminalizar determinadas condutas, mas também transformar a informação num bem juridicamente tutelado.

Desta forma, questiona-se, sobre a necessidade da lei penal adaptar-se a estas mudanças dinâmicas que a era cibernética trouxe, reconsiderando os valores

atribuídos aos bens jurídicos, que sabe-se, vão se alterar numa velocidade inalcançável pelo direito, pois estas mudanças vão ocorrer sempre e a todo momento.

Em reflexão acerca do tema, Liliana Minardi Paesani (2003, p. 38), afirma que:

> A rede mundial é dotada de características absolutamente próprias e conflitantes: ao mesmo tempo que se tornou um espaço livre, sem controle, sem limites geográficos e políticos, e, portanto, insubordinado a qualquer poder, revela-se como um emaranhado perverso, no qual se torna possível o risco de ser aprisionado por uma descontrolada elaboração eletrônica.

Nos crimes digitais impróprios, em que um aparelho de informática, ligado à internet (como um ipad ou iphone) é um meio usado para a prática de um delito comum, seria também conveniente a alteração legislativa, para que hovesse uma punição maior, aumentando a sanção, como forma de coibir tal prática por meio informático. Entretanto, estaríamos diante da criação de legislação desnecessária.

Como exemplos destes crimes digitais impróprios, temos a situação em que o infrator envia a um usuário de serviços bancários e-mails com menssagens falsas, buscando capturar suas informações pessoais, para obter vantagem patrimonial. (COSTA, 2011).

Tais infratores, aproveitam-se do conhecimento limitado em termos informáticos por parte das vítimas (e das autoridades), associado a um incipiente conhecimento da tecnologia informática apta a investigar os delitos, e praticam modalidades criminosas antigas, já conhecidas pela nossa legislação Penal, que são os crimes digitais impróprios.

Nos crimes digitais próprios em que a informática é um meio e também um fim desejado pelo agente, se não houver criação de legislação específica, pelo princípio da anterioridade do Direito Penal, não teremos como punir os responsáveis por estas condutas, pois é neste momento que surge a dúvida, em se tratando de ações prejudiciais, se as ações estão ou não tipificadas na legislação.

Portanto, mesmo que as ações praticadas pelos agentes sejam prejudiciais ao convívio social, não poderão ser punidas, já que não estão previstas em lei.

Sendo assim, a questão que merece reflexão, é aquela relacionada à adequação correta da figura típica existente com as ações do mundo digital.

Como o computador tornou-se indispensável à sociedade atual, essa era digital trouxe também um novo meio para alcançar resultados danosos a essa sociedade. E uma lesão praticada contra um computador, atinge também todo o conteúdo nele existente, além do hardware e do software, os dados destruidos muitas vezes possuem valor intangível.

Quando um banco de dados é danificado, copiado ou divulgado, há bens que possivelmente serão lesados, como o patrimônio, a honra, a imagem, a intimidade e até a segurança nacional. Neste caso, a informação tornou-se um bem valioso, nessa nossa sociedade digital, seja pelo valor patrimonial ou pelo valor intelectual agregado. Entretanto, estes bens jurídicos lesados não estariam adequados ao mundo da informática. Por esta razão, há a necessidade de que o Direito Penal se adeque à nova realidade social.

Embora não seja somente a ausência de legislação específica, a incentivadora da criminalidade informática, incluindo a utilização incorreta da internet pelos usuários de computador, provavelmente é um dos principais motivos que explicam o aumento desta criminalidade.

A esse respeito, qualquer lesão a estes bens informáticos ou digitais, como uma invasão a *homepages*, com alteração de seu conteúdo, ou pichação com palavras de escárnio, será ainda tratada como conduta atípica pelo Direito Penal. Tratam-se de condutas que necessitam de legislação específica.

Outra questão importante é se deveria proteger o proprietário das informações, ou o possuidor das informações, e se as informações devem se vincular a pessoas, ou devem ser tratadas de forma independente. E ainda, é preciso questionar aspectos como o lugar do crime, quando do cometimento de delitos digitais. (GIL, 2002).

Sendo assim, é importante esclarecer que o ordenamento jurídico brasileiro não tipificou a conduta de acesso não autorizado a sistemas informáticos, entretanto, mesmo assim, é reconhecida consensualmente a postura ilícita de acessar sem autorização um sistema informatizado.

Na verdade, o acesso não autorizado é uma conduta reconhecida por toda a sociedade como grave, e apesar de entender que deva ser regulada pelo ordenamento jurídico pátrio, mostra-se mais como um passo do *iter criminis* para

condutas que podem gerar prejuízo muito maior do que a simples invasão ilegítima. E esta conduta já é tipificada pelo direito penal em algumas legislações estrangeiras há algum tempo (CRESPO, 2011).

A questão importante é, se a conduta informática irregular deve ser tipificada no ordenamento jurídico pátrio ou não. Isso, porque o mero acesso a sistemas informatizados não autorizados não traria grandes problemas, senão a exposição da vulnerabilidade do sistema invadido, podendo ser considerado como um crime de perigo.

Por outro lado, seria importante também a regulação do uso da internet numa escala mundial, visto que, não há legislação que limite o uso e, portanto, que impeça o acesso não autorizado a sistemas informáticos, senão a ética e o bom senso comum. Paesani reclama, com razão, desta situação:

> Chama a atenção pública mundial a absoluta ausência de uma legislação supranacional para discipliná-la (a internet e seu uso), decorrente, principalmente de sua própria estrutura, para servir no controle, na censura e na distribuição da informação. (PAESANI, 2003, p.84).

Apesar de não haver regulação no Brasil, para as invasões a sistemas ou bancos de dados informatizados, já há o projeto de lei PLC nº 35/2012, aprovado recentemente pelo Senado, de autoria do deputado Paulo Teixeira (PT-SP), que modificará o Código Penal prevendo a regulação de uma série de delitos cibernéticos, como a violação indevida de equipamentos e sistemas concectados ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização do titular, ou ainda para instalar vulnerabilidades, incluindo dentre tais dispositivos celulares, notebooks, desktops, tablets ou caixas eletrônicos.

O PLC nº 35/2012, estabelece em seu artigo 154-A:

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não a rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades:
>
> § 1o Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no *caput*."

O mesmo projeto de lei, prevê, além destas, condutas bastante prejudiciais como obter, pela invasão, conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais e informações sigilosas podem ter pena de três meses a

dois anos de prisão, além de multa. Há ainda a tipificação de condutas menos graves, como a invasão de dispositivo informático, que podem alcançar penas de três meses a um ano, além de multa.

Além disso, ainda de acordo com o PLC nº 35/2012, estará praticando crime quem produzir, oferecer ou vender programas de computadores que permitam a invasão a outros computadores.

Contudo, o citado projeto ainda encontra-se em trâmite, aguardando revisão na Câmara dos Deputados, por haver sofrido emendas durante a aprovação de seu texto pelo Senado Federal.

Dentre as outras principais iniciativas legislativas no Brasil, acerca de crimes digitais, ainda tramitando no Congresso Nacional está o PL, nº 84/99, que visa a regulação das invasões a sistemas ou bancos de dados informatizados. Desse modo, o dispositivo busca regular a conduta de acesso não autorizado, conforme seu art. 2º do Substitutivo ao PL, nº 84/99:

> Art. 285-A. 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.

E, neste sentido, pode-se afirmar que na legislação penal pátria é quase inexistente a repressão a condutas atentatórias no campo da informática. E conforme já foi mencionado, a analogia é proibida, exceto para uso em benefício do réu, tornando-se difícil até mesmo enquadrar condutas já previstas no Direito Penal Brasileiro, como violação de correspondência, praticada por meio informático. É o que ocorre quando há violação de e-mail, situações que, somente com esforço extraordinário podem ser adaptadas às normas existentes.

Entretanto, resta questionar até quando poderá ser sustentada a aplicação das normas existentes no Direito Penal, como também em outros ramos do Direito, para a adequação dos crimes comuns às condutas ilícitas dos crimes digitais.

Ocorre que, enquanto isso, parece haver uma flexibilização da tipicidade formal, ou seja, da necessidade da subsunção perfeita da conduta ao tipo previsto, ou talvez uma corrente que busca adequar a norma existente ao fato que se apresenta, até

que o Direito se reinvente, se modernize, afinal, não pode o bem jurídico ficar desamparado. Entretanto, apesar desse esforço interpretativo, em adequar os tantos crimes informáticos ao Código Penal atual, é evidente que tal tentativa resvalará para a atipicidade penal.

3.5 TEMPO, LUGAR E CONSUMAÇÃO DOS CRIMES DIGITAIS

Para analisar a questão do “Tempo e do Lugar” voltada para os crimes virtuais, é preciso inicialmente ressaltar que o Código Penal brasileiro adotou a teoria da ubiqüidade, para a determinação do lugar do crime, conforme o artigo 6º, a seguir: “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”.

A determinação do lugar do crime é fundamental para a aplicação ou não da lei brasileira e para a determinação da competencia. Assim, para que seja aplicada a lei brasileira é necessário que o crime haja tocado o território nacional. (Nelson Hungria, comentários ao CP, 1997).

Muito comum é o chamado crime à distância, aquele que a conduta é praticada fora do país e o resultado ocorre aqui, e vice-versa. A regra acima é aplicável aos crimes de informática. Destarte, é necessário identificar o local da ação e o do resultado; se ambos ou algum deles ocorreram no território nacional, o Brasil será competente. Todavia, se a ação foi praticada na França e o resultado ocorreu nos Estados Unidos, a lei brasileira não será aplicada. Mas em qualquer caso que a ação, parte dela ou o resultado ocorrem no Brasil será aplicada a lei brasileira. (CASTRO,2003)

Entretanto, o surgimento do “mundo virtual”, em que não há um território físico, confere maior importância ao lugar onde está localizada a informação, ou seja, o território onde a informação ou mercadoria está fisicamente estabelecida. (CRESPO, 2011).

