CRIMES DIGITAIS: SEGURANÇA JURÍDICA NA INTERNET

Giovane Saviotti Rodrigues[1]

Orientador: Gustavo Campos Menezes
Co-orientadora: Débora Amaral

Universidade Presidente Antônio Carlos – (UNIPAC)
Rua Palma Bageto Viol s/n Campolide – Antônio Carlos – MG CEP: 36.220-000

RESUMO

Este artigo tem a finalidade de demonstrar o quanto é importante um estudo sobre os crimes digitais, que já estão presentes no dia-a-dia da sociedade e prejudicando não apenas pessoas comuns como também grandes empresas, devido à facilidade com que os criminosos, também chamados de hackers, estão encontrando para praticar alguns delitos e não sofrerem nenhuma sanção pelo crime cometido. Também possui exemplos de como os crimes podem ser praticados por meio do computador e o que a legislação brasileira e mundial têm feito para tentar manter o controle sobre essas novas modalidades de infrações.

1 INTRODUÇÃO

Nos últimos anos o mundo evoluiu bastante em se tratando de tecnologia, apareceram novas formas de comunicação encurtando distâncias entre as pessoas. O computador é um desses avanços tecnológicos e com o surgimento da Internet tornou-se um importante instrumento para as pessoas.

Juntamente com essa nova forma de comunicação, também apareceram as pessoas que se utilizam desse instrumento, que já está acessível para boa parte da população, não para resolver seus problemas ou interagir-se com outras pessoas, mas para cometer crimes.

Esse tipo de infração vem acontecendo com maior freqüência e os criminosos, muitas vezes, acabam impunes. A atual legislação brasileira prevê punição para grande parte dos delitos praticados, mas ainda assim, uma grande parte não possui uma legislação específica que proíba essa prática criminosa.

A legislação mundial também tem vários problemas para tentar punir os culpados, muitos Tratados internacionais estão sendo negociados para tentar coibir e, senão extinguir de vez, pelo menos diminuir consideravelmente esse tipo de

[1] Aluno do 8° período do curso de Ciência da Computação da Universidade Presidente Antônio Carlos.

infração.

O propósito deste artigo é justamente esse, esclarecer melhor, tanto para os profissionais do Direito quanto da Computação, como esses crimes são praticados por meio do computador e até onde a lei pode interferir para tentar solucionar esse problema que perturba não apenas usuários comuns como também grandes e pequenas empresas, além do Governo Federal, que acabam tendo prejuízos enormes, podendo até mesmo chegar a falência.

Na primeira seção será mostrada uma breve história sobre a Internet, como surgiu, qual a sua finalidade inicial e o quanto a Internet evoluiu e mudou até chegar nos dias atuais. Em seguida, na segunda seção abrange-se definições sobre o que é crime para o Código Penal brasileiro, teorias a respeito de como se deve punir, aborda também o que são crimes digitais. Na terceira seção, avalia-se o que a legislação brasileira tem feito para tentar inibir a ação dos criminosos digitais, existe vários exemplos de como podem ser praticados os crimes por meio da Internet e traz as penas para os delitos praticados. Na última seção, trata-se de como a legislação mundial vem agindo para conseguir punir os criminosos, que muitas vezes saem impunes devido aos vários Tratados Internacionais existentes entre os países, e faz uma breve análise de como a legislação de outros Países age perante essas práticas delituosas.

2 A INTERNET E A SUA HISTORICIDADE

A Internet surgiu por volta de 1960 onde o objetivo de todas as pessoas envolvidas no projeto era o grande potencial de trocas e compartilhamento de informações, era um projeto que visava principalmente a pesquisa e fins militares. À partir da II Guerra Mundial os Estados se interessaram para o desenvolvimento e aperfeiçoamento dos computadores, pois, perceberam o grande potencial estratégico que essas máquinas poderiam possibilitar. Na época buscava-se uma troca de informações que pudesse ao mesmo tempo ser rápida e segura[2].

A idéia inicial da Internet era principalmente interligar várias cidades para que no caso de uma guerra nuclear, se alguma fosse destruída, ainda sim se

[2] Informação retirada dos seguintes endereços:
www.aisa.com.br/historia.html
www.malagrimo.com.br/online/olminter.html
http://kpls.cosmo.com.br/matéria.asp?co=11&rv=vivencia

conseguiria manter contato com todas as outras, ou seja, não ocorreria uma interrupção na informação devido aos vários caminhos que poderiam ser utilizados.

As universidades americanas começaram a se interessar pela Internet devido à facilidade de pesquisar e comunicar-se com outros pesquisadores em locais diferentes e distantes. É claro que nessa época era inimaginável onde a Internet iria chegar, mudando, inclusive, a forma de vida das pessoas na atualidade.

