UNIVERSIDADE PRESIDENTE ANTÔNIO CARLOS
INSTITUTO DE ESTUDOS TECNOLÓGICOS E SEQUENCIAIS DE JUIZ DE FORA

CARLOS IURI DE OLIVEIRA DIAS

CRIMES VIRTUAIS

Juiz de Fora
2014

CARLOS IURI DE OLIVEIRA DIAS

CRIMES VIRTUAIS

Monografia de conclusão de curso apresentada ao Instituto de Estudos Tecnológicos da Universidade Presidente Antônio Carlos, como requisito parcial à obtenção do título de Bacharel em Direito. Orientador: Prof. Rodrigo Ribeiro Rolli.

Juiz de Fora
2014

FOLHA DE APROVAÇÃO

Carlos Iuri de Oliveira Dias

Aluno

Crimes Virtuais

Tema

Monografia de conclusão de Curso apresentada ao Curso de Direito, da Universidade Presidente Antônio Carlos / Juiz de Fora, como exigência para obtenção do grau de Bacharel em Direito.

BANCA EXAMINADORA

Aprovada em 17 / 12 / 2014.

AGRADECIMENTO

Ao Deus Eterno, Soberano e Fiel, que me fortaleceu e sustentou ao longo destes anos, possibilitando a conclusão desta importante etapa de minha vida acadêmica.

À minha mãe e ao meu pai, que com carinho e compreensão ajudaram-me a superar as dificuldades que cruzaram meu caminho.

Ao amigo Douglas Alves pelo apoio e incentivo em momentos decisivos desta jornada.

Ao Profº. Rodrigo Ribeiro Rolli pelo carinho e dedicação com que orientou este trabalho.

À todos que direta ou indiretamente contribuíram para a conclusão deste artigo científico

Só depois que a tecnologia inventou o telefone, o telégrafo, a televisão, a internet, foi que se descobriu que o problema de comunicação mais sério era o de perto.

(Millôr Fernandes)

RESUMO

A expansão da rede mundial de computadores, ao passo que facilitou a vida da sociedade moderna, criou uma série de problemas aos seus usuários, possibilitando o surgimento de inúmeras condutas ilícitas. O presente trabalho tem por objetivo abordar a evolução tecnológica, os crimes virtuais, o direito comparado e a legislação brasileira.

PALAVRAS CHAVE: Internet; Crimes Virtuais; Legislação.

SUMÁRIO

1 INTRODUÇÃO

O advento da Internet produziu uma verdadeira revolução no mundo globalizado em que vivemos, encurtando distâncias, derrubando barreiras, difundindo informação e conhecimento. Inúmeros avanços científicos e tecnológicos que a sociedade moderna alcançou devem ser creditados a esta poderosa ferramenta.

Apesar dos inegáveis benefícios trazidos pela rede mundial de computadores, criminosos encontraram nela um novo e vasto campo de atuação a ser explorado, propício à realização de práticas delitivas. Sendo assim, a internet tem se tornado um ambiente insólito e inseguro para os incautos usuários da rede.

Com a crescente ocorrência de tais práticas delituosas, a discussão sobre este tema ganha cada vez maior relevância no âmbito jurídico, que, de forma alguma, pode quedar-se inerte diante da presente demanda.

Percebe-se que a polêmica sobre a necessidade de implementação das ações de combate aos crimes virtuais ganha cada vez maior espaço na mídia, que, entretanto, não aborda as dificuldades encontradas na efetivação dessas ações.

O presente trabalho tem por objetivo estimular a reflexão a respeito do crescimento de tais crimes, do desenvolvimento tecnológico, dos crimes virtuais, do direito comparado, do nosso ordenamento jurídico e dificuldades encontradas pelas autoridades para identificar e punir os responsáveis pelas práticas criminosas perpetradas no ambiente virtual.

No presente trabalho serão expostos temas de grande relevância.

O primeiro capítulo será tratado acerca da evolução tecnológica, a qual se demonstra fundamental para a expansão de novos direitos, deveres e crimes que merecem ser tutelados pelo Estado.

Já no segundo capitulo será exposta a relação entre a informática e o direito, que é de suma importância para o entendimento do trabalho, pois, apesar da informática não ter um ramo autônomo no direito, não significa que não mereça relevância pelo legislador.

No que tange ao terceiro capítulo, será abordado os crimes virtuais em espécie, bem como, seu conceito, classificação, sujeitos e bens jurídicos tutelados.

No quarto capítulo irá ser demonstrado as diretrizes traçadas internacionalmente traçadas, tendo em vista, que para se combater o delito

informático é de extrema importância a uniformização de normas para se tornar efetiva ação estatal.

Por fim, no quinto capítulo será explanado acerca da legislação internacional, para o tema ser entendido de forma mais ampla e com fins de comparar com a legislação brasileira que será falada no último capitulo.

2 A ERA DA INFORMAÇÃO

Desde o começo até os dias atuais, o homem sempre buscou desenvolver máquinas e ferramentas que lhe fossem úteis nas atividades diárias. A internet surgiu na década de 60, mais precisamente no ano de 1966, quando algumas universidades se uniram para desenvolver a ARPANET (*Advanced Research Projects Administratrion* - Administração de Projetos e Pesquisas Avançados). Quando foi desenvolvida, seu uso era exclusivo das Forças Armadas norte-americanas.

A ARPANET cresceu muito com a grande expansão da telefonia norte-americana. Porém, foi a implementação do TCP/IP (Protocolo de Controle de Transferência/Protocolo de Internet) que efetivamente possibilitou o surgimento da internet. Com esse protocolo é possível a interligação entre computadores, possibilitando que atuem em grupo. "O tempo passou, mas o princípio básico da internet não desapareceu. Até hoje ela baseia-se na ideia de não se produzir comandos centrais, tornando todos os pontos equivalentes. Assim, não importa onde estejam os computadores". (CRESPO, 2011, p. 31).

Com esse avanço evolutivo tecnológico, as relações comerciais, as administrações públicas e a sociedade como um todo passaram a depender muito da segurança e eficiência da chamada tecnologia da informação. Vejamos que transações financeiras de grandes negócios é feita pelo computador, empresas guardam eletronicamente suas informações de atividades e arquivos mais valiosos, bem como os sistemas marítimos, aeronáuticos e espaciais. Com isso, percebe-se que a sociedade moderna se prende e depende cada vez mais da informática.

Segundo Sieber:

> Para a compreensão da evolução acima referida, aponta três mudanças fundamentais percebidas no final do século XX até a formação da atual sociedade, no início do século XXI (i) a formação da sociedade de informação; (ii) o desenvolvimento da sociedade de riscos; e (iii) a configuração de uma sociedade global e digital. (2002, p. 14)

De acordo com o autor supracitado, a passagem da sociedade industrial para a sociedade de informação foi definida por sociólogos e economistas como uma *"segunda revolução industrial"*, sendo que, enquanto a primeira operou-se de

substituir a mão de obra humana por uso de máquinas e animais, a segunda foi caracterizada pela substituição da atividade intelectual humana por máquinas.

Com esse significativo passo à evolução tecnológica alcançada pelo homem, começa a formação da *"sociedade da informação"*, que adveio de um longo processo de desenvolvimento, que se constituiu em um conjunto de mudanças tecnológicas com grande reflexo na economia e na vida social.

Segundo Sieber (2002) o desenvolvimento tecnológico não tornou a sociedade apenas mais informatizada, mas, como também se passou a ter maior cuidado e valor com bens imateriais, como é o caso da propriedade intelectual, do segredo industrial e de depósitos em dinheiro, desse modo, a informação passou a não ter mais valor, mas tornou-se fator de poder e de perigos potenciais. Logo, conclui-se que apesar do sistema de informatização ser uma ferramenta usada para a facilitação e otimização usada nas atividades elaboradas pelo homem, também possui falhas e brechas. Sendo assim pode ser atacada por criminosos, a fim de praticar dos mais diversos tipos de crimes, pois é importante ressaltar que o uso indevido de computadores e da tecnologia em geral constitui verdadeira ameaça global, sendo de suma importância que a segurança dos sistemas informáticos seja a grande preocupação da sociedade da informação.