Nos casos de crimes praticados por meios virtuais, a localização do lugar da informação ou da mercadoria, torna-se importante, entretanto, em muitos casos

estes delitos vão ocorrer em ambientes virtuais entre países diferentes, conferindo uma natureza internacional a este crime, pois é praticado em um país e ao mesmo tempo em outro (o país que vai sofrer os efeitos do crime virtual). Assim, os crimes digitais podem ser praticados em diversos países, de forma parcial.

Isso pode ocorrer por meio da criação de um vírus, ou a invasão de um sistema informatizado e o roubo destes dados, com a venda de informações importantes para empresas rivais, etc. Desta forma, o lugar do crime passa a ser indeterminado, pois é necessário determinar qual a teoria será aplicada para determinar o lugar do crime, levando em consideração que a depender do país, vai-se aplicar teorias diferentes (CRESPO, 2011).

E o artigo 5º, caput do Código Penal, estabelece a regra da territorialidade, determinando a aplicação da lei brasileira, sem prejuízo de convenções, tratados ou regras de direito internacional, ao crime cometido em território nacional: “Art. 5º. Aplica-se a lei brasileira, sem prejuízo de convenções, tratados e regras de direito internacional, ao crime cometido no território nacional.” .

Porém, o fato relevante é que o crime virtual pode ser cometido em qualquer lugar, o resultado deste e o prejuízo, em outro lugar e o agente que praticou o crime pode estar em outro país. Torna-se difícil a apuração do crime com as regras positivadas no Código Penal, por não solucionar questões determinantes como estas, e sendo assim, pode-se reforçar a constatação de que estes crimes não estão previstos em lei no Brasil.

Para a solução destas questões, talvez seja necessário a integração de paises envolvidos no combate aos crimes digitais, estabelecendo convenções e tipificando as condutas apontadas como crimes virtuais (CRESPO, 2011).

Quanto ao momento consumativo a legislação penal pátria codificada conceituou o momento da consumação do crime e também estabeleceu quando o crime permanece na fase da tentativa, conforme pode-se verificar no artigo da lei, transcrito abaixo:

> Art. 14. Diz-se o crime:
> I – Consumado, quando nele se reúnem todos os elementos de sua definição legal.
> II – Tentado, quando, inicada a execução, não se consuma por circunstancias alheias à vontade do agente.
> Parágrafo único: Salvo disposição em contrário, pune-se a tentativa com pena correspondente ao crime consumado, diminuída de um a dois terços.

Bitencourt (2000, p.354) ensina que consuma-se o crime quando o tipo está inteiramente realizado, ou seja, quando o fato concreto se subsume no tipo abstrato da lei penal. Quando são preenchidos todos os elementos do tipo objetivo, pelo fato natural ocorre a consumação. Consuma-se o crime quando o agente realiza todos os elementos que compõem a descrição do tipo legal.

O mesmo Autor trata do crime tentado evidenciando que a tentativa é a realização incompleta do tipo penal, do modelo descrito na lei. Assim, ele pontua:

> A tentativa é o crime que entrou em execução, mas no seu caminho para a cnsumação é interrompido por circunstâncias acidentais. A figura típica não se completa. A conduta desenvolve-se no caminho da tipicidade, mas, antes que o agente a atinja, causa estranha detém seu movimento. Fica faltando, para dizer com Beling, “a fração última e típica da ação”. (2000, p.356)

Os delitos possuem instantes consumativos diferentes, variando de acordo com a infração penal selecionada pelo agente. E quanto aos crimes praticados no meio eletrônico também não é diferente, possuindo estes, momento de consumação de difícil verificação.

Para a sociedade que utiliza os serviços por meio da internet, já é indiscutível a conveniência da adoção de medidas de segurança e prevenção, como também da regulamentação de condutas ilícitas digitais, antes de tornar tais condutas incriminadoras. Entretanto, para determinar o momento consumativo do crime praticado pelo uso do computador, é necessário verificar o *iter* percorrido, ou seja, o caminho percorrido pelo agente dentro do ambiente digital até a execução do delito. Isso quer dizer que o *iter* exige a verificação do planejamento, da preparação, da execução, da consumação com ou sem o exaurimento, e também a verificação da destruição do rastro do crime ou das provas. Isso é algo ainda difícil de investigar, o que torna o ilícito mais atrativo, pois conta com essa facilidade a favor do autor do delito (COSTA, 2011).

E para piorar a situação, a dificuldade de determinação do momento do crime, algumas vezes leva o direito penal a ser incapaz de solucionar estes novos desafios.

4 RESPONSABILIDADE PENAL EM CRIMES DIGITAIS

4.1 SUJEITOS ATIVOS E SUJEITOS PASSIVOS DOS CRIMES DIGITAIS

Em princípio, qualquer pessoa pode ser um sujeito ativos dos crimes de informática. Entretanto, para praticar um crime com um computador através da internet, é preciso ter algum conhecimento de informática por parte do infrator, pois, para invadir outro computador e ter acesso a arquivos e dados ou mesmo causar algum estrago, é preciso compreender o funcionamento daquele sistema informático que vai ser invadido, conseguir de alguma forma as senhas de acesso, e no mínimo, saber qual o conteúdo dos arquivos que se busca.

Em se tratando da invasão do sistema de uma empresa, o agente terá que obter, ainda, informações sobre a empresa, sobre os clientes e talvez até sobre os funcionários. Um agente invasor com este perfil é chamado de *hacker,* que é o sujeito ativo do delito digital.

Tcom relação aos sujeitos ativos dos delitos digitais, tem-se que sempre que se fala em *hacker,* deve-se lembrar que são conhecidos como “bandidos” ou “piratas” da internet, como uma forma de identificar os autores de condutas ilícitas no meio digital.

> Hacker – é o nome genérico dado aos piratas de computador. Surgiu nos laboratórios do MIT (Massachuts Institut of Tecnology), onde os estudantes ficavam noites em claro averiguando tudo o que se podia fazer com um computador. A melhor tradução para esta expressão é “fuçador”, e é usada na grande maioria das vezes, sempre de forma pejorativa. O harcker é aquele que invade sistemas em benefício próprio, obtendo dados e informações alheias (documentos, programas, músicas, etc), mas sem danificar nada. Ou, pode ser, qualquer um que tenha grande conhecimento sobre computadores e faça invasões. O fato é que as definições são inúmeras, e nenhuma em consenso, sendo a última a mais razoavelmente aceita (CRESPO, 2011, p. 95).

Diante disto, percebe-se que o *hacker* não é bem um desinteressado em prejudicar outras pessoas, mas alguém que está interessado em aprender uma forma eletrônica para cometer atos ilícitos, com algum objetivo, e assim, conseguir algo deste conhecimento.

> Hacker é o indivíduo que tem a intenção, através do computador, de adentrar um sistema sem ter autorização. Hacking seria este ato. Seria o

> mesmo que ultrapassar, quebrar, ou entrar em algum lugar para o qual é necessária prévia autorização. (CORRÊA, 2002, p 57).

Segundo Crespo (2011), apesar da fama de criminosos virtuais, nem todo hacker deseja causar prejuízo ao outro usuário de computador, havendo o *hacker* do bem, que invade computadores com o intuito de aprender e descobrir falhas e deixando mensagens que informam sobre a falha de segurança no sistema, e ainda, aconselhando a providenciar segurança mais efetiva. Alguns destes passam até a trabalhar na empresa invadida, desenvolvendo programas para prevenir outras invasões.

Porém, o hacker é o termo mais conhecido, genérico, que pode se subdividir em diversos outros, como *cracker, carders, lammers e wannabes*, e etc.

Para Schoueri (2000, p. 103): “Aquele que invade sistemas para causar dano é chamado *cracker*.”

Já conforme Paesani (2003, p. 38), cracker seria um *hacker* não ético:

> *Hacker* não ético (cracker) é o invasor destrutivo que tenta invadir, na surdina, os portões de entrada dos servidores internet, que são a melhor forma de disseminar informações. É forçoso admitir que, até o momento são os grandes vitoriosos nessa batalha informática. No Brasil, a invasão mais agressiva ocorreu no dia 6 de junho de 1999, quando as páginas da Presidência da República na internet foram invadidas por hackers e os textos com ataques ao governo também ocuparam o site do Supremo Tribunal Federal.

Portanto, segundo Crespo (2011), *os Crackers* é que seriam os verdadeiros criminosos da rede mundial de computadores, pois destroem sites e se divertem com isso, deixando mensagens de escárnio ou ofensivas, para causar repercussão na imprensa. Além disso, também vendem informações roubadas da internet (CRESPO, 2011).

Já os *Carders* são estelionatários que fazem compras pela internet com números de cartão de credito roubados de sistemas de informações ou de usuários que desconhecem a segurança dos computadores (CRESPO, 2011).

Nos anos 70, os crimes digitais eram praticados por agentes com formação em computação, com conhecimento especializado na área, como os técnicos de informática. Entretanto, com o passar dos anos, o computador tornou-se mais acessível às milhares pessoas de todas as classes sociais, em todo o mundo, fato este que vem facilitando a pratica de tais crimes por qualquer pessoa. (LIMA, 2011).

De qualquer forma, todos estes sujeitos ativos precisam ter um alto conhecimento em informática e uma certa inteligência, para usar na invasão de computadores e cometimento de delitos virtuais, além de ser capaz de conseguir apagar o rastro deixado por este tipo de prática ilícita.

O sujeito passivo também pode ser qualquer pessoa que esteja conectada à internet, e, por exemplo, através de um virus pode ter todos os seus programas destruidos.

Entretanto, neste tipo de crime as empresas são os maiores alvos e preferem arcar sozinhas com os prejuízos, do que tornar pública a sua vulnerabilidade na segurança do sistema de informática que possuem. Porém, essa atitude dificulta o conhecimento e a apuração destes crimes. Por outro lado, essa publicidade pode trazer mais prejuízos do que o já sofrido, se em consequência disto, houver a perda de seus clientes, por não se sentirem seguros com o sistema utilizado pela instituição.