Em 1969, foi colocada em execução a ARPANET (nome dado à Internet naquela época), que interligava grandes universidades americanas e que com o sucesso obtido um número grande de adesões ao novo sistema aumentava continuamente. Esse crescimento talvez não tenha sido maior devido à dificuldade encontrada pelas pessoas em utilizar um computador que realmente era muito complicado, pois era necessário que se entendesse bastante de linguagem de máquina e, por isso, poucas instituições aventuraram-se na nova área e a Internet ainda não era muito conhecida. Para tentar uma atração maior pelo sistema pouco conhecido e não muito simples de se manipular, foram surgindo novos softwares com interfaces cada vez mais agradáveis para que as pessoas acabassem com o receio existente entre a máquina e o ser humano, e começassem a usufruir da Internet que tinha como atrativo a troca de idéias, estudos e informações com pessoas conhecidas e desconhecidas.

Hoje, passados alguns anos e com a evolução nesse ritmo desenfreado, a Internet também evoluiu bastante e espalhou-se pelo mundo inteiro através da Web como é mais conhecida atualmente.

Internet é um conjunto de cabos, protocolos, conexões, roteadores, etc, que permite que a pessoa na sua casa consiga trocar informações com seus amigos, acessar uma página de jornal, saber as notícias do esporte, ter acesso a uma infinidade de informações para trabalhos, pesquisas, etc, o que você procura provavelmente conseguirá encontrar na Internet. Ela permite que as pessoas naveguem – linguagem utilizada pelos “internautas” entre milhões de homepages (páginas na Internet), que pessoas totalmente estranhas e que nunca imaginariam se conhecer encontrem-se nos canais de “bate-papo”, o acesso a informação sobre tudo o que acontece no mundo está disponível em questão de minutos. A compra pela Internet já está acontecendo com bastante freqüência, apesar do medo que as pessoas têm em relação a este tipo de negociação. Existe, por exemplo, o receio da não entrega da mercadoria comprada, desta forma, a desconfiança em cadastrar dados pessoais em sites, desconfiança realmente admitida, uma vez que nem todos

os sites são seguros. Em se tratando de Internet é melhor desconfiar, inclusive, do seu melhor amigo, pois muitos e-mails podem chegar como sendo emitidos por nossos amigos quando na verdade são vírus enrustidos que poderão destruir seu computador.

É indiscutível que a Internet tornou a vida da maioria das pessoas muito mais fácil em termos da praticidade de resolução de problemas e é inegável que este já é um caminho sem volta, não é mais possível viver sem esse meio de comunicação que já é o maior dentre todos os existentes em todos os tempos. Qualquer pessoa consegue ter acesso à Internet hoje, basta apenas utilizar o computador em casa ou em local público[3] e desfrutar desse magnífico meio que é um paraíso e um inferno ao mesmo tempo. Paraíso por todas as facilidades descritas anteriormente, e inferno pela quantidade de crimes que estão acontecendo por meio da Internet e, que vem propondo desafios a outras áreas, como o Direito, para tentar controlar esse tipo de abuso que acontece cada vez com maior freqüência, devido talvez ao fato de mais pessoas no mundo inteiro estarem tendo acesso a essa forma de comunicação.

A Internet é um dos grandes desafios que o ordenamento jurídico do mundo inteiro precisa enfrentar a fim de obter uma solução rápida. Crimes são praticados ficando, muitas vezes, os criminosos impunes, devido á falta de uma legislação competente para julgá-los e condená-los. Estes criminosos se aproveitam dessas “falhas” contidas na lei para continuar a prática de condutas que estão prejudicando, de várias maneiras, desde pessoas físicas até as pequenas e grandes empresas e Governo Federal que vêm sendo lesados por causa de invasões nos seus sistemas de informações.

O Direito existe para dar maior segurança à população, preservar a vida, a intimidade e os bens das pessoas. Desta forma, faz-se necessária a promulgação de uma nova legislação que condene o tipo de conduta denominada crime digital, devendo ser colocada em prática antes que a situação fuja ao controle, e a justiça fique de mãos atadas e olhos vendados para esse fato extremamente importante e atual.

3 CRIMES DIGITAIS

[3] Não recomendado para situações extremamente pessoais, pois, um computador que qualquer pessoa pode ter acesso é um grande atrativo para os hackers (criminosos e/ou piratas cibernéticos) agirem.

Com o surgimento da Internet, apareceram várias outras modalidades de crimes que dentro do nosso ordenamento jurídico[4] não possuem uma solução clara e bem definida para esse tipo de prática que vem acontecendo em todo o mundo.

Antes de falarmos de crimes digitais, que é o tema proposto, faz-se necessário um conhecimento sobre o que venha a ser crime, ou, o que nosso sistema jurídico considera crime.

3.1 CONSIDERAÇÕES SOBRE CRIME NA LEI PENAL BRASILEIRA

Conforme o conceito analítico de crime, é preciso que o agente tenha praticado uma ação que possua três características imprescindíveis, são elas: Tipicidade (fato típico), Antijuridicidade (antijurídico) e Culpabilidade[5].