Rovira Del Canto (2002, p.18) sustenta "que parte da doutrina alemã entende haver três categorias de riscos: (i) riscos tradicionais (que são pessoais); (ii) riscos próprios do estado de bem-estar social (iii) novos riscos (tradicionais e os do estado de bem estar social". Visto essa definição percebe-se que nasce novos riscos, com maiores impactos sem que possam ser limitados no tempo ou espaço. São riscos que adquirem dimensão social, não se limitando aos indivíduos. Surgi, pois, a noção de bem jurídico difuso.

Dentro do âmbito desses novos riscos é que devemos levar em consideração a evolução tecnológica informática. E, nesse sentido, fica claro que a delinquência informática aparece configurada como um fenômeno social com relação aos novos riscos, sendo, portanto, parte da *"sociedade de risco".*

Netto, (2006, p. 123) "aponta que a doutrina já é clara em configurar a criminalidade informática como forma de ilícito complexo, decorrente da sociedade de risco". Já Valle (1996, p. 76) entende "como mero fenômeno associado ao tempo de nascimento de novos riscos". Em resumo, quer-se dizer que há novos paradigmas. As sociedades desde os primórdios sempre foram *"de risco"*. Entretanto

é importante ressaltar, que o termo *“sociedade de riscos”* deve ser interpretado com ressalvas, pois com a evolução humana, certos riscos que havia no passado não nos atormentam mais.

Outra mudança significativa da evolução social é progressivo contato dos cidadãos do mundo, pois graças os serviços de telecomunicação internacional ou os próprios meios digitais pode-se obter um contato sólido com o mundo todo, ainda que fisicamente distantes.

O filósofo canadense Herbert Marshall McLuhan criou o termo *“Aldeia Global”*, que explica que devido ao progresso tecnológico reduz todo planeta como é reduzida uma aldeia, havendo possibilidade de se intercomunicar diretamente com qualquer pessoa.

Tais considerações nos fazem crer que a atual tecnologia informática deu lugar à entrada de novas minúcias nas relações sociais. Rigorosamente falando o mundo vive em processo de evolução desde os tempos mais remotos. Todavia o fenômeno que se denomina “globalização” é bem mais recente.

3 INFORMÁTICA E O DIREITO

Interessa, para a continuidade do trabalho, estabelecer quais as relações que pode haver entre o Direito e a informática, tendo em vista, que o direito é um fenômeno cultural, sendo assim, deve acompanhar, de algum modo, a realidade temporal e geográfica em que se desenvolve, uma vez, que as evoluções do mundo social, político econômico reflete os aspectos jurídicos para que se regularize a vida em sociedade e também proporcionar a segurança e bem estar de todos.

Dessa forma, naturalmente surgem inquietações dos homens quanto as leis que venham regular o desenvolvimento tecnológico, pois este avanço das tecnologias impõe complexos problemas jurídicos a serem decifrados pelos operadores do Direito.

A doutrina define a informática jurídica como o ramo da informática que compreende as suas aplicações específicas ao mundo do Direito, complementando o trabalho daqueles que operam com o Direito através do processamento eletrônico das informações jurídicas. Nas palavras de Marques e Martins (2006, p. 25) “trata-se da análise e resolução do complexo de problemas jurídicos levantados pelo computador”. Em suma, o direito da informática não merece até agora ser um ramo específico do Direito, entretanto isso não quer dizer que as irregularidades e crimes praticados não merecem ter a devida atenção do ordenamento jurídico.

Através dessa analise, não se pode ignorar que a informática possui estreita relação com o direito, pois está interligado com o Direito Constitucional, já que a Constituição Federal é a base do sistema jurídico, Um exemplo claro é a liberdade de comunicação, especialmente via internet, onde se verifica uma das expressões fundamentais da liberdade de pensamento.

Com relação ao Direito Civil, também há relação, especialmente nas relações obrigacionais praticadas via internet.

Há ainda, importante relação com o Direito do Consumidor, pois nota-se que há significativa movimentação de comércio pelos meios eletrônicos.

No que tange ao Direito administrativo, a informática também tem seus vínculos. É o que se nota com os serviços de E-CPF e E-CNPJ. Estes são arquivos eletrônicos que identificam o usuário, constituindo verdadeiro documento eletrônico de identidade e fornecendo as garantias da privacidade, integridade e autenticidade

do documento. Há ainda outros serviços prestados pela administração pública através da internet ou informática.

Por fim, quanto ao Direito Penal, a relação com a internet também se faz clara na medida em que são discutidas questões de acesso não autorizado a sistemas, *"spam",* estelionato, vírus entre outros. Com todas essas mazelas no sistema informático, percebe-se que este é vulnerável e merece que o Estado o tutele como bem jurídico a ser protegido pelo nosso Direito.

No Brasil, foi fundado em 2007, o IBDI (Instituto Brasileiro de Política e Direito da Informática) é uma associação civil sem fins lucrativos, religiosos ou partidários, que desenvolve atividades dirigidas ao ensino, a pesquisa científica, ao desenvolvimento tecnológico, a proteção e preservação do meio ambiente, a cultura e a saúde, especialmente para:

> - implementar atividades e pesquisas que tenham por objeto o estudo científico do Direito e, em especial, do Direito da Informática;
> - realizar seminários, congressos, cursos, simpósios e conferencias, inclusive em conjunto com outras instituições, sobre temas de Direito da Informática e Administração de recursos informáticos, ou outros temas jurídicos relevantes;
> - estimular o advento de matérias do âmbito do universo do Direito da informática nos cursos de graduação e pós-graduação das Faculdades de Direito e de Administração;
> - promover intercâmbio cultural com entidades congêneres nacionais e estrangeiras;
> - emitir pareceres técnicos e apresentar anteprojetos de lei em matéria de Direito da Informática;
> - celebrar convênios com quaisquer instituições para melhor realização de suas finalidades, mormente com as universidades, faculdades e outros institutos congêneres;
> - manter biblioteca e setor de jurisprudência especializada;
> - editar revistas, boletins ou trabalhos sobre Direito da Informática;
> - conceder bolsas de estudo para seus sócios;
> - firmar contratos de gestão com o Poder Público com vistas a formação de parceria para fomento e execução de suas atividades sociais;
> - desenvolver, em parceria com outros órgãos, projetos de estruturação e planejamento informático de órgãos da Administração Pública, especialmente do Poder Judiciário;
> - prestar assistência técnica e jurídica, no âmbito do D. da Informática, a órgãos públicos ou outras organizações sociais, mediante a assinatura de convênios ou contratos de gestão (2007, p.1)

Vejamos que a criação do IBDI é de grande relevância, pois é uma associação que busca aperfeiçoar os serviços de informática e busca ainda consolidar o direito da informática no país.

Passa-se então a se preocupar com o as atividades exercidas no meio eletrônico no nosso país, pois não se pode ignorar que cada vez mais o homem se prende à tecnologia, sendo assim, torna-se um instrumento essencial para vida civil dos cidadãos, contudo, uma vez, que o homem passa a interagir com as máquinas também abre caminhos para a realização dos crimes virtuais cada vez mais presentes em nossa sociedade.

4 PRINCÍPIOS CONSTITUCIONAIS

O Art. 5º, II, CF/88 dispõe sobre o Princípio da Legalidade. No entanto, uma das dificuldades para se punir os crimes praticados no ambiente virtual é a prévia tipificação destes crimes por meio de lei.

Muitos criminosos virtuais ficam impunes por falta de uma legislação específica, que enquadre as suas respectivas condutas delitivas, fazendo da internet um “ambiente seguro” para a prática de alguns crimes.

> Art. 5º, XII – Princípio da Inviolabilidade das Comunicações. A Constituição garante o sigilo das comunicações, dificultando a identificação daqueles que cometem crimes no ambiente virtual (BRASIL. 1988).
> Art. 5º, XXXIX da C.R.F.B. – Princípio da Anterioridade. Infelizmente, percebe-se que a legislação não consegue acompanhar o ritmo das mudanças nas estratégias dos criminosos virtuais (Brasil, 1988).

5 DOS CRIMES VIRTUAIS

Inicialmente, cumpre ressaltar que há várias acepções conceituais dos chamados crimes virtuais. Tais conceitos são amplos e é importante salientar alguns deles.