A título de exemplo, observa-se a empresa Sony, que revelou em 2011, que sofrera invasão de harckers em sua rede virtual de videogames Playstation. Após esta invasão, os dados pessoais e dados de cartão de crédito, bem como senhas de acesso, de usuários de jogos on line do Playstation, serviço com mais de 70 milhões de usuários em todo o mundo, foram roubados, gerando insegurança e insatisfação de seus clientes com referida empresa. Por este motivo, algumas empresas preferem ficar em silêncio em relação a estes crimes.

E, nesta situação é que surge um dos maiores obstáculos para conhecimento e apuração dos crimes. Na maioria das vezes a empresa prejudicada prefere arcar com os danos causados pela infração, do que tornar público o fato de ter sido vítima deste tipo de crime. Tornar pública a vulnerabilidade do sistema de informática da empresa pode causar prejuízos maiores do que os efetivamente sofridos. (CASTRO, 2003).

A título de exemplo, como ocorre em uma instituição financeira que tenha seu sistema de informática violado e, com isso, o dinheiro de alguns clientes tenha sido transferido para uma conta desconhecida. Certamente o banco ressarcirá seus clientes, sendo este o prejuízo sofrido. Porém, se tornar público este episódio, o mesmo banco poderá perder milhares de clientes, inseguros com o sistema utilizado

pela instituição e temerosos que seu dinheiro também desapareça. A perda dos clientes provoca um prejuízo muito maior do que o efetivamente sofrido. Daí algumas empresas preferirem omitir tais informações. (CASTRO, 2003).

O serviço de provedor de acesso à internet consiste em um serviço em que é disponibilizado ao usuário meios que permitam a conexão de um computador à internet.

Por ser de difícil identificação do autor dos crimes digitais, é que surgiu uma polêmica a respeito da possibilidade de apontar um substituto a ser responsabilizado, no âmbito penal, pela prática de tais delitos virtuais. São as pessoas jurídicas provedoras de acesso à rede mundial de computadores, que, de alguma forma, favoreceu o crime praticado, por meio do serviço de disponibilização do ambiente virtual. (CRESPO, 2011).

Ocorre que, muitas vezes, os provedores de acesso á internet são omissos, pois têm conhecimento da prática abusiva, ou ilícita, por meio do próprio serviço que presta, ou têm conhecimento do conteúdo exibido pelos seus usuários, e nada faz. Mas, também há situações em que os provedores não detêm o conhecimento do conteúdo ilícito que os usuários possuem dentro de seus computadores pessoais. E os usuários de provedores de acesso à internet também não gostariam de ser monitorados eletronicamente sobre o uso que fazem na rede mundial de computadores, podendo caracterizar a invasão da sua privacidade.

Além disso, a Constituição Federal do nosso país, apenas prevê a responsabilização penal da pessoa jurídica, quanto a crimes ambientais:

> Art. 225. Todos têm direito ao meio ambiente ecologicamente equilibrado, bem de uso comum do povo e essencial à sadia qualidade de vida, impondo-se ao Poder Público e à coletividade o dever de defendê-lo e preservá-lo para as presentes e futuras gerações.
> § 3º. As condutas e atividades consideradas lesivas ao meio ambiente sujeitarão os infratores, pessoas físicas ou jurídicas, a sanções penais e administrativas, independentemente da obrigação de reparar os danos causados.

Isso quer dizer que, para ser possível a responsabilização penal de provedores, teria que haver uma alteração da Constituição Federal.

Portanto, esse não é o caminho mais adequado para se coibir os crimes praticados na forma digital, pois, não atinge os criminosos, mas atinge os facilitadores dos crimes virtuais. Entretanto, uma possibilidade eficiente é exigir dos provedores de

acesso à rede de computadores mundial, o controle de acesso dos seus usuários, mas não caberia a penalização dos provedores, há menos que estes desobedeçam a determinação de controlar o conteúdo exposto por seus clientes-usuários do provedor de acesso à internet.

4.2 AUTOCOLOCAÇÃO DA VÍTIMA EM PERIGO

Na sociedade moderna, a vítima sempre teve uma conduta passiva nos crimes digitais, sendo esta a parte que sofre os danos decorrentes dos ilícitos informáticos. E os riscos de um ataque virtual são inerentes às sociedades mais complexas, modernizadas, necessárias ao desenvolvimento.

Entretanto, pode-se considerar que há riscos permitidos e riscos não permitidos. E pode-se dizer que quando há um risco que é permitido, não há que se falar em ilícitos penais, porque são riscos que trazem benefício genérico para a sociedade e aceitos por esta. Mas o risco não permitido, esse sim, não é aceito pela sociedade.

Porém, na Alemanha, década de 80, houve um debate interessante sobre o papel da vítima de tais delitos, surgindo a tese da autocolocação da vítima em perigo. Tratava-se da análise do comportamento da vítima em relação ao delito, chegando a conclusões inusitadas, como a teoria de que, nos casos de autocolocação da vítima em risco, os sujeitos ativos dos crimes virtuais não teriam a imputação dos ilícitos contra si, uma vez que as vítimas teriam criado o perigo para si mesmas, até mesmo com o desconhecimento dos recursos do mundo virtual. Essa tese prega uma diminuição da culpabilidade do autor do delito, já que a vítima teria agido de forma a permitir o risco, e portanto, facilitar o delito. Esta tese ainda não é consenso, mas já vem sendo aplicada na doutrina alemã há algum tempo (CRESPO, 2011).

Todavia, no Brasil é preciso ter cuidado com as interpretações, podendo levar à conclusões de atribuir responsabilidade à vítima ao se colocar em risco. Mas, a questão é: até que ponto poderia-se responsabilizar parcialmente a vítima pelo risco que se permitiu, e até que ponto isso estaria incluindo um consentimento para um resultado lesivo? (CRESPO, 2011).

Para se chegar ao ponto de responsabilizar também a vítima por ter colaborado, de alguma forma, com o ilícito informático, precisa ser analisado conjuntamente com aspectos subjetivos dos usuários, já que alguns deles nem sabem o que estão fazendo, navegando na internet sem estar devidamente protegido por programas para este fim (como firewall, antivírus), flexibilizando a segurança do computador, ou permitindo a entrada de um invasor, etc. Também não se pode deixar de mencionar aqueles usuários que abrem todos os tipos de e-mail recebidos, ou os que sempre clicam em tudo e em qualquer conteúdo.

Assim sendo, tratam-se de interpretações muito frágeis, que abrem margem para a responsabilização da vítima que se colocasse em perigo. E não é isso que se busca, e sim uma mensuração mais justa da pena do agente ativo do delito.

Aliás, isso é previsto no Código Penal brasileiro, no art. 59, quando se refere ao comportamento da vítima, que deve ser considerado pelo juiz, quando da aplicação da pena:

> Art. 59 - O juiz, atendendo à culpabilidade, aos antecedentes, à conduta social, à personalidade do agente, aos motivos, às circunstâncias e conseqüências do crime, bem como ao comportamento da vítima, estabelecerá, conforme seja necessário e suficiente para reprovação e prevenção do crime:
> I – as penas aplicáveis dentre as cominadas;
> II - a quantidade de pena aplicável, dentro dos limites previstos;
> III – o regime inicial de cumprimento da pena privativa de liberdade;
> IV- a substituição da pena privativa da liberdade aplicada, por outra espécie de pena, se cabível.

Reafirmando, é preciso ter muita cautela na interpretação dessa teoria, especialmente tratando-se do Brasil, onde a sociedade virtual detém pouco conhecimento informático, limitando-se, em sua grande maioria, meramente ao uso dos serviços oferecidos e disponíveis, podendo ser considerados até como “analfabetos digitais”, e porque, isso exigiria uma maior conscientização por parte dos usuários da grande rede mundial de computadores. Portanto, é preciso distinguir claramente a situação de uma pessoa que sofre as conseqüências do crime, por meio de atitudes no mundo virtual que a coloquem em risco, para aquela pessoa que contribui efetivamente para que o crime aconteça. A necessidade desse tipo de proteção penal tem que ser justificada pela necessidade de proteção do bem jurídico em questão.

4.3 RESPONSABILIDADE PENAL DOS PROVEDORES

O serviço de provedor de acesso à internet consiste em um serviço em que é disponibilizado ao usuário meios que permitam a conexão de um computador à internet.

Por ser de difícil identificação do autor dos crimes digitais, é que surgiu uma polêmica a respeito da possibilidade de apontar um substituto a ser responsabilizado, no âmbito penal, pela prática de tais delitos virtuais. São as pessoas jurídicas provedoras de acesso à rede mundial de computadores, que, de alguma forma, favoreceu o crime praticado, por meio do serviço de disponibilização do ambiente virtual. (CRESPO, 2011).

Ocorre que, muitas vezes, os provedores de acesso á internet são omissos, pois têm conhecimento da prática abusiva, ou ilícita, por meio do próprio serviço que presta, ou têm conhecimento do conteúdo exibido pelos seus usuários, e nada faz. Mas, também há situações em que os provedores não detêm o conhecimento do conteúdo ilícito que os usuários possuem dentro de seus computadores pessoais. E os usuários de provedores de acesso à internet também não gostariam de ser monitorados eletronicamente sobre o uso que fazem na rede mundial de computadores, podendo caracterizar a invasão da sua privacidade.

Além disso, a Constituição Federal do nosso país, apenas prevê a responsabilização penal da pessoa jurídica, quanto a crimes ambientais:

> Art. 225. Todos têm direito ao meio ambiente ecologicamente equilibrado, bem de uso comum do povo e essencial à sadia qualidade de vida, impondo-se ao Poder Público e à coletividade o dever de defendê-lo e preservá-lo para as presentes e futuras gerações.
> § 3º. As condutas e atividades consideradas lesivas ao meio ambiente sujeitarão os infratores, pessoas físicas ou jurídicas, a sanções penais e administrativas, independentemente da obrigação de reparar os danos causados.

Isso quer dizer que, para ser possível a responsabilização penal de provedores, teria que haver uma alteração da Constituição Federal.