> Fato típico – é o padrão de conduta que o Estado, através da lei, visa impedir que seja praticada. Tipo é a descrição precisa do comportamento humano feita pela lei penal.
> O fato típico possui os seguintes elementos: - conduta dolosa ou culposa, comissiva ou omissiva; - resultado (nos crimes onde se exija um resultado naturalístico.) - nexo de causalidade entre conduta e resultado; -tipicidade (formal e conglobante).
> Antijuridicidade ou ilicitude – é a relação de contrariedade que existe entre a conduta que o agente realiza e o ordenamento jurídico.
> Culpabilidade é a reprovação pessoal que se faz sobre a conduta ilícita do agente.
> A culpabilidade possui os seguintes elementos: - imputabilidade; - potencial consciência sobre a ilicitude do fato; - exigibilidade de conduta diversa.

Deve-se seguir uma ordem determinada na análise do fato praticado por um agente para determinar se é ou não crime, ou seja, devemos analisar primeiramente a tipicidade da conduta, em seguida a antijuridicidade e por final a culpabilidade.

Depois de entendermos o que venha a ser crime, analisemos agora os crimes digitais.

A Internet tornou-se um fato social e desde então o Direito fez-se necessário para garantir a segurança dessas relações e proteger o bem jurídico quando lesionado. O Direito penal surgiu para proteger os bens jurídicos considerados de maior importância para a sociedade, a vida é um exemplo desse

[4] Ordenamento jurídico é a organização da sociedade pelo Direito; rege-se pelo princípio da justiça e abrange todas as atividades relacionadas com a segurança social.
[5] GRECO, Rogério. Curso de direito penal - parte geral, v. I, p. 158-159.

tipo de proteção. A definição de crime é a mesma tanto para delitos comuns quanto para os crimes digitais, ou seja, ação humana, que cause lesão ou perigo contra os bens mais importantes para a sociedade, a conduta humana em ambos os casos está sujeita a uma sanção prevista em lei.

O art 1° do CP[6] diz que: “Não há crime sem lei anterior que o defina. Não há pena sem prévia cominação legal” ·. Esse artigo é aplicável tanto para os crimes digitais quanto para os crimes comuns, pois, não há como punir alguém se o fato cometido não for considerado crime pelo nosso ordenamento jurídico.

Como poderemos julgar alguém que comete algum delito por meio da Internet? A resposta não é tão clara e simples como parece, a informática possui certas particularidades em seu *modus operanti*, e o que separa os crimes digitais dos crimes comuns é a utilização do computador. O nosso Código Penal permite que muitos crimes que são cometidos com o uso do computador sejam enquadrados nos tipos penais descritos, pois quando a conduta humana, seja comissiva ou omissiva, se ajusta na norma repressiva ela está sujeita a uma sanção penal.

As leis brasileiras ainda estão engatinhando dentro de um setor jurídico de proteção aos dados, e apesar da promulgação da lei de Software[7], muito ainda precisa ser feito para que os crimes digitais sejam punidos como a sociedade deseja.

As normas existentes em nosso ordenamento jurídico como o direito do autor, têm sido empregadas na defesa do direito autoral. A lei acima tipificou algumas condutas, sendo certo que elas não são exaustivas nas possibilidades de alguém cometer crimes virtuais, mas com certeza foi o início para que seja elaborada uma codificação. Os crimes cometidos por meio da Internet trazem um enorme desafio para o Direito devido ao grande universo em que agem os criminosos e o alto nível intelectual que os agentes possuem.

Os crimes digitais podem ser cometidos em qualquer lugar do mundo. Uma pessoa que esteja no Japão poderá cometer um crime aqui no Brasil por meio da Internet, e como seria punida essa ação? No nosso ordenamento jurídico consta o princípio da territorialidade, ou seja, local onde o crime foi praticado. Para esse princípio existem três teorias: -teoria da atividade; -teoria do resultado e teoria mista ou ubiqüidade. A esse respeito esclarece GRECO[8]:

[6] Esclareço que CP refere-se à Código Penal.
[7] Lei 9.609 de 19 de fevereiro de 1998.
[8] GRECO, Rogério. Curso de Direito penal – parte geral, v. I, p.136.

> A teoria da atividade diz que lugar do crime seria o da ação ou da omissão, mesmo que outro fosse o da ocorrência do resultado. A teoria do resultado despreza o lugar da conduta e defende a tese de que lugar do crime é onde ocorre o resultado, e teoria mista ou da ubiqüidade adota as duas posições anteriores e diz que lugar do crime será o da ação ou da omissão, bem como onde se produziu ou deveria produzir-se o resultado.

O nosso Código Penal adota a teoria mista ou da ubiqüidade conforme o art 6°[9] aduz: “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".

Existe, também, o princípio da extraterritorialiedade, que é a aplicação da lei penal brasileira àqueles que praticarem infrações penais fora do território brasileiro, ou seja, em países estrangeiros.

A extraterritorialidade pode ser condicionada ou incondicionada, no segundo caso como o próprio nome sugere, é a possibilidade da aplicação da lei penal brasileira a fatos ocorridos no estrangeiro sem que para isso não exista qualquer condição. As hipóteses de extraterritorialidade incondicionada estão previstas no inciso I, alínea b, art 7° do Código Penal que diz[10]:

> Art 7º – Ficam sujeitos à lei brasileira, embora cometidos no estrangeiro:
> I – os crimes:
> a) [...}
> b) contra patrimônio ou a fé pública da União, do Distrito