Pode-se citar Fabrizio Rosa que conceitua o crime de informática como sendo:

> A conduta que atente contra o estado natural dos dados e recursos oferecidos por um sistema de processamento de dados, seja pela compilação, armazenamento ou transmissão de dados, na sua forma, compreendida pelos elementos que compõem um sistema de tratamento, transmissão ou armazenagem de dados, ou seja, ainda, na forma mais rudimentar; 2. O 'Crime de informática' é todo aquele procedimento que atenta contra dados, que faz na forma em que estejam armazenados, compilados, transmissíveis ou em transmissão; 3. Assim, o 'Crime de Informática' pressupõe dois elementos indissolúveis: contra os dados que estejam preparados às operações do computador e, também, através do computador, utilizando-se software e hardware, para perpetra-lo; 4. A expressão crimes de informática, entendida como tal, é toda a ação típica, antijurídica e culpável, contra ou pela utilização de processamento automático e/ou eletrônico de dados ou sua transmissão; 5. Nos crimes de informática para atentar contra um bem ou interesse juridicamente protegido, pertença à ordem econômica, à integridade corporal, à liberdade individual, à privacidade, à honra, ao patrimônio público ou privado, à Administração Pública, etc (2002, p. 53-54).

Já Roque (2007, p. 25), conceitua crime de informática como sendo *"*toda conduta, definida em lei como crime, em que o computador tiver sido utilizado como instrumento de sua perpetração ou consistir em seu objeto material".

Através desses conceitos, pode-se concluir que, apesar de ter diferentes posicionamentos para tipificar a conduta criminosa, o meio sempre será o mesmo, sendo o instrumento o computador e o meio pelo qual o ato é praticado é a Internet.

Segundo Crespo:

> Os crimes digitais compreendem às condutas de acesso não autorizado a sistemas informáticos, ações destrutivas nesses sistemas, a interceptação de comunicações, modificações de dados, infrações a direitos de autor, incitação ao ódio e descriminação, escárnio religioso, difusão de pornografia infantil, terrorismo, entre outros (2011, p. 46).

Nota-se, assim, que o ciberespaço é campo para o cometimento de crimes que já estão previstos em ordenamentos jurídicos de alto dano à vítima.

Impende salientar ainda algumas características aduzidas por Casabona, que expressa a vulnerabilidade do ciberespaço:

> a) Capacidade de processar, guardar e circular, de forma automatizada e em tempo real, grandes quantidades de informações em formato digital dos mais variados (fotos, filmes, sons). Isso é facilitado pela própria estrutura descentralizada e não hierarquizada da internet que inviabiliza a existência de órgãos de controle de informação circulante e, como consectário lógico, torna praticamente impossível supervisionar a qualidade e o volume de informações; b) O número enorme de usuários, a frequência com que acessam a liberdade que têm para enviar, transferir, difundir e acessar informações, de modo que os internautas passam a ser potencias vítimas, mas também potenciais sujeitos ativos de delitos; c) As próprias características físicas, técnicas das TIC, que podem ser acessadas de forma ilegítima, tendo seu conteúdo alterado. Consegue-se acesso a arquivos das mais distintas naturezas e aos mais variados programas de computador; d) A enorme potencialidade de multiplicação das ações ilícitas. Isso decorre da própria estrutura das TIC, como mencionado acima, A criação de fóruns de debates, páginas na internet, comunidades de relacionamento etc., podem facilitar a prática de delitos, podendo, ainda, dar maior repercussão a eles, como nas ofensas contra honra, por exemplo (2006, p. 3-4).

Assim, nota-se que da mesma forma que um internauta tem facilidade para acessar os dados contidos na rede, um delinquente também terá, e estará munido de maldade para distorcer o bom uso de um instrumento que em tese seria usado para o bem comum de uma sociedade, causando dano à terceiros.

Sendo assim, com essa dificuldade de controlar os dados que estão sendo jogado na rede, o Direito Penal enfrenta novas realidades quanto às práticas delitivas, de modo que não se pode ignorar a realidade de novos "*modi operandi*" e novas ponderações de condutas danosas.

Conforme demonstrado acima, o termo *"crimes digitais"* pode delimitar várias condutas, tendo grande amplitude, sendo assim, uma das primeiras questões que deve ser abordada é a nomenclatura de tais ilícitos. É de suma importância a apresentação clara daquilo que se busca discutir a fim de que não haja lacunas e pontos pouco claros sobre o que pretende dissertar.

Crespo disserta algumas denominações, dentre as quais:

> Crimes de computador, infrações cometidas por meio de computador, crimes por meio da informática, fraude informática, delinquência informática, crimes digitais, "*computer-related crimes"* ou crimes cibernético (2011, p. 47).

A doutrina espanhola no inicio dos anos 1980, passou usar *"delitos informáticos"* como nomenclatura, trazida pelo departamento de justiça norte americano que usa *computer crime.*

Na doutrina brasileira, encontramos diversas variações. Segundo Reis, aduz oito possíveis denominações:

> (a) *computer crimes* (aduz que o crime não é do computador, mas do agente); (b) abuso de computador (detectar o que sejam abusos dependeria de amadurecimento do campo ético-informático); (c) crime de computação (há crimes próprios – puros - e os impróprios, sendo que esta denominação leva em conta apenas a primeira categoria); (d) criminalidade mediante computadores (mesma crítica feita ao termo anterior; (e) delito informático (mais comum em países de língua espanhola, é feito pensando-se no objeto jurídico tutelado – proteção da informação – mas nem sempre esse será o foco de proteção); (f) fraude informática (nem todos os delitos praticados com o auxilio da tecnologia são fraudulentos); (g) delinquência econômica (há crimes sem motivo econômico) e; (h) *computerkriminalistät*(conceito mais amplo e que talvez fosse mais adequado) (1997, p.24).

Por seu turno, Gouvêa (2007, p. 54) prefere o uso da expressão *"crimes por meio da informática"*, justificando sua escolha aduzindo que os computadores não são os únicos instrumentos capazes de serem usados nas práticas delituosas. Vianna (2007, p.9-10) considera que *"*o bem jurídico tutelado, na sua exposição sobre acesso não autorizado a sistemas computacionais, considera duas possibilidades: delitos informáticos ou delitos computacionais".

Verifica-se, que ainda não há o menor consenso em nossa doutrina a respeito da denominação dos delitos relacionados com a tecnologia. Há de se concluir ainda, que os delitos praticados por meio da informática não se podem vincular somente ao computador, já que se verificam delitos cometidos através do uso de telecomunicações, da telemática, e sabemos que a telecomunicação depende da informática, portanto, não julgamos equivocado o uso da expressão *"delitos informáticos".*

Com a nomenclatura ressaltada no parágrafo anterior, conseguimos direcionar o sentido das condutas delituosas praticadas na área da informática, assim, a ação criminosa abrangerá todas as tecnologias da informação, do processamento e da transmissão de dados, portanto, apesar da diversidade de suas classificações, pode ser identificada pelo seu objeto ou pelos meios de atuação, os quais fornecem um denominador comum, embora com diferentes denominações.

Passado a questão da definição e nomenclatura, é importante ressaltar acerca dos bens jurídicos que podem ser agredidos pelo infrator e o que merece ser tutelado pelo nosso ordenamento jurídico.

Após a Segunda Guerra Mundial, surgiram novos riscos social, que foram tomando lugar e alterando as relações entre os homens, pois ainda que se pregue a aplicação do Direito Penal como a *"ultima ratio",* nota-se o incremento de novos tipos penais relativo a novos riscos.

Dessa forma, não se pode deixar de questionar se há novos bens jurídicos, decorrente do avanço tecnológico e se estes merecem ser tutelados por parte do Direito Penal. Diante disso nosso direito deixa de se preocupar com os bens jurídicos tradicionais como a vida, a integridade física, o patrimônio, a fé pública, mas também as informações armazenadas, a segurança dos sistemas de rede e informática ou de telecomunicações.

Diante disso, a informação possui traços de mercadoria, pode-se afirmar que significa como uma nova matéria-prima do gênero "bens imateriais", portanto é um bem jurídico valorado pelo homem e deve ter atenção e resposta do Direito Penal como qualquer outro bem jurídico já perpetuado em nosso ordenamento. Além disso, não há como negar que, além da informação, os dados, a confiabilidade e segurança dos sistemas e redes informáticas e de comunicação sejam novos paradigmas de bem jurídicos a serem tutelados pelo Direito Penal.