Portanto, esse não é o caminho mais adequado para se coibir os crimes praticados na forma digital, pois, não atinge os criminosos, mas atinge os facilitadores dos crimes virtuais. Entretanto, uma possibilidade eficiente é exigir dos provedores de acesso à rede de computadores mundial, o controle de acesso dos seus usuários,

mas não caberia a penalização dos provedores, há menos que estes desobedeçam a determinação de controlar o conteúdo exposto por seus clientes-usuários do provedor de acesso à internet.

4.4 CULPABILIDADE

De maneira simplificada é possível afirmar que a culpabilidade repousa em um juízo de reprovação social diante da lesão a um bem jurídico penal.

Para Paulo Queiroz (2006, p. 151): “A culpabilidade constitui as condições subjetivas que devem decorrer para que seu autor seja punido, pois, do contrário, isto é, se não culpável, não sofrerá pena alguma, sendo absolvido.”.

Rogério Greco (2009, p.381), citando Welzel, conceitua o instituto da seguinte maneira:

> Culpabilidade é o juízo de reprovação pessoal que se realiza sobre a conduta típica e ilícita praticada pelo agente. Nas lições de Welzel, “culpabilidade é a ‘reprovabilidade’ da configuração da vontade. Somente aquilo a respeito do qual o homem pode algo voluntariamente lhe pode ser reprovado como culpabilidade”.

A análise do elemento culpabilidade adquire contornos curiosos ao ser aplicada ao “mundo dos crimes virtuais”, isto porque cada vez mais surgem praticas de conduta reprovaveis, que, de alguma maneira, trazem conflitos sociais e juizos de censura, por abarcarem em si a ideia de culpabilidade, e, consequentemente, buscam no direito penal a devida regulação. Entretanto, nessa seara, embora formada a ideia de culpabilidade diante de várias práticas, reside a particularidade de haver, muitas vezes, imensa dificuldade em indentificar e punir o infrator, não só diante da questão da atipicidade, como do ambiente virtual em que se dão os crimes.

A capacidade de culpabilidade ou a imputabilidade como pressuposto da culpabilidade é uma questão bastante polêmica porque há uma grande dificuldade de se identificar o autor do ato das transações eletrônicas ilícitas. E no que diz respeito à responsabilidade civil da vítima de tal ato criminoso, existe também a possibilidade de demonstrar que houve a culpa *in vigilando*, por ausência do dever de cuidado na guarda da senha de acesso, etc (COSTA, 2011).

A privacidade informática é uma preocupação mundial, pois com os avanços tecnológicos, há uma vulnerabilidade muito grande quanto ao grampo de comunicações, cópias e gravações não autorizadas de mensagens, fotos, dados, documentos e informações em geral, enviadas eletronicamente, dada a dificuldade probatória, a desconfiança da vítima na eficácia do sistema jurídico, na aparência de legalidade no comportamento do agente e a possibilidade de manter o delito no anonimato (DRUMMOND, 2003).

Como se vê, na configuração atual, sobretudo, da realidade pátria, a impunidade constantemente impera quando se trata de crimes de informática, tornando a sociedade tecnológica frequentemente exposta a riscos muitas vezes irreparáveis.

5 CONVENÇÃO DE BUDAPESTE E DIREITO COMPARADO

Os problemas referentes à criminalidade digital e aos agentes delituosos existentes nos mais variados ordenamentos jurídicos dos países, como também a sua tipificação e a devida punição, têm sido discutidos há alguns anos nos Fóruns Internacionais.

Somente em 1970 ocorreu alguma reação legislativa sobre o assunto, tendo os Estados Unidos como o pioneiro dentre os demais países, na regulamentação penal sobre “abuso informático”. Em 1978 foi proposto o projeto de lei *Ribicoff Bill*, sobre crimes informáticos, e apesar de não ter sido aprovado, serviu de modelo para elaboração de legislações dos Estados norte-americanos. O mencionado projeto conferia valor econômico aos bancos de dados e aos softwares.

Entretanto, foi na década de 80 que as entidades governamentais e a comunidade científica constataram o desenvolvimento dos crimes digitais, mostrando-se um problema de índole internacional, especialmente devido à possibilidade de acesso remoto aos sistemas informáticos, ou seja, devido à possibilidade de se controlar à distância um computador alheio. (CRESPO, 2011).

A Convenção de Budapeste, também conhecida como Convenção sobre o Cibercrime, é o principal Tratado Internacional de Direito Penal e Processual Penal, visando definir, de forma equilibrada entre os países, os crimes praticados por meio informático e as formas de persecução penal destes, no âmbito do Conselho da Europa.

Desta maneira, o objetivo da Convenção é adaptar fundamentos relativos ao Direito Penal dos países subscritores, para então, definir as ações que possibilitem a persecução penal no âmbito internacional, assim como a composição de critérios para uma cooperação internacional rápida e eficiente.

Assim, a Convenção de Budapeste busca a harmonização das legislações, de forma que se evite que um crime praticado em determinado país, seja também praticado em outro país, e desta maneira, facilite a persecução penal. (CRESPO, 2011).

Neste sentido, o Protocolo Adicional à Convenção de Budapeste sobre o Cibercrime, também buscou harmonizar disposições que visam o combate a crimes. Entretanto,

os crimes referidos por este Protocolo são mais específicos, pois tratam-se de atos de racismo e xenofobia que sejam praticados por meio de sistemas informáticos, de forma que, na composição do Protocolo Adicional citado, foram consideradas as noções básicas de direitos humanos, especialmente ressaltando o valor à liberdade, ao fato de todos nascerem livres e iguais em direitos e em dignidade, e priorizando a aplicação plena e efetiva de tais direitos.

Dentre as disposições do Protocolo Adicional à Convenção de Budapeste, há previsão de que os países subscritos deverão criar legislações que busquem punir a distribuição de qualquer material racista e xenófobo ao público através de sistemas digitais.

Por fim, o aludido Protocolo, ainda impõe aos países subscritos a ele, que em suas legislações haja previsão de punição à condutas que aprovem ou justifiquem atos que constituam genocídio ou crimes contra a humanidade, de acordo com as definições do Direito Internacional.

Vê-se, portanto, que o Protocolo Adicional à Convenção do Cibercrime busca reforçar os mecanismos de combate aos crimes digitais impróprios, ou seja, aqueles crimes praticados através de meios tecnológicos, mas que afinal, atingem bens jurídicos já protegidos pelas legislações em geral. (CRESPO, 2011).

Diante da constante evolução tecnolócia que cresce em todo o mundo, e que vem trazendo a reboque os crimes da era digital faz-se necessário, para enriquecer o presente trabalho monográfico, ter noção, ainda que brevemente, da situação do ordenamento jurídico de alguns países.

Assim, verifica-se a existência de legislação específica em países como, Portugal, Itália, Estados Unidos da América, Inglaterra, com condutas devidamente tipificadas acerca dos crimes digitais.

Alguns, dentre os países citados, já possuem legislação específica sobre estes crimes tecnológicos, e outros, inseriram recentes modificações em suas legislações existentes, com a finalidade de regulamentar esta nova modalidade de delitos.

12.1 PORTUGAL

Portugal dispõe de legislação específica para regular a criminalidade informática desde o ano de 1991 e esta vem sendo aplicada regularmente pelos tribunais desde então. Trata-se da Lei nº109/91, denominada Lei da Criminalidade Informática.

O debate acerca dos crimes informáticos encontra-se sempre presente em Portugal, principalmente quanto à possibilidade do anonimato dos sujeitos ativos do crime pela rede internacional de computadores, revelando ser este um país mais avançado que o Brasil no que diz respeito à legislação aplicável ao tema.

O Código Penal Português, decreto-lei nº 48/95, também demonstra preocupação, ao prever dois tipos penais informáticos no seu texto legislativo. O primeiro deles, previsto no capítulo dos crimes contra a reserva da vida privada refere-se à modalidade de devassa por meio da informática.

O tipo penal acima citado, volta-se à tutela dos dados, mas não o faz indiscriminadamente, restringindo-se àqueles referentes às convicções políticas, religiosas ou filosóficas, à filiação partidária ou sindical, à vida privada e a origem étnica.

Carla Rodrigues Araújo de Castro (2003, p. 156) ensina, ainda, que o crime de devassa por meio de informática é público, não dependendo de queixa ou participação do ofendido. (CASTRO, 2003).

Eis o teor do art. 193 do Código Penal português:

> Art. 193º. Devassa por meio de informática.
> 1. Quem criar, mantiver ou utilizar ficheiro automatizado de dados individualmente identificáveis e referentes a convicções políticas, religiosas ou filosóficas, à filiação partidária ou sindical, à vida privada, ou a origem étnica, é punido com pena de prisão até 2 anos ou com pena de multa até 240 dias.
> 2. A tentativa é punível.

Outro tipo de delito previsto no Codigo Penal Português sobre crimes de informática, consta do seu artigo 221, infracitado, cujo capítulo é destinado aos crimes contra o patrimonio em geral, e dispõe sobre a burla informática e nas comunicações.

Trata-se de causa atenuante da pena, devendo ser aplicado, segundo Castro (203, p.157), quando o agente restitui o bem ou repara o dano causado.

> Art. 221. Burla informática e nas comunicações.
> 1. Quem, com intenção de obter para si ou para terceiro enriquecimento ilegítimo causar a outra pessoa prejuízo patrimonial, interferindo no resultado de tratamento de dados ou mediante estruturação incorrecta de programa informático, utilização incorrecta ou incompleta de dados, utilização de dados sem autorização ou intervenção por qualquer outro modo não autorizado no processamento, é punido com pena de prisão até 3 anos ou com pena de multa.
> 2. A mesma pena é aplicável a quem, com intenção de obter para si ou para terceiro um benefício ilegítimo, causar a outrem prejuízo patrimonial, usando programas, dispositivos elecrónicos ou outros meios que, separadamente ou em conjunto, se destinem a diminuir, alterar ou impedir, total ou parcialmente, o normal funcionamento ou exploração de serviços de telecomunicações.
> 3. A tentativa é punível.
> 4. O procedimento criminal depende de queixa.
> 5. Se o prejuízo for:
>   a) de valor elevado, o agente é punido com pena de prisão até 5 anos ou com pen de multa até 600 dias.
>   b) De valor consideravelmente elevado, o agente será punido com pena de prisão de 2 a 8 anos.
> 6. É corespondentemente aplicável o disposto no artigo 206º.

Outro aspecto que merece ressalva é a definição de vários conceitos informáticos pela Lei de nº 109/91, tendo em vista que nem todos os profissionais de Direito conhecem os termos específicos pertinentes à ciência informática.

Há ainda que comentar sobre a responsabilidade penal das pessoas coletivas e equiparadas, que ocorre quando o crime for praticado em nome ou no interesse da pessoa coletiva, sendo as principais penas aplicáveis: admoestação, multa e dissolução; e as penas acessórias são: perda de bens, caução de boa conduta, interdição temporária do exercício de certas atividades ou profissões, encerramento temporário do estabelecimento, encerramento definitivo do estabelecimento e publicidade da decisão condenatória. (CASTRO, 2003).

Vale descatar, a título de obter uma visão geral, que o legislador português previu 6 tipos penais quanto aos delitos informáticos: falsidade informática, danos relativos a dados ou programas informáticos, sabotagem informática, acesso ilegítimo, acesso ilegítimo, interceptação ilegítima e reprodução ilegítima de programa protegido.

12.2 ITÁLIA

O Código Penal Italiano não ignorou os crimes informáticos, e seu texto, de alguma maneira não muito específica, trata dos delitos relacionados à informática.

As alterações do Legislação Penal Italiana datam de 1993, e incluem 6 tipos penais informáticos: sabotagem, acesso ilegal, violação de segredo informático e do sigilo, falsificações, fraude informática e violação dos direitos do autor concernentes ao software. Após a mencionada alteração, de forma geral, portanto, o país passou a contar com quinze tipos penais previstos referentes ao tema.

Destaca-se aqui o crime de sabotagem que possui 2 vertentes: o ataque ao funcionamento do sistema informático, sendo que se esse sistema for público ou privado, caracterizam crimes de gravidades diversas, e portanto, aplicação de penas diversas. Ressalte-se que a ofensa mais grave é quando tratar-se de sistema de utilidade pública, onde a pena é de 1 a 4 anos, enquanto que a lesão a sistema informático privado tem pena variável de 3 meses a 3 anos. (CASTRO, 2003).

O envio de vírus também é tipo penal previsto no Código Penal italiano, sendo punível a conduta do agente que que difunde programa informático com a intenção de provocar danos nos dados, programas informáticos ou telemáticos de computadores de terceiros, ou que venha a interromper seu funcionamento de forma total ou parcial.

Também é punível a conduta do agente que acessa ilegalmente um sistema informático ou telemático (hacker), e da mesma forma, a conduta de quem dissemina ilegalmente esses códigos de acessos, palavras-chaves (senhas) ou outros meios que permitam acesso à sistemas de informática dotados de proteção.

Vale salientar, por fim, que o Código Penal Italiano regulou, especificamente, a conduta de utilização abusiva de cartões magnéticos, o que facilitou, de maneira geral, a punição dos agentes autores destes delitos, estabelecendo uma maior sensação de seguraça na utilização desta tecnologia.

12.3 ESTADOS UNIDOS

Os Estados Unidos estão bem à frente do Brasil em matéria de legislação sobre crimes informáticos, uma vez que dispõem de várias leis específicas sobre a informática. Cada Estado norte-americano pode criar seus estatutos penais, dentre os quais, alguns mostram-se verdadeiros Códigos.

Uma destas leis específicas mais importantes, é a Lei 18 U.S.C.1030, que conceitua os termos técnicos relacionados à informática e disciplina a fraude e atividades relacionadas a computadores, prevendo penas de multa e de encarceramento.

A conduta caracterizada como crime, de acordo com a lei citada, é o acesso a computador não autorizado ou excedendo autorização, e com isso, vir a obter ilícitamente, informação de registro financeiro de instituição financeira ou informações do departamento e agências dos Estados Unidos ou computador não exclusivo, mas utilizado pelo Governo. (CASTRO, 2003).

Além disso, a legislação americana inclui como conduta punível a prática de transmitir um programa de computador, informação, código ou comando, e com isso provocar dano a computador protegido, assim como a conduta que tenha intenção de extorquir dinheiro ou algo de valor, através da ameaça de dano a computador protegido de pessoa, firma, associação, instituição educacional, instituição financeira, entidade de governo ou outra entidade legal.

Ainda sim, recente pesquisa feita pela Hewlett-Packard – HP, com companhias norte-americanas, publicada pela Revista Exame Info, aponta o crescimento de crimes digitais, indicando que no ano de 2011 foram detectados 72 crimes por semana às empresas, enquanto que 50 ataques semanais aconteceram no ano de 2010 nos Estados Unidos.

Os dados revelam ainda, que o custo das empresas americanas para solucionar problemas devidos a ataques em seus sistemas quase dobrou nos últimos três anos, e demonstram que o custo médio anual causado pelas falhas de segurança digital foi de 8,9 milhões de dólares – 38% maior do que em 2010.

Constam entre as perdas, casos como roubo de informações e interrupção de negócios que continuam a representar os custos mais altos. A informação é de que, anualmente, os roubos representam 44% dos gastos externos. Já a interrupção dos negócios ou perda de produtividade atualmente são 30% do dinheiro gasto.

O estudo mostra ainda, que o custo médio para solucionar um ataque em 24 dias foi de 590 mil dólares. Vale lembrar que, o gasto pode ser maior se resolvido em mais tempo. Por fim, tem-se que aquelas empresas que destinaram maiores investimentos à segurança digital alcançaram uma economia de 1,6 milhão por ano.

12.4 INGLATERRA

A Inglaterra possui um projeto de lei bem avançado em termos de legislação de delitos informáticos, em que prevê o rastreamento do tráfico de informações na internet pelos serviços de segurança do país. E de acordo com este projeto de lei, os provedores de acesso à internet serão obrigados a permitir acesso irrestrito da polícia às informações sobre seus usuários. (CASTRO, 2003).

A lei inglesa de crimes informáticos em vigor, conhecida por Computer Misuse Act, elenca, dentre outros crimes informáticos, a obtenção de acesso não autorizado a programa ou informação.

Entretanto, fica caracterizada a excludente de responsabilidade, sempre que o agente obtem informação, sem a intenção de violação do sistema alheio, ou a modificação de informações de computador alheio culposa. Também está tipificado na legislação inglesa o acesso a computador utilizado como meio para execução de outro delito, chegando até mesmo a punir atos preparatórios.

Em artigo a respeito das questões técnicas que dificultam condenações por crimes cometidos pela internet, o Juiz de Direito Demócrito Reinaldo Filho (32a. Vara Cível do Recife) cita um julgamento recente, realizado com base na lei inglesa, demonstrando que a dificuldade em julgar tais crimes atinge também aquele país. O Magistrado relata:

> Num dos casos mais famosos, julgado por uma corte da Inglaterra no início de outubro passado, o réu Aaron Caffrey (um adolescente de 19 anos) foi absolvido da acusação de ter atacado o servidor de uma empresa. Denunciado com base na lei inglesa de crimes informáticos (o Computer Misuse Act), ele alegou que seu computador foi tomado por um vírus do tipo trojan e, dessa forma, utilizado remotamente por um terceiro para o cometimento do crime. Muito embora especialistas tenham confirmado não terem encontrado sinais de vírus no computador dele, o Júri terminou por inocentá-lo – o réu alegou também que o vírus foi programado para se auto-destruir após realizar a operação. Esse foi apenas um de um total de três casos onde a alegação de vírus trojan teve sucesso (para os réus). Os dois anteriores estavam relacionados a acusações de pedofilia; os réus foram acusados de fazer downloading de pornografia infantil. Os seus advogados também sustentaram a tese de que os computadores foram “seqüestrados” por um vírus colocado por outra pessoa.

O caso ilustrado serve para demonstrar que as questões relacionadas à informática ainda figuram como desafios a serem enfrentados e regulados devidamente pelo

direito, sob pena de tais crimes permanecerem impunes, mesmo em se tratando de países que já possuem alguma legislação específica sobre o tema.

12.5 FRANÇA

Habitualmente, a França não apresentava tipificação penal destinada a punir os crimes informáticos, até o ano de 1988, quando houve a modificaçao do Código Penal Francês, introduzindo um capítulo especial destinado a coibir atentados contra sistemas informáticos.

Essa alteração do Código Francês também previu a punição a condutas específicas, como a conduta de acessar ou manter-se de forma fraudulenta, em um sistema de tratamento automático de dados. A pena pode ser aumentada, se, através destas condutas ocorrer a supressão ou modificação de dados contidos no sistema, ou ainda, ocorra qualquer alteração no funcionamento de tal sistema de dados.

Por sua vez, a Legislação Penal Francesa tipifica uma das condutas mais disseminadas no mundo contemporâneo. Trata-se da conduta de introduzir vírus em sistema informático de forma dolosa. Além desta, a responsabilidade penal das pessoas jurídicas foi contemplada também na alteração penal de 1988, e prevê desde a interdição do exercício das atividades, até a dissolução desta.

Vale dizer, por fim, que a França tem uma das leis pioneiras sobre criminalidade digital e que as condutas tipificadas como crimes informáticos respeitam as imposições da Convenção de Budapeste sobre o Cibercrime, dentre outras orientaçoões internacionais (CRESPO, 2011).

12.6 OUTROS PAÍSES

O Chile figura como país pioneiro na América Latina com relação à iniciativa de modernizar seu aparato legal frente às nuances do crime digital. Crespo destaca que a Lei nº 19.223/93 tratou de tipos penais que versam sobre crimes atentatórios a sistemas de informação. Tal dispositivo legal, esclarece o Autor (2011, p.150), “visa

proteger os bens jurídicos da informação e seus componentes funcionas, também atendendo, ao menos em parte, às diretrizes internacionais".