Segundo Crespo pode-se dizer que:

> Os crimes digitais são pluriofensivos na exata medida em que há a proteção de bens jurídicos tradicionais, mas, ao mesmo tempo, proteção de novos interesses derivados da sociedade de risco e de informação. Sem essa concepção parece não existir categoria específica dessa criminalidade. Justamente por isso que foi dito não ser correto atrelar unicamente e exclusivamente o meio pelo qual se pratica a conduta, devendo se constituir em torno da afetação da informação como bem jurídico protegido, primordial e basicamente, ainda que não de forma exclusiva (2011, p. 57).

Deve-se, portanto, pensar em qual o principal bem jurídico afetado. Segundo Rovira Del Canto (2002, p.72) sustenta que "é a informação é o bem jurídico principal a ser tutelado nos crimes digitais e, secundariamente, os dados ou sistemas".

Assim, considerando-se tanto a informação quanto os sistemas informáticos ou dados, quanto à sua integridade e inviolabilidade, há que se pensar em novos

paradigmas sobre bens jurídicos, o que se reputa perfeitamente adequado e condizente com as novas perspectivas de risco da sociedade da informação.

6 DA CLASSIFICAÇÃO DOS CRIMES

Primeiramente, cumpre registrar que é de grande relevância classificar os crimes digitais, pois a partir disso, que se fará a exposição sobre as condutas específicas, porém, antes de adentrarmos a classificação é importante ressaltar algumas ideias sobre as classificações apresentadas pela doutrina.

Segundo Crespo:

> Tal ideia justifica-se na explicação de que muitas vezes o sistema informático é mero instrumento para consecução delitiva, casos em que seria perfeitamente dispensável na realização da conduta. Em outras palavras: referimo-nos a delitos de ação livre, que podem ser cometidos por diferentes *modi operandi*. Por outro lado, há condutas que só poderiam ser realizadas contra um sistema informático ou informações nele contidas (2011, p. 60).

Crespo expressa na ideia acima, que o a classificação não será somente por um *modi operandi,* ou seja, o delito poderá ser praticado mediante a ação de diversos modos não ficando assim, preso à apenas um modo de cometer a infração.

Ferreira sugere a classificação dos crimes virtuais como:

> Atos dirigidos contra um sistema de informática, tendo como subespécies atos contra o computador e atos contra os dados ou programas de computador. Atos cometidos por intermédio de um sistema de informática e dentro deles incluídos infrações contra o patrimônio; as infrações contra a liberdade individual e as infrações contra a propriedade imaterial (2005, p.261).

Dentre as diversas classificações apresentada pela doutrina, nos parece ser essas explicitadas acima as mais didáticas e a que se acredita estar mais próxima da realidade dos fatos sendo divididas entre crimes virtuais próprios e impróprios.

Os crimes virtuais próprios são aqueles em que o sujeito ativo se utiliza necessariamente do computador ou do sistema informático do sujeito passivo, no qual será usado como objeto e meio para execução do crime. Nesse raciocínio corrobora Damásio de Jesus (2000) apud ARAS, quando diz que:

> Crimes eletrônicos puros ou próprios são aqueles que sejam praticados por computador e se realizem ou se consumem também em meio eletrônico. Neles, a informática (segurança dos sistemas, titularidade das informações e integridade dos dados, da máquina e periféricos) é o objeto jurídico tutelado (2001, p.1).

A doutrina trouxe à tona, os crimes próprios mais decorrentes e corriqueiros dentro da sociedade que é o: acesso não autorizado, mais conhecido como invasão praticada por hackers; obtenção de transferência ilegal de dados, que se perfaz pelos *"spywares"*(termo genérico para designar arquivos espiões) que se trata de um programa que rastreia informações do usuário contidas em seu computador; dano informático, por este crime há uma discussão doutrinária que argumenta que tal conduta poderia ser passível de sansão nos termos do art. 163 do Código Penal, entretanto não é interessante prolongarmos tal discussão sob pena de alterar o tema principal do presente trabalho; dos vírus e sua disseminação, que nada mais é do que arquivos maliciosos a fim de inutilizar o computador do sujeito passivo e explorar as falhas de segurança de um sistema de dados; divulgação ou utilização indevida de informações, que nada mais é que correspondência virtual não solicitada pelo usuário de um computador e que é remetida em massa, portanto para número enorme de pessoas, denomina-se como *"spam";* embaraçamento ao funcionamento de sistemas, ocorre com fins de tirar de operação um serviço ou outros computadores conectados à internet; engenharia social e *"phishing",* é todo método ardiloso de mascarar a realidade para explorar ou enganar a confiança de uma pessoa detentora de dados importantes a que se quer ter acesso; e interceptação ilegal de dados no qual o infrator interceptará dados alheio em próprio proveito ou de outrem.

Como visto no parágrafo anterior, são esses os crimes virtuais próprios mais recorrentes no nosso meio social. Além dos crimes próprios há que se falar ainda dos impróprios que será tratado no parágrafo seguinte.

Os crimes digitais impróprios nada mais são aqueles já tradicionalmente tipificados no ordenamento, mas agora praticados com auxílio de modernas tecnologias. Assim, essa denominação apenas representa os ilícitos penais tradicionais podem ser cometidos por meio de novos *modi operandi*. Ou seja, são crimes já previstos no nosso ordenamento jurídico, porém são realizados agora com a utilização do computador e da rede utilizando o sistema de informática seus componentes como mais um meio para realização do crime, e se difere quanto a não essencialidade do computador para concretização do ato ilícito que pode se dar de outras formas e não necessariamente pela informática para chegar ao fim desejado como no caso de crimes como: pedofilia.

A respeito do tema, corrobora Damásio de Jesus (2000) apud ARAS:

> [...] Já os crimes eletrônicos impuros ou impróprios são aqueles em que o agente se vale do computador como meio para produzir resultado naturalístico, que ofenda o mundo físico ou o espaço "real", ameaçando ou lesando outros bens, não-computacionais ou diversos da informática (2001, p. 1).

Como se nota, há diferenças fundamentais quanto os crimes próprios e impróprios. Em suma os crimes próprios afetam diretamente bens jurídicos “virtuais”, tal prática afeta diretamente o sistema de dados e computadores alheios. Já os crimes impróprios se valem como meio de execução para produzir resultado, que ataque o mundo físico, bens não-computacionais ou até mesmo bens imateriais.

Impende salientar ainda, que tais classificações são de suma importância, uma vez que se consegue perceber essa diferença, poderá ser feito uma analise mais profunda da conduta praticada, que consequentemente irá facilitar o legislador a criar leis eficazes, a fim de combater esses crimes, que vem se perpetuando e disseminando na sociedade.

7 DOS SUJEITOS DOS CRIMES VIRTUAIS

Antes de adentrarmos, aos sujeitos ativo e passivo dos delitos virtuais, é importante discorrer acerca da estrutura do crime, pois é de suma importância deixar bem claro quanto a estrutura delituosa para que não haja duvidas quanto aos sujeitos.

No direito penal o sujeito ativo é quem pratica a conduta (ação ou omissão) criminosa. Segundo o ilustre doutrinador Cezar Roberto Bitencourt – em Tratado de Direito Penal – Volume 1 Parte Geral (2006, p. 286), afirma que tenha como "sujeito ativo o ser vivo nascido de mulher, embora em tempos remotos tenham sido condenados, como autores de crimes, animais, cadáveres e até estátuas".

A pedra angular da Teoria do Delito, analisa Bitencourt (2006, p. 286), é a conduta (ação ou omissão), algo exclusivo do ser humano: "A capacidade da ação, de culpabilidade, exige a presença de uma vontade, entendida como faculdade psíquica da pessoa individual, que somente o ser humano pode ter."

O sujeito ativo, será então a pessoa como possível autora do ilícito penal e que é, via de regra, pessoa física. Luiz Régis Prado, em Curso de Direito Penal Brasileiro – Volume 1 Parte Geral (2011, p. 258), define "sujeito ativo, autor, ou agente, é todo aquele que realiza a ação ou omissão típica, nos delitos dolosos ou culposos. Ou seja, é aquele cuja atividade é subsumível ao tipo legal incriminador".

Fernando Capez, em Curso de Direito Penal – parte geral Volume 1, complementa que:

> O conceito abrange não só aquele que pratica o núcleo da figura típica (quem mata, subtrai etc.), como também o partícipe, que colabora de alguma forma na conduta típica, sem, contudo, executar atos de conotação típica, mas que de alguma forma, subjetiva ou objetivamente, contribui para a ação criminosa (2011, p. 167).