Na Argentina, segundo Castro (2003, p.162), existe um programa de uso de assinaturas digitais no âmbito da Administração Pública, para atos internos que não produzam efeitos jurídicos, instituido pelo Decreto 427/98.

Mas já há previsão de um projeto de lei sobre delitos informáticos, tratando do acesso ilegítimo a dados, dano informático e fraude informática, entre outros tipos. (CASTRO, 2003).

Crespo (2011, p.150) lembra que "o sistema penal argentino, no que tange aos crimes digitais, parte da regulação do comércio eletrônico para dele extrair condutas ilícitas relevantes".

Houve, entretanto, alteração, do Código Penal, através da Lei nº 26.388/08 com relação aos crimes digitais próprios e impróprios.

No Canadá, os principais tipos de crime considerados, em matéria de delito informático, são as condutas de acesso não autorizado, danos a dados, furto de telecomunicações e violação autoral de software. (CASTRO, 2003).

Crespo (2011, p.136), afirma que "a Constituição espanhola incide na tecnologia, vez que indica a intimidade como bem jurídico protegido". Consta do art.18, parágrafo 4º da Constituição mencionada, que a lei limitará o uso da informática para garantir a honra e a intimidade pessoal e familiar dos cidadãos e o pleno exercicio de seus direitos.

Já o Código Penal Espanhol prevê uma figura específica de delito, o dano informático, que refere-se a uma forma agravada do dano tradicional já conhecido, para as situações de destruição, alteração ou inutilização de dados, programas ou documentos eletrônicos. Outra figura específica é o acesso ilícito a dados considerados como segredos de empresa, sendo de difícil definição do termo segredos de empresa, por não estar conceituado no Código Penal espanhol. (PEREIRA, 2011).

A China, por sua vez, possui normas de controle de conteúdo da Internet, utilizando o argumento de que a rede é utilizada para filtrar segredos de Estado e difundir informações danosas. Portanto, tendo em vista a proteção da segurança de

informações, o acesso às redes informáticas através do uso de computadores é bastante restrito.

6 DOS CRIMES DIGITAIS EM ESPÉCIE

Diante da ausência de legislação penal específica aplicável aos crimes digitais, torna-se necessário utilizar a legislação existente, ou seja, o Código Penal e as Leis Especiais.

Entretanto, essa legislação não é satisfatória nem suficiente, para enquadrar todos os fatos aos tipos penais existentes, o que acaba configurando uma atipicidade de tais fatos, e, por fim, vem a ser um estímulo à prática de crimes face a sua impunidade. Portanto, a elaboração de lei regulando a informática e a internet, interessa a toda a sociedade, e não apenas na seara do Direito Penal, mas também no campo do direito Civil, Comercial, Tributário, e outros mais.

Há uma infinidade de delitos que podem ser praticados pelo uso de sistemas de informática, porém, ao estabelecer os limites deste escrito, é possível afirmar que os crimes contra a honra, a ameaça, interceptação de e-mail, furto, favorecimento à prostituição, apropriação indébita e a divulgação de segredo, encontram-se entre as práticas mais disseminadas por meio digital.

.

6.1 CRIMES CONTRA A HONRA

São crimes contra a honra previstos no Código Penal, a calúnia, injúria e difamação.

> Art. 138. Caluniar alguém, imputando-lhe falsamente fato definido como crime:
> Pena – detenção, de 6 (seis) meses a 2 (dois) anos, e multa.
> Art. 139. Difamar alguém, imputando-lhe fato ofensivo à sua reputação:
> Pena – detenção, de 3 (três) meses a 1 (um) ano, e multa.

O crime de calúnia é aquele que atinge o conceito que outros membros da sociedade têm a respeito do indivíduo, no que diz respeito aos seus atributos morais, éticos, culturais, intelectuais, físicos ou profissionais. Portanto, o crime de calúnia atinge a honra objetiva do sujeito, a reputação do indivíduo. É possível afirmar, em outros termos, que é a percepção de um terceiro sobre as nossas qualidades ou nossos atributos. (BITENCOURT, 2001)

A calúnia e a difamação são muito parecidos, pois ambos lesam a honra objetiva do sujeito, através da imputação de um fato, e consumam-se quando um terceiro ou mais, tomam conhecimento do fato. Entretanto, no crime de calúnia o fato imputado tem que ser falso e definido como crime, ao passo que, na difamação, mesmo o fato sendo verdadeiro, caracteriza-se o crime.

Diante disso, percebe-se que estes crimes, além dos modos tradicionais, também podem ser praticados por meio da internet e do computador, como por exemplo através do facebook ou do twitter, atribuindo um fato ofensivo à honra de alguém, e esse fato poderá ser conhecido por todos aqueles que receberem as mensagens do facebook ou que se utilizarem do twitter. Entretanto, nestas redes sociais há a possibilidade de conversar privativamente, impedindo a visualização por qualquer terceiro. Neste caso, quando as ofensas são dirigidas particularmente ao ofendido, não haverá consumação da infração, pois esta necessita do conhecimento de tal fato por um terceiro.

Por sua vez, o crime de injúria protege a honra subjetiva, sendo que, para sua caracterização basta que o ofendido tome conhecimento do fato. Este delito pode ser praticado por conversas on-line, em sites e também por e-mail.

6.2 AMEAÇA

Ameaça é o crime que consiste em aterrorizar a vítima, mediante promessa de causar-lhe um mal grave e injusto. O artigo 147 do Código Penal Brasileiro protege a liberdade da pessoa relativa ao sentimento de segurança, ao sossego:

> Art. 147. Ameaçar alguém, por palavra, escrito ou gesto, ou qualquer outro meio simbólico, de causar-lhe mal injusto e grave:
> Pena – detenção, de 1 (um) a 6 (seis) meses ou multa.

A prática deste tipo penal é a ameaça, a intimidação do sujeito passivo, que pode ser feita também através de um computador. O sujeito ativo envia um texto contendo uma ameaça para um email, ou mesmo insere um texto num site, facebook, twitter, etc. Não configura o crime de ameaça se esta for falsa, ou seja, se o sujeito estiver fazendo uma brincadeira, pois é preciso que realmente tenha o dolo de ameaçar. A

ameaça tem que ser séria e idônea. Entretanto, a ameaça feita com ódio, com exaltação, no calor da discussão não configura o crime. (CARLA, 2003).

6.3 INTERCEPTAÇÃO DE E-MAIL

Correspondência é a comunicação que se estabelece entre duas ou mais pessoas, ausentes, normalmente por escrito, e que ocorre por meio de cartas, bilhetes, telegramas, e mais recentemente por e-mail. A correspondência tem a garantia de sigilo por previsão constitucional, disposta no artigo 5º, inciso XII, da Constituição Federal.

Deste modo, o e-mail configura-se como espécie de correspondência eletrônica, escrita, entre pessoas ausentes, sendo que há diferença no seu modo de expedição e recebimento, que ocorre por meio da internet.

> Art. 5º, XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;

Além disso, a lei 9.296/96, que regula o artigo 5º, inciso XII, em sua parte final, da Constituição Federal, prevê no seu artigo 10 o seguinte crime:

> Art. 10. Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo de Justiça, sem autorização judicial ou com objetivos não autorizados em lei.
> Pena – Reclusão, de dois a quatro anos, e multa.

Assim, a lei 9.296/96, é especial em relação ao Código Penal Brasileiro, trata dos crimes nas comunicações realizadas por meio da informática, situação em que se adapta mais perfeitamente ao caso. Portanto, legislação pátria protege também o email, embora seja uma comunicação eletrônica, transmitida através do computador, via internet e demais acessórios, também trata-se de uma correspondência. (CASTRO, 2003).

Contudo, o conhecimento do conteúdo de um email, recebido por equívoco, destinado a outra pessoa não pode constituir crime de violação de correspondência, por total ausência de dolo.

Fernando Célio de Brito Nogueira se contrapõe a tal posição, oportunidade em que relata:

> A menssagem de correio eletrônico poderá ser equiparada à correspondencia fechada prevista no tipo penal? A resposta é negativa, pois o conceito de correspondencia nos é dado pela Lei nº 6.538/78, em seu art. 47 (toda comunicação pessoa a pessoa, por meio de carta, através da via postal ou telegrama). Além disso, o Código Penal referiu-se à correspondencia fechada, envelopada ou embrulhada, lacrada, e não a uma menssagem transmitida por meio de computadores ou, como se diria hoje, pela telemática (uso da telefonia + informática), meio de veiculação da internet entre nós. (NOGUEIRA, 2000).

Para o autor supramencionado, a Lei Federal de nº 9.296/96, artigo 10, o núcleo deste tipo penal é interceptar, obstruir, impedir, e sendo assim, não teria o sentido de devassar, conhecer, violar o sigilo, mas o sentido correto e pretendido, seria o de impedir a passagem, cortar, deter, interromper o curso da correspondência.

Como o Direito Penal Brasileiro não admite crime por analogia, mas apenas admite a analogia para beneficiar o agente, não seria cabível punir ou agravar a punição, enquanto não sobrevier norma legal específica, restando nos casos de violação por e-mail a configuração da atipicidade penal. (NOGUEIRA, 2000).

> Art. 151. Devassar, indevidamente o conteúdo de correspondência fechada, dirigida a outrem:
> Pena – Detenção, de 1 a 6 meses, ou multa.

Apesar das posições doutrinárias divergentes, acentua-se a previsão constitucional de que a obtenção de uma correspondência particular, contendo uma informação privada, sem a devida autorização, é um atentado contra a liberdade individual e à garantia do sigilo das comunicações, vedado pela Lei Maior.

Quanto ao Código Penal, o tipo previsto é devassar, ou seja, termo mais amplo do que violar. Portanto, a devassa, de modo geral, é vedada pelo ordenamento jurídico, mesmo que não se viole a correspondência, mantendo-a íntegra, ou que não se tenha conhecimento do conteúdo, contudo, seu acesso obtido indevidamente é combatido na legislação penal pátria.

Desse modo, urge a necessidade de criação de nova legislação, com novos tipos penais tendentes a reprimir a criminalidade moderna, ou seja, a conduta ilícita praticada por meio da informática, tendo em vista que as normas existentes nosso Código Penal de 1940, já não protege de forma plena.

6.4 FURTO

O crime de furto no mundo virtual pode ser praticado contra o sistema de infomática ou através deste. O furto do próprio computador ou seus acessórios é um crime contra o sistema de informática, ao passo que, a utilização do computador como um instrumento para a prática do ilícito é crime praticado através do sistema de informática, como ocorre na transferência indevida de valores de uma instituição financeira para a conta corrente do agente, pelo meio informático. É imprescindível que o objeto do furto tenha algum valor econômico para a configuração do delito, de forma que, na subtração de um simples arquivo sem valor, não há que se falar em crime. (CASTRO, 2003).

> Art. 155. Subtrair, para si ou para outrem, coisa alheia móvel:
> Pena – Reclusão, de 1 a 4 anos, e multa.
> § 1º - A pena aumenta-se de um terço, se o crime é praticado durante o repouso noturno.
> § 2º - Se o criminoso é primário, e é de pequeno valor a coisa furtada, o juiz pode substituir a pena de reclusão pela de detenção, diminuí-la de um a dois terços, ou aplicar somente a pena de multa.
> § 3º - Equipara-se à coisa móvel a energia elétrica ou qualquer outra que tenha valor econômico.
> § 4º - A pena é de reclusão de dois a oito anos, e multa, se o crime é cometido:
> I – com destruição ou rompimento de obstáculo à subtração da coisa;
> II – com abuso de confiança, ou mediante fraude, escalada ou destreza;
> III – com emprego de chave falsa;
> IV – mediante concurso de duas ou mais pessoas.
> § 5º - A pena é de reclusão de três a oito anos, se a subtração for de veículo automotor que venha a ser transportado para outro Estado ou para o exterior.

Pode ser causa de aumento da pena, também para crimes informáticos, o furto praticado durante o repouso noturno. Aplica-se tanto no furto de um notebook na residência do sujeito passivo, quanto na exploração do computador como instrumento do crime.

Da mesma forma, o abuso de confiança pode ser empregado nos delitos informáticos, como quando o sujeito ativo conhece as senhas de acesso ao sistema informático em razão da relação de amizade com o ofendido, e furta arquivos particulares de valor econômico.

Entretanto, não são todas as hipóteses de furto qualificado que poderão ser aplicadas a estes crimes. Contudo, o concurso de pessoas aplica-se a tais crimes,

quando o sujeito ativo do crime é composto por duas ou mais pessoas, como na situação em que dois agentes penetram no sistema de uma instituição financeira e transfere uma importância em dinheiro para um deles, ou um terceiro.

Não é possível a aplicação do furto de tempo ou furto de uso aos delitos informáticos, como na situação em que o agente utiliza o equipamento de forma abusiva e não autorizada pelo proprietário. Deste modo, tanto o abuso na utilização do computador enquanto equipamento (hardware), quanto a utilização sem autorização na rede de internet do proprietário, não são previstos na legislação, não configurando crime. (CASTRO, 2003).

6.5 FAVORECIMENTO DA PROSTITUIÇÃO

Prostituição é a troca de favores sexuais por valores em dinheiro ou outra recompensa patrimonial. Pode ser praticada tanto por homens quanto por mulheres. A prostituição praticada com o consentimento não caracteriza crime, entretanto o Código Penal Brasileiro combate a conduta daquele que favorece ou se aproveita financeiramente da prostituição alheia.

As condutas tipificadas para o favorecimento da prostituição são três: induzir ou atrair, facilitar e impedir que alguém a abandone a prostituição. Desta forma, é possível a prática de induzir ou atrair para a prostituição por meio da internet, quando o sujeito mostra as vantagens e benefícios da atividade, através de e–mail ou conversas on-line, oferecendo o meio propício para o exercício da atividade. (CASTRO, 2003).

A conduta denominada de facilitação da prostituição, significa oferecer auxílio, e também pode ser praticada por meio informático, quando o agente fornece informações à vítima, por e-mail ou por conversas on-line, sobre os locais de prostituição, os preços praticados com a atividade e sobre a segurança pessoal da prostituta. Também pode-se conciliar as duas práticas ilícitas num site ou num blog próprios, construído para atrair vítimas para a atividade, divulgando os valores recebidos pelas prostitutas por dia, relatos detalhados do trabalho oferecido e contatos telefônicos.

> Art. 228. Induzir ou atrair alguém à prostituição, facilitá-la ou impedir que alguém a abandone:
> Pena – Reclusão, de 2 a 5 anos .

Todavia, a única conduta que não pode ser praticada pelo meio digital é a de impedir que a vítima abandone a prostituição.

Por estas e outras razões, a internet é o meio mais propício para o favorecimento da prostituição, facilitando a conuduta por ser anônimo e impessoal, de baixo custo de manutenção, e principalmente, pela rapidez da comunicação.

6.6 APROPRIAÇÃO INDÉBITA

A previsão do crime de apropriação indébita está tipificda no artigo 168 do Código Penal:

> Art. 168. Apropriar-se de coisa alheia móvel, de que tem a posse ou detenção:
> Pena – Reclusção, de 1 a 4 anos e multa.
> 1º A pena é aumentada de um terço, quando o agente recebeu a coisa:
> I – em depósito necessário
> II – na qualidade de tutor, curador, síndico, liquidatário, inventariante, testamenteiro ou depositário judicial:
> III – em razão de ofício, emprego ou profissão.

A apropriação indébita ocorre quando o sujeito do delito transforma a posse legítima de um bem alheio, em posse ilegítima, ou seja, quando a passa passa a possuir a coisa como sua, de sua propriedade.

Isso acontece em relação a crimes informáticos, quando um funcionário de uma empresa, leva um equipamento de informática, pode ser um scanner, um computador ou uma impressora para casa e passa a utilizá-lo como seu, enquanto deveria fazer uso apenas no exercício de sua função, configurando, desta forma, o ilícito da apropriação indébita.

6.7 DIVULGAÇÃO DE SEGREDO

Trata-se de crime que se consuma apenas dolosamente podendo se configurar de duas maneiras, tendo a Administração Pública como vítima, ou tendo como

acupante do pólo passivo o indíviduo, ou seja, qualquer pessoa. Nos dois casos é prevista a punição de quem coleta a informação e divulga de forma danosa.

Sobre a prática em análise dispõe o art. 153 do Código Penal brasileiro:

> Art. 153. Divulgar alguém, sem justa causa, conteúdo de documento particular ou de correspondência confidencial, de que é destinatário ou detentor, e cuja divulgação possa produzir dano a outrem.
> Pena – Detenção, de 1 a 6 meses, ou multa.
> § 1º - 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:
> Pena – detenção de um a quatro anos, e multa.
> § 1º - Somente se procede mediante representação.
> § 2º - Quando resultar prejuízo para a Administração Pública, a ação penal será incondicionada.

Neste caso tem-se a inviolabilidade dos segredos da vítima e da Administração Pública como bem jurídico protegido. E, o dispositivo legal aponta que o crime pode ser praticado por meio da informática, uma vez que as informações podem estar dispostas em banco de dados da Administração Pública, em que o uso do computador será imprescindível para a prática ilícita, e divulgar o segredo.

Nesta situação somente admite-se a modalidade dolosa do crime de divulgação de segredo.

7 PROPOSTAS LEGISLATIVAS

A sociedade contemporânea traz constantes desafios aos doutrinadores, legisladores e operadores do direito, diante da enxurrada de condutas nocivas ao convívio social, mas que não configuram ilícito penal. Ao pretender criar novos tipos penais, é preciso muito cuidado com a incriminção indistinta de condutas, que poderiam ser objeto de políticas sociais nas áreas Civil e Administrativa, deixando o Direito Penal como *ultima ratio*.

Não se pode ignorar que os avanços da tecnologia na sociedade atual vieram para ficar. A sociedade da informação é uma realidade e as pessoas que a compõem estão cada vez mais informatizadas e dependentes dos computadores. E para uma nova realidade, faz-se necessário uma nova regulação das condutas.

Desta forma, verifica-se a real necessidade de tipificação de condutas que caracterizam ilícitos informáticos, seja através da modificação da legislação existente ou da criação de novas legislações diante do novo mundo globalizado. Com esta intenção, diversos projetos de lei estão sendo criados, visando a criminalização dos novos comportamentos advindos da era digital, a fim de redefinir um novo perfil de comportamento destes indivíduos e seus grupos sociais. Todavia, não se pode admitir que eventuais propostas legislativas venham a ignorar os princípios constitucionais e penais.

Entretanto, antes da criação de novas tipificações penais, torna-se necessário tentar adequar as novas condutas às já tipificadas em nossa legislação penal, visto que, o nosso Código Penal já é hábil a punir muitas destas condutas praticadas com o uso da tecnologia. (CRESPO, 2011).

Assim, os inujstos penais em que apenas o *modus operandi* é novo, o Direito Penal está, apto a punir com sua legislação existente, como nos crimes contra a honra, crimes econômicos e muitos outros.

Dessa forma, temos os crimes praticados com a presença da informática, que ofendem os bens jurídicos já tradicionalmente tutelados pelo Direito Penal, e não necessitam de intervenção legislativa, e por outro lado, temos novos ilícitos que afetam bens jurídicos relativos à sociedade da informação, como acontece com os

dados informáticos, sistemas informáticos, que necessitam alteração legislativa para que possam ser punidos. (CRESPO, 2011).

Neste sentido, as alterações na legislação penal devem ser feitas com muita cautela e desde que seja imprescindível, uma vez que está se lidando com o diploma mais enérgico que pode interferir na liberdade dos cidadãos.

Entretanto, apesar de não haver alterações legislativas significativas, o legislador pátrio não ignorou completamente o fenômeno dos crimes tecnológicos, pois é possível perceber alguns projetos de leis referentes ao tema.