Cabe fazer alguns adendos, ainda no tocante ao assunto sujeito ativo, em termos de Direito Penal. É autor quem realiza ou executa o núcleo do tipo penal. O co-autor realiza conjuntamente a conduta criminosa com o autor. O partícipe colabora com o crime sem realizar ou executar o núcleo do tipo. O partícipe moral faz nascer a idéia (induz) ou reforça a ideia para realizar o ato criminoso. Maiores detalhes a respeito de autor, co-autor e partícipe serão abordados em texto específico.

Passamos agora a estudar acerca do sujeito passivo.

O sujeito passivo do crime – o ofendido, ou vítima – é “titular do bem jurídico tutelado pela norma penal, que vem a ser ofendido pelo crime”, ensinam Paulo José da Costa Júnior e Fernando José da Costa (2010, p. 115). O Estado é o sujeito passivo constante de todo o crime pelo fato de a Lei Penal situar-se no ramo predominantemente público, enquanto a pessoa que teve o bem diretamente atingido pelo crime é o sujeito passivo variável.

Também não se pode confundir sujeito passivo do crime com sujeito passivo da ação, alertam Paulo José da Costa Júnior e Fernando José da Costa, visto que sujeito passivo da ação é aquele sobre o qual recai materialmente a ação ou omissão criminosa. “Também não se confunde o sujeito passivo com aquele que suporta o dano. No homicídio, sujeito passivo é o morto; sofrem o dano os familiares. Assume relevo o sujeito passivo sob diversas angulações, inclusive qualificando o interesse jurídico tutelado, como no crime de desacato, que constitui hipótese particular de injúria caracterizada pelo fato de que o ofendido é um funcionário público (art. 331 do CP).” (2010, p. 115).

Em resumo. Sujeito passivo constante (geral, genérico, formal, mediato, ou indireto) é o Estado, titular do *“jus puniendi”*. Sujeito passivo variável (particular, material, acidental, eventual ou direto) é a pessoa física (crimes contra a pessoa, por exemplo) ou jurídica (crimes contra o patrimônio, por exemplo) vítima da lesão ou ameaça de lesão. O sujeito passivo também pode ser indeterminado (coletividade - crimes contra a saúde pública - e família, por exemplo).

Como se sabe, a doutrina criminal aborda todos os pontos de uma tipificação delituosa. Discorre sobre pontos importantes, controvérsias, tipificação classificação, elemento subjetivo, modalidades comissivas e omissivas, objeto material, bem jurídico protegido e sujeito ativo e passivo.

Para este trabalho, é de grande relevância que se deixe claro o que são e quem são os sujeitos ativo e passivo do crime virtual, pois são a partir dessa ideia que, se identifica quem incorreu para a conduta criminosa e quem foi a vítima que teve o bem jurídico lesado.

Há de se vislumbrar que o sujeito ativo será o quem lesiona o sujeito passivo. O sujeito ativo dos crimes virtuais é extremamente difícil de identificar, frente à ausência física do autor do crime. Diante dessa dificuldade de identificar o sujeito ativo do crime, surgiu a necessidade de traçar de se traçar um perfil denominando

grupos que praticam determinados crimes virtuais, dentre essas denominações temos a figura do *“hacker”*.

Segundo a definição de Crespo:

> Hacker é o nome dado aos chamados “piratas” de computador. Essa expressão surgiu nos laboratórios de computação do MIT (Massachusetts Instituteof Technology), onde estudantes passavam noites em claro averiguando tudo o que se podia fazer com um computador (2011, p. 95).

Crespo discorre ainda que *hacker* “é aquele que invade sistemas em benefício próprio, obtendo dados e informações alheias” (2011, p. 95). Entretanto é importante ressaltar, que nem sempre o *“hacker”* será necessariamente um criminoso, pois há aqueles que se dizem *“hackers do bem”*, já que invadem os computadores a fim de alertar o usuário quanto a riscos pertinentes para que busque uma proteção mais efetiva. Outros passam a trabalhar em empresas a fim de desenvolver programas que sejam capazes de frear invasões.

A definição de *“hacker”* constitui-se um tanto genérica, uma vez que se tem outros tipos de nomes para outras condutas delituosas ligada com a informação e banco de dados, porém tais denominações não nos interessam, já que no fim todos esses tipos de criminosos terão um único objetivo, que é de degradar e ofender o bem jurídico tutelado.

Por fim, vale ressaltar, ainda que esteja claro, o sujeito passivo da ação delituosa, será sempre uma pessoa física ou jurídica ou uma entidade titular seja pública ou privada titular do bem jurídico tutelado, sempre haverá o sujeito passivo, ou seja, alguém que está sendo lesado, enfim o que sofre a ação.

Portanto, o sujeito passivo da infração penal pode ser qualquer indivíduo normal, pessoa física, ou até mesmo uma pessoa jurídica, haja vista poder, por exemplo, ter seus bens desviados, seu patrimônio deteriorado ou mesmo ter informações violadas. Ambas são capazes de determinar a ação do agente criminoso.

8 DIRETIVAS INTERNACIONAIS E DIREITO COMPARADO

Primeiramente, cumpre aduzir, que este capitulo é de suma importância para a continuidade do trabalho, uma vez, que para o direito se perfazer em um país, deve-se observar as legislações diversas, para que se busque uma direção correta de determinado tema, assim, ajuda o legislador a traçar pontos importantes para que se possa consolidar uma lei aplicável e eficaz dentro de seu país.

Nos Fóruns internacionais, as análises dos problemas relacionados com os crimes informáticos e das figuras delituosas existentes em diversos ordenamentos jurídicos, bem como sua expressão tipificação e apropriada sanção imposta vêm se perpetuando há anos.

Segundo o nobre doutrinador Crespo:

> Foi na década de 1970 que se notou algum impulso legislativo sobre o assunto, verificando-se os Estados Unidos como o primeiro país a criar regulamentação penal e específica sobre “abuso informático”. Assim, em 1978 foi proposto o “Ribicoff Bill” que, mesmo não sendo aprovado, foi modelo para posteriores propostas legislativas, tendo tido forte influência na elaboração de legislações dos Estados daquele país. Tal projeto reconhecia o valor econômico dos bancos de dados e de *softwares*, incluindo-os na noção que se tinha de propriedade (2011. p, 120).

Como aduz o douto doutrinador Marcelo Xavier de Freitas Crespo, os Estados Unidos, foi o primeiro país a observar e se preocupar acerca dos crimes virtuais. Tomou partida de criar legislação específica a fim de combater a criminalidade virtual, elaborou ainda propostas legislativas para o combate a esta ação criminosa e ainda consolidou o valor econômico de bancos de dados e *“softwares”*. Tal iniciativa foi de grande importância para o direito mundial, pois além de reconhecer que há bens jurídicos que merecem ser apreciados e tutelados pelo Estado, reconheceu ainda o valor econômico de banco de dados e *“softwares”,* sendo de grande importância para o crescimento da economia. Entretanto, verifica-se que a iniciativa dos Estados Unidos teve de abarcar tais condutas no ordenamento jurídico era apenas um começo de uma grande luta contra tais crimes, uma vez, que são de grande complexidade para o legislador combater de forma eficaz.

Abaixo, seguem algumas considerações sobre as discussões correntes em importantes órgãos que tratam, direta ou indiretamente, de aspectos penais relacionados à evolução tecnológica.

8.1 OCDE – ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO

A OCDE trata-se de uma organização mundial que abrange países comprometidos com a democracia e economia de mercado com fins de apoiar o crescimento econômico sustentável, incremento de empregos e de qualidade de vida, estabilidade financeira, assistência a países em desenvolvimento econômico e contribuir para o crescimento do comércio mundial.

A OCDE foi fundada em 1961, em Paris, sendo composta atualmente por 30 países.

A importância da OCDE para o tema é de um trabalho desenvolvido por ela em 1983, no qual desenvolveu um trabalho por uma equipe de *"experts"* em crimes digitais, abordando aspectos penais da criminalidade econômica perpetrada com o uso de computadores além de abordar possíveis alterações legislativas dos países a ela vinculados.

Em 1985 foi apresentado um informe pela OCDE, que se delineou um conceito de crime informático além de se apresentar análise das peculiaridades inerentes à sua forma de realização, incluindo-se, ainda, um inventário sobre a capacidade das legislações nacionais para combater tal crime.

8.2 ONU – ORGANIZAÇÃO DAS NAÇÕES

Em 1985, no sétimo Congresso das Nações Unidas sobre a prevenção do delito e tratamento de delinquentes, houve um informe, no qual foram dedicados dois parágrafos ao direito informático.

Todavia, em 1990, em Havana, que um representante do Canadá preparou uma resolução sobre crimes informáticos. Tal resolução convocava os Estados-Membros a intensificar esforços para combater os crimes digitais. Da mesma forma, o Congresso recomendou que o Comitê para a prevenção e controle de crimes devia promover esforços internacionais para o desenvolvimento e a difusão de diretrizes e normas a serem adotadas pelos Estados-Membros sobre os crimes informáticos e que deviam começar a desenvolver, mais profundamente, estudos para lidar com os problemas decorrentes dos delitos tecnológicos.

8.3 – AIDP – ASSOCIAÇÃO INTERNACIONAL DE DIREITO PENAL

A Associação Internacional de Direito Penal, foi fundada em 1924, a fim de dar continuidade ao trabalho desenvolvido pela União Internacional de Direito Penal. É um órgão para desempenhar o intercâmbio acadêmico e cientifico. É constituída e guiada pelos princípios da Carta das Nações Unidas e da Declaração Universal dos Direitos Humanos. Sua participação acerca dos crimes cibernéticos foi desempenhada através de conferências. Tais conferências foram organizadas até agora pelo ilustre Ulrich Sieber, grande dominador do tema, no qual abordou três assuntos importantes: Fraude informática e Direito Penal Europeu; contribuição das Nações Unidas na persecução e prevenção da criminalidade informática; e delitos informáticos e outros delitos no campo da tecnologia informática.

Tais conferências são de grande relevância para o estudo do tema e sua evolução, pois é através dessas, que se têm a possibilidade de traçar diretrizes internacionais e planejar o combate à esse crime.

8.4 DO DIREITO ESTRANGEIRO

Como se sabe, os crimes digitais estão presentes em todos os países, assim, diante da complexidade das questões jurídicas advindas do incremento do uso da tecnologia e informática, portanto as soluções penais não podem ser tomadas de forma isolada, mas sim de forma conjugada, ou seja, deve haver planos internacionais de uniformização ao combate desse crime, diretrizes traçadas e união entre países.

A lei penal sobre os crimes relacionados com a informática e com os computadores passou por intensas mudanças, desde o conceito de crime digital até as novas formas de cometimento de crime. Segundo Crespo (2011, p. 134) “especialmente a partir dos anos 1970 notou-se um crescente número de reformas legislativa em diversos países”. E ainda aduz que:

> As razões para alteração legal não foram apenas de ordem técnica, mas por conta de mudanças de paradigmas. É que até o meio do século XX os códigos penais protegiam predominantemente coisas tangíveis. Entretanto, próximo ao fim do século passado, o delineamento da sociedade de informação mudou o tratamento dispensado aos bens incorpóreos e às

> informações. Esses novos valores não poderiam ser protegidos da mesma forma que os bens corpóreos, já tradicionalmente tutelados pelo Direito Penal, sendo necessárias novas medidas. Além do mais, o âmbito da criminalidade informática logo se tornou um complexo temário de novas questões 10 (CRESPO, 2011, p. 134).

Apesar da crescente gama de questões jurídicas específicas Sieber (1998, p.25-31) sustenta que se pode falar em uma sistematização de até seis grandes ondas legislativas referentes à criminalidade informática. São elas “proteção da privacidade; direito penal econômico; proteção da propriedade intelectual; conteúdo ilegal e lesivo; aspectos processuais; e leis de segurança”.

Conclui-se, portanto, que os ordenamentos jurídicos em geral têm mecanismos visando coibir a delinquência informática.

Para que fique clara a questão da legislação ao combate dos crimes virtuais, é importante salientar alguns países e suas legislações.

8.4.1 Espanha

A informática na Espanha possui proteção constitucional, na qual dispõe em seu art. 18, parágrafo 4º, que a “lei limitará seu uso para garantir a honra e a intimidade pessoal e familiar dos cidadãos e o pleno exercício de seus direitos”. Através do texto citado, percebe-se que, a Constituição espanhola incide na tecnologia, tendo em vista, que indica a intimidade e honra como bem jurídico a ser protegido.

Podemos citar ainda a Lei Orgânica de n. 5/1992, na qual dispõe sobre o tratamento automatizado de dados, tendo alterado o Código Penal Espanhol, incriminando as condutas acerca de crimes digitais, existe ainda o Real Decreto 1332/1994, que veio regulamentar a citada Lei.

8.4.2 Itália

O Código Penal Italiano regula desde 23 de dezembro de 1993, alguns dos delitos praticados por meio da informática. No parágrafo seguinte explanaremos alguns artigos do Código.

O art. 615 prevê punição para o acesso abusivo a sistema informático ou telemático. A pena é majorada quando a ação é praticada por funcionário público, quando há emprego de violência ou, ainda, quando haja danos ao sistema ou a dados armazenados. No mesmo artigo há sansão para aquele que difundir, abusivamente, senhas e vírus (CRESPO, 2011).

No art. 617 trata-se da punição de instalação de equipamentos como a própria interceptação, impedimento ou interrupção ilícita de comunicação informática ou telemática. No mesmo artigo é punida a conduta de falsificar ou suprimir o conteúdo de comunicação informática ou telemática desde que haja intuito lucrativo ou de causar prejuízo a outrem (CRESPO, 2011).

Já o art. 635 prevê sanção para quem promove dano ao sistema informático e telemático, punindo-se a destruição, deterioração ou inutilização deles ou de qualquer outro (CRESPO, 2011).

Com relação às fraudes, o art. 640 reprime a conduta que altera o funcionamento do sistema informático ou telemático.

8.4.3 Alemanha

Na Alemanha, foi apurado que não há grande incidência quanto aos crimes informáticos, contudo, há dados que demonstram crescimento significativo dessa atividade criminosa.

Os dispositivos legais que reprimem os crimes virtuais, estão inseridas na Segunda Lei de Combate à Criminalidade Econômica, editada e promulgada em 1986, que contém conjunto de normas contra a criminalidade informática.

A legislação alemã deu prioridade em punir ações de comportamentos que atingem o processamento e armazenamento de dados pessoais, o uso abusivo dos sistemas telemáticos, o fenômeno de invasão de computadores pessoais e subtração de informação, o uso ilegítimo de cartões magnéticos, a utilização de redes informáticas por organizações criminosas, autores de delitos econômicos e grupos neonazistas.

Como visto, foi dada mais atenção pelo legislador aos aspectos patrimoniais, esquecendo-se de tutelar, a honra, intimidade e integridade moral.

8.4.4 Holanda

Na Holanda, consideravam-se manipulações informáticas fraudulentas como um tipo penal que lembra o nosso estelionato.

Já na década de 1980, o Departamento de Inteligência da Polícia de Haia vinha registrando diferentes casos de delinquência informática.

Visto então, que havia lacunas no ordenamento jurídico o Comitê Holandês, que foi fundado para analisar a adequação dos textos penais e processuais ao combate aos delitos tecnológicos, apresentou um relatório, dizendo a necessidade de algumas mudanças no ordenamento jurídico. Feito algumas mudanças ainda não era suficiente, pois houve lacunas pelo legislador, bem como a falta de definição de crime virtual.

A legislação se preocupou apenas em proteger os *"softwares"* (leis contra a *"pirataria informática"*). Só no final da década de 1980 que foi implantada e aprovada lei penal específica, promovendo novo entendimento sobre o que eram *"informação"* e *"banco de dados"*. Crespo assevera que trouxe ainda

> Tipos que incriminaram a perturbação da paz informática, acesso não autorizado a sistemas de sabotagem por bomba lógica, cópia ilegal de dados, disseminação de vírus, espionagem informática, interferência na comunicação de dados, falsificação de cartões bancários e pornografia (2011, p. 148).

Pelo texto citado acima, verifica-se que, o ordenamento jurídico Holandês é bem abrangente quanto aos crimes virtuais, atendendo as normativas internacionais sobre o tema.

8.4.5 Chile

O Chile desenvolveu um papel de grande importância acerca dos crimes virtuais, pois foi o primeiro país da América Latina a modificar sua legislação com fins de se modernizar para o combate eficaz dos crimes dessa natureza.