Na Câmara, é possível citar o PLC nº 35/2012, recentemente aprovado no Senado, de autoria do deputado Paulo Teixeira (PT-SP) que altera o Código Penal para tipificar como crimes uma série de delitos cibernéticos, como a violação indevida de equipamentos e sistemas concectados ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização do titular, ou ainda para instalar vulnerabilidades, incluindo dentre tais dispositivos celulares, notebooks, desktops, tablets ou caixas eletrônicos. (Agência Senado).

Além destas, outras condutas bastante prejudiciais como obter, pela invasão, conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais e informações sigilosas podem ter pena de três meses a dois anos de prisão, além de multa. Há ainda a tipificação de condutas menos graves, como a invasão de dispositivo informático, que podem alcançar penas de três meses a um ano, além de multa.

Além disso, estará incorrendo na prática de crimes quem produzir, oferecer ou vender programas de computadores que permitam a invasão.

Vale dizer que existe previsão de aumento de pena se os vitimizados pela prática de tais crimes forem autoridades públicas.

A aprovação deste projeto de lei, é um grande avanço para a sociedade, dada a urgência da situação de grave desproteção da população e das empresas, em razão de lacuna legislativa existente no Código Penal Brasileiro.

Portanto, propostas legislativas são várias, mas o PLC nº 35/2012, apelidado de Lei Carolina Dieckman, justamente pelo incidente sofrido pela atriz em que teve suas fotos íntimas roubadas e divulgadas na internet, sem dúvidas, merece destaque por

ser o principal projeto de lei em trâmite no Brasil, já aprovado no Senado, e aguardando revisão na Câmara dos Deputados.

Dentre as outras iniciativas legislativas, que encontram-se tramitando no Congresso Nacional, a de maior interesse do Poder Legislativo quanto aos delitos digitais, é o PL 84/99 e seu substitutivo. O projeto mencionado visa a tipificação de condutas realizadas mediante uso de sistema eletrônico, digital ou similar, de rede de computadores, ou que sejam praticadas contra dispositivo de comunicação ou sistemas informatizados e similares. Contudo, apesar de tratar-se de um importante projeto de lei, mostra-se extremamente abrangente e impreciso, sendo, por esse motivo, alvo de diversas críticas quanto a limitação do ambiente de inovação tecnológica. (CRESPO, 2003).

Enfim, as propostas de invovação são várias, e a pretensão de punir condutas que trazem prejuízos e muitos problemas a todos que usam a tecnologia é relevante. Contudo, a sociedade aguarda ansiosamente a conclusão dos trabalhos legislativos, buscando a positivação penal das condutas informáticas reprováveis na era digital, mas também em outras áreas do direito que sofreram reflexos com a evolução na informática.

8 CONSIDERAÇÕES FINAIS

A constatação de que a sociedade digital corre riscos com a proliferação da prática de crimes digitais, é inevitável, porque o computador está cada vez mais presente na vida das pessoas, e de certa forma, este é o preço da modernidade e dos avanços tecnológicos. Como consequência, os casos de crimes digitais continuam aumentando, sem que haja providências efetivas para o aumento da segurança dos usuários da rede de computadores mundial.

Os usuários de computadores, que utilizam, por exemplo, serviços bancários *on-line*, apesar da insegurança que sentem no uso destes sistemas, e apesar do conhecimento de ataques virtuais a contas bancárias, continuam utilizando os serviços, na sua grande maioria, não por ignorar tais perigos, mas devido as facilidades que o sistema on-line oferece, economizando tempo, dinheiro, no conforto de casa, etc. É o risco informático.

E a sociedade, que utiliza essa tecnologia, precisa ter a segurança de que as condutas lesivas, praticadas por meio digital, serão coibidas, não ficarão impunes. O amplo meio digital da rede mundial de computadores traz muitas facilidades de comunicação, de negócios, mas traz junto consigo a facilidade da prática de delitos virtuais. É essa segurança que a sociedade precisa ter, para continuar usufruindo dos maravilhosos avanços que a tecnologia nos proporciona, e possibilitando um desenvolvimento responsável e equilibrado da ciência da tecnologia.

É certo que, a maior instrução dos usuários de computadores diminui as chances de sofrer risco de um ataque virtual, mas não é totalmente eficaz, tendo em vista as constantes inovações dos crimes praticados por meio de computadores, tomando as vítimas de surpresa em novos golpes digitais, mesmo as mais instruídas, nas diversas situações de risco criadas pela sociedade global informatizada. Portanto, é preciso uma renovação do direito penal, como talvez, a criação de um direito penal informático, de modo a conferir soluções efetivas às modernidades (os ilícitos informáticos) surgidas na sociedade. E, em uma última análise, ainda é preciso determinar aspectos do espaço digital quanto ao lugar do crime, quanto à velocidade de adaptação do direito às modernidades virtuais, e até mesmo quanto a possibilidade de intervenções a ataques praticados no ambiente informático.

REFERÊNCIAS

ARANHA, Maria Lúcia de Arruda; MARTINS, Maria Helena Pires. **Temas de Filosofia**. São Paulo: Moderna, 2005.

ARAS, Vladimir. Crimes de informática. Uma nova criminalidade. **Jus Navigandi**, Teresina, ano 6, n. 51, 1 out. 2001 . Disponível em: <http://jus.com.br/revista/texto/2250> . Acesso em: 22 out. 2012.

BAUMAN, Zygmunt. **Amor Líquido**. Rio de Janeiro: Zahar, 2004.

BITENCOURT, Cezar Roberto. Manual de Direito Penal: Parte Especial. Volume 2, São Paulo, Saraiva, 2001.

BRASIL. Constituição (1988). **Constituição da Republica Federativa do Brasil**. Brasília, DF: Senado Federal.

BRASIL. **Código Penal Brasileiro**. Vade Mecum.10 ed. São Paulo: Saraiva, 2010.

BRASIL. PROJETO DE LEI 84/99. Disponível em <www.brdatanet.com.br/infocenter/biblioteca/ pl8499.html>. Acesso em: 6 nov. 2011

CAPEZ, Fernando. **Processo Penal Simplificado**. 18 ed. São Paulo: Saraiva, 2011.

CASTRO, Carla Rodrigues Araújo de. **Crimes de Informática e Seus Aspectos Processuais**. Rio de Janeiro, Lumen Júris, 2003.

CHAVES, Cristiano; ROSENVALD, Nelson. **Direito Civil. Parte Geral**. 7 ed. Rio de Janeiro: Lúmen Júris, 2008.

CORRÊA, Gustavo Testa. **Aspectos Jurídicos da Internet**. 2 ed. São Paulo: Saraiva, 2000.

COSTA, Álvaro Mayrink da. **Temas de Direito Penal**. Rio de Janeiro: Lúmen Júris, 2011.

COSTA, Fernando José da. Locus Delicti nos Crimes Informáticos. Faculdade de Direito da USP, São Paulo, 2011.

CRESPO, Marcelo Xavier de Freitas. **Crimes digitais**. São Paulo: Saraiva, 2011.

DRUMMOND, Victor. **Internet, Privacidade e Dados Pessoais**. Rio de Janeiro: Editora Lúmen Juris, 2003.

FERREIRA, Fabio Jânio Lima. **Crimes Digitais**. Disponível em< http://segurancadigital.info/ dicas/49-seguranca-da-informacao/59-crimes-digitais. Acesso em: 4 dez 2011.

GIL, Antonio de Loureiro. "**Fraudes Informatizadas**". 2 ed. rev. São Paulo: Saraiva, 2002.

GRECO, Rogério. **Curso de Direito Penal. Volume I, parte geral**. 11 ed. Rio de Janeiro: Impetus, 2009.

GOMES, Wilson ; REIS, Lucas. **Publicidade Digital:** Formatos e tendências da nova fronteira publicitária. Salvador: P&A editora, 2011.

LIMA, Paulo Marco Ferreira. **Crimes de Computador e Segurança Computacional**. 2 ed. São Paulo: Atlas, 2011.

MARZOCHI, Marcelo de Luca. **Direito.br:** aspectos jurídicos da Internet no Brasil. São Paulo, Ed. LTr, 2000.

MIRABETE, Júlio Fabbrini. **Manual de Direito Penal**. Volume I. 28 ed. São Paulo: Atlas, 2012.

NOGUEIRA, Fernando Célio de Brito. **Violação de e-mail é crime?.** Disponível em: <http://jus.com.br/revista/texto/1789>. Acesso em: 25 out. 2012.

PAESANI, Liliana Minardi. **Direito e Internet:** Liberdade de informação, privacidade e responsabilidade civil. 2ª ed. São Paulo: Atlas, 2003.

PRADO, Luiz Regis. **Curso de Direito Penal Brasileiro**. Volume I, Parte Geral. 7 ed. São Paulo, Editora Revista dos Tribunais, 2007.

FILHO REINALDO. Demócrito. **Questões Técnicas Dificultam Condenações por Crimes Cometidos pela Internet.** Jus Navigandi. Disponível em: < http://www.pontojuridico.com/modules.php?name=News&file=print&sid=79>. Acesso em: 02 nov 2012

Agência Senado – Senado aprova projeto que define crimes cibernéticos – Paola Lima. Disponível em: <http://www12.senado.gov.br/noticias/materias/2012/10/31/ senado-aprova-projeto-que-define-crimes-ciberneticos>. Acesso em: 31 out. 2012.

QUEIROZ, Paulo. **Direito Penal: Parte geral**. 3 ed. São Paulo. Saraiva, 2006.

RECUERO, Raquel da Cunha. **Internet e a Nova Revolução na Comunicação Mundial**. Disponível em: <http://www.pontomidia.com.br/raquel/revolucao.htm>. Acesso em 6 nov. 2011.

SCHOUERI, Luís Eduardo. **Internet; o direito na era virtual**. São Paulo; Ed. Lacaz Martins, Halemberck, Pereira Neto, Gurevich e Schoueri Advogados, 2000.

TOLEDO, Francisco de Assis. Princípios Básicos de Direito Penal. 5 ed. São Paulo. Saraiva, 2000.