Segundo o grande doutrinador Marcelo Xavier de Freitas Crespo (2011, p. 149) o Chile instituiu "a Lei nº. 19.223, de 28 de maio de 1993, que foi responsável por introduzir tipos penais que versam sobre crimes atentatórios a sistemas de informação".

Trata-se, no entanto de uma lei especial com apenas quatro artigos que dispõe epune aquele que destruir ou inutilizar um sistema e seus componentes ou que impeça ou obstaculize seu bom funcionamento; o acesso e interceptação indevidos em sistemas; e aquele que altere ou destrua dados contidos de um sistema.

Verifica-se, portanto, que os bens jurídicos que o sistema legal do Chile busca tutelar são os meios de informação, banco de dados e componentes funcionais, atendendo pelo menos em parte às diretrizes internacionais.

8.4.6 Argentina

É de notório saber que o governo argentino exerce um forte poder no que tange a liberdade de informação em seu país, pois o governo filtra e veta o que pode ser veiculado para seu povo. A respeito dos crimes virtuais não é diferente.

O ordenamento jurídico argentino, no que tange aos crimes virtuais, parte da regulação do comércio eletrônico, para assim extrair condutas lesivas relevantes.

Um diploma de grande relevância é a Lei n. 24.766, denominada *“Lei do Sistema de Sigilo de Dados”.* Na lei referida aborda condutas que incriminam os que violam informações de cunho comercial (segredo comercial). Outra leique é interessante falarmos é a de n. 25.326, referente ao *Habeas Data,* que tem a função de proteger as informações pessoais arquivadas eletronicamente. Vale ressaltar ainda a Lei n. 11.723, que dispõe sobre propriedade intelectual.

Quanto ao Código Penal argentino, foi recentemente alterado pela Lei n. 26.388, passando a discorrer sobre os crimes digitais, tanto os próprios quanto os impróprios.

Tais artigos punem aquele que armazena qualquer tipo de mensagem que contenha traços ou representações pornográficas de menores de 18 anos. Esse tipo penal é bem parecido com o nosso art. 241 do Estatuto da criança e Adolescente. Pune ainda aquele que abre ou se apodera, sem autorização, de qualquer forma de correspondência, aberta ou fechada, inclusive comunicações eletrônicas ou telegráficas. Foi acrescentado ainda um artigo que incrimina o acesso não autorizado a sistemas informáticos. O código Penal argentino dispõe também como conduta criminosa aquela em que o agente dá publicidade a informações pessoais, inclusive aquelas obtidas por meio eletrônico, porém desde que causem ou passam

causar prejuízo a outrem. Como quase todos os países o agente será punido também quando acessar banco de dados não autorizados protegidos por lei. Por fim o código foi alterado para que incrimine aquele que destruir, inutilizar ou fizer desaparecer dados ou programas informáticos.

Por fim, para encerrar esta parte e darmos seguimento ao trabalho, impende salientar algumas considerações.

No decorrer desde capitulo foi apresentado diferentes órgãos mundiais com fins de estabelecer diretrizes na legislação e uniformizar de modo que se possa ter um controle pré-estabelecido de tais condutas, pois essas iniciativas e procedimentos realizados são de suma importância para que se possam combater estes crimes, tendo em vista, que são crimes de grande complexidade e que ultrapassam fronteiras. Foi visto ainda que os países de modo geral tentam tratar de modo mais coerente tais condutas, contudo, alguns países quedaram-se inertes sobre alguns temas, ou apenas falharam em alguns pontos, pois nota-se que há controvérsias em ordenamentos jurídicos de certos lugares. Entretanto podemos afirmar que de maneira genérica o mundo está caminhando para aperfeiçoar a legislação para proporcionar uma tutela mais eficaz.

9 LEGISLAÇÃO BRASILEIRA

A difusão da internet trouxe mudanças radicais nos hábitos das pessoas, diminuindo as distâncias, interligando culturas e criando um novo modelo de mundo. Nota-se, que com essas mudanças, acarretam também novos tipos penais e o legislador deve estar pronto para enfrentá-las, buscando a solução mais eficaz para tanto, uma vez, que o estado é o único que detém o "*ius puniendi".*

O Brasil está avançando cada vez mais com esse tipo de crime, pois foi criada as Delegacias Especializadas de Repressão a Crimes contra Informática e Fraudes eletrônicas. No âmbito Federal é possível contar com a Unidade de Perícia Informática da Polícia Federal, criada desde 1996 e denominada como SEPFIN (Serviço de Perícia em Informática). O Ministério Público Federal ainda firmou uma parceria com uma organização não governamental denominada SaferNet, que visa receber denúncias de crimes que violem os direitos humanos praticados pelo meio virtual.

Quanto às conferências internacionais a participação do Brasil se consolida a cada vez mais e aborda temas como: perícia forense, estudos realizados com o enfoque sobre a identificação do criminoso virtual. A OAB possui participação de grande relevância, já que grande parte desses estudos vem sendo feito por ela com a elaboração de cartilhas de prevenção destinadas aos usuários de meios de telecomunicação, bem como o custeio de professores e pesquisadores brasileiros no exterior para o estudo dos cibercrimes.

Entretanto, não é suficiente apenas participação de conferencias e realização de estudos, é importante ter uma legislação específica com procedimentos eficazes,proporcionando à investigação penal por meios necessários em legítima conformidade constitucional, respeito ao garantismo penal que permeia o sistema processual brasileiro.

Passamos agora a examinar a legislação implantada no ordenamento jurídico brasileiro.

Inicialmente, havia um projeto de lei n. 84/99 (Azeredo) criado há mais de dez anos, objetivava criminalizar condutas consideradas graves ao meio informático como a pedofilia, o acesso indevido para obtenção de senhas e a disseminação de vírus. Contudo, há que se observar que o projeto possui algumas deficiências e imprecisões, talvez até mesmo devido ao período de sua criação, levando em conta

o avanço tecnológico, pois no decorrer de dez anos trouxe muitas outras formas de insegurança ao meio cibernético. Impende salientar ainda, que por força de incompatibilidade com o avanço social e tecnológico o PL. 84/99 obteve 17 artigos vetados dos seus 23, portanto, percebe-se facilmente que tal projeto não merece prosperar.

Só em 2011 foi criado um novo projeto de lei n. 2793, determinando em suas proposições apenas os crimes mais danosos e graves cometidos no cyber espaço como: invadir dispositivo informático alheio e violar mecanismo de segurança com o fim de obter, adulterar ou destruir dados ou informações sem autorização.

Em 30 de novembro de 2012 a Presidenta Dilma Roussef sancionou a Lei n. 12.737, que Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei n. 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências.

Essa lei que acabou por se denominada popularmente como Carolina Dickman Dieckmann, por abarcar o momento em que a atriz teve suas fotos (arquivos particulares) publicadas na internet, sem sua permissão por uma invasão ao seu computador, podendo a presente ação ser reconhecida como phishing, prevê também o aumento da gravidade da conduta delituosa aumentando a pena de um terço até a metade, se seu alvo for políticos, o Presidente da República, do Senado, da Câmara, do Supremo Tribunal Federal, ou pessoas de alto cargo aos quais é conferida fé pública.

A mencionada lei dispõe sobre a invasão de dispositivo informático, interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública, falsificação de documento particular e falsificação de cartão de crédito ou débito. A lei altera ainda o Código Penal Militar e criminaliza a entrega de dados eletrônicos a um *“inimigo”* do país. A criação de delegacias especializadas em crimes cibernéticos no âmbito das policias civil e federal também foi incluída na lei, mas depende de regulamentação.

Por fim, conclui-se, que o legislador está se preocupando com o tema há pouco tempo, estamos então no inicio de uma luta jurídica, pois percebe-se, que mesmo com essa lei em vigor o nosso sistema legal ainda possui falhas, devendo ter maior amplitude tipificando condutas com mais especificidade, só assim teremos um meio mais eficaz para o combate aos crimes no cyber espaço.

10 CONCLUSÃO

Da leitura deste artigo, notamos que o combate aos crimes cometidos por meio da internet é um grande desafio.

É impostergável a implementação de medidas de combate à criminalidade virtual, que cresce de forma alarmante, a fim de deixarmos a perturbadora posição de *“paraíso dos cibercrimes”.*

Ademais, a urgência na adoção destas medidas pode ser revelada pelo fato de praticantes de outras modalidades delitivas terem migrado para o cibercrime, exatamente pela liberdade de ação que encontram no ambiente virtual. Evidencia-se, desta forma, que a impunidade na rede serve de estímulo para estes criminosos.

O efetivo combate aos criminosos virtuais exige ações multilaterais, visto que as ações isoladas não lograram êxito ao longo do tempo, sendo necessária uma mudança de postura por parte das autoridades. Assim, seria salutar a integração dos setores público e privado, bem como de segmentos da sociedade civil voltados ao combate à criminalidade virtual.

Em termos práticos, defendemos a obrigatoriedade da identificação do usuário para acesso à internet, através de identificação biométrica e validação de dados pessoais gerenciada pela Polícia Federal.

Por outro lado, revela-se imperativa a necessidade de atualização da legislação referente aos crimes de informática, criando-se dispositivos que autorizem a sua revisão automática pelo Poder Legislativo, mediante parecer do Comitê Gestor de Internet, órgão responsável pela administração da internet no Brasil. Tal medida mostra-se coerente com a necessidade de um elevado conhecimento técnico a respeito das questões informáticas para um trabalho legislativo satisfatório e adequado. Ressaltamos que, nesta circunstância o Comitê Gestor da Internet atuaria apenas como órgão consultivo, não tendo qualquer ingerência sobre o trabalho legislativo.

Outrossim, defendemos o combate ao casuísmo legislativo, que, em detrimento ao caráter abstrato da lei, cria uma *“pseudo-legislação”*, fundamentada em situações fáticas concretas, simplesmente com objetivo de atender aos reclames da mídia.

Comparando-se a produção legislativa brasileira relativa ao combate dos cibercrimes com a de países em que esta modalidade criminosa ocorre com menor

incidência, percebemos o atraso no despertamento dos nossos legisladores em sua apreciação.

Atualmente, nota-se um sentimento equivocado de revolta da sociedade contra as autoridades judiciárias, que, por força de uma legislação obsoleta e lacunosa, são constrangidas a ordenar a liberdade de criminosos perigosos. Cumpre-nos informar que a incumbência de tais autoridades é a estrita aplicação da lei, e sendo a lei silente é impossível a manifestação da justiça.

Desta feita, é imprescindível a elaboração de uma legislação consistente, com abrangência sobre as novas condutas delitivas identificadas na rede e a cominação de penas mais severas. Do contrário, as autoridades continuarão impedidas de aplicar as devidas medidas coercitivas contra os criminosos digitais.

Por outro lado, o investimento na formação de policias especializados no combate ao cibercrime é outra medida inadiável. É preciso treinar policiais para investigação preventiva, evitando a consumação do crime, tendo em vista que o criminoso encontra-se numa condição vantajosa em relação às autoridades. Objetivando-se de diminuir esta vantagem, é preciso sair na frente, monitorando as ações mal-intencionadas daqueles que desejam cometer crimes digitais, agindo-se de modo preventivo.

Não obstante, ao judiciário cabe uma interpretação da norma, não somente como letra fria e morta, mas, acima de tudo, e em observância aos preceitos pós-positivistas, uma interpretação da sociedade em que o Direito está inserido, buscando o equacionamento entre conceitos imutáveis e inegociáveis com a realidade moderna, que exige transigibilidade e flexibilidade.

Por fim, por tratar de questões que extrapolam os limites territoriais de qualquer Estado soberano, no que tange ao combate dos crimes transnacionais, somos favoráveis ao estabelecimento de uma competência internacional. Esta competência deve ser estabelecida mediante a celebração de acordos de cooperação internacionais multilaterais.

Seguindo este pensamento, sugerimos a criação de uma Corte Internacional com competência para o processamento e julgamento das ações que tratem de crimes digitais cometidos à distância, medida que terminaria definitivamente com a ideia de impunidade nestas hipóteses.

Sem ações enérgicas de combate aos cibercrimes, os dados de pessoas e empresas que transitam na internet a cada dia continuarão vulneráveis aos ataques

de criminosos, aumentando o número de vítimas e os prejuízos por elas contabilizados.

O fato é que o problema existe, nascendo no mundo virtual, mas causando enormes prejuízos no mundo real, sendo indispensável um esforço conjunto visando o seu combate. É inadmissível a inércia das autoridades, que não podem esquivar-se da tarefa de dar uma resposta a este anseio social.

REFERÊNCIAS BIBLIOGRÁFICAS

BITENCOURT, Cezar Roberto. **Tratado de Direito Penal***.* Parte Geral 1. 10. ed. São Paulo: Saraiva, 2006.

BRASIL. **Constituição da República Federativa do Brasil de 1988.** Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>. Acesso em: 20 out. 2014.

CAPEZ, Fernando. **Curso de Direito Penal**. Parte Geral. Volume 1. 15. ed. São Paulo: Saraiva, 2011.

CASABONA, Carlos Maria Romeo. De los delitos informáticos al cibercrimen: una aproximación conceptual y político criminal. In: _____ (Coord). **El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-crimninales**. Granada: Comares, 2006.

COSTA JR, Paulo José da; COSTA, Fernando José. **Curso de Direito Penal**. 12. ed. rev. atua. São Paulo: Saraiva, 2010.

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

_____. **“A brincadeira do desmaio” e a teoria da imputação objetiva**. Boletim do IBCCrim, Sâo Paulo, v.15, n.185, p.12, abr. 2008.

FERREIRA, Ivette Senise. **Direito & Internet: Aspectos Jurídicos Relevantes**. 2 ed. São Paulo: Quartier Latin , 2005.

GOUVEIA, Flávia. Tecnologia a serviço do crime. **BR – Notícias do Brasil.** Disponível em: <http://www.cienciaecultura.bvs.br/pdf/cic/v59n1/aobv59n1.pdf>. Acesso em: 30 out. 2014.

Instituto Brasileiro de Política e Direito da Informática – IBDI. **Objetivos Sociais**. Disponível em: < http://www.ibdi.org.br/site/objetivos.php>. Acesso em 20 out. 2014.

JESUS, Damásio E. de. apud ARAS, Vladimir. **Crimes de Informática**. Jus Navigandi, Ed. 12, out. 2001. Disponível em: <http://www1.jus.com.br/doutrina/texto.asp?id=2250 >. Acesso em: 25 out. 2014.

NETTO, Alamiro Velludo. **Tipicidade penal e sociedade de risco**. São Paulo: QuartierLatin, 2006.

PRADO, Luiz Regis. *Comentários ao Código Penal.* 6. ed. rev. atua. ampl. São Paulo: RT, 2011.

____. **Curso de Direito Penal Brasileiro.** Volume 1. Parte Geral – arts. 1º a 120. 6. ed. rev. atua. ampl. São Paulo: RT, 2006

_____. **Bem jurídico penal e Constituição**. 2° ed. São Paulo: Rev. Dos tribunais, 1997.

REIS, Maria Helena Junqueira**. Computer crimes**. Belo horizonte: Del Rey, 1997.

ROMEO CASABONA, Carlos M. De Los delitos informáticos AL ciber-crime: una aproximación conceptual y político criminal. In: **(Coord). El cibercrimen: nuevos retos jurídico-penales, nuevasrespuestas político-criminales.** Granada: Comares, 2006.

ROVIRA DEL CANTO, Enrique. **Delincuencia informática y fraudes informáticos.** Granada: Comares, 2002.

ROSA, Fabrizio. **Crimes de Informática**. Campinas: Bookseller, 2002.

ROQUE, Sérgio Marcos. **Criminalidade informática: crimes e criminosos do computador**. São Paulo: ADPESP Cultural, 2007.

SIEBER, Ulrioh. **Computer crime and criminal information law: neuw teds in the international risk information society.** Disponível em: <www.jura.uniwerzburg.de/sieber>. Acesso em 02 nov. 2014.

_____. **Criminalidad informática: peligro y prevención**. In: MIR PUIG, Santiago (Comp.). Delincuenciainformática. Barcelona: PPU, 1992 (Iura n.7).

_____.**The international handbook on computer crime**. New York: Jonh Wiley Sons, 1986.

VIANNA, Tulio Lima**. Do delito de dano e da sua aplicação ao direito penal informático.** Alfa-Redi: rev. De derecho informático, n.62, set, 2003. Disponível em: <http://www.alfa-redi.org/rdi-articulo.shtml?x=1289>. Acesso em: 02 nov. 2014.

_____. **Fundamentos de direito penal informático**. Rio de janeiro: Forense, 2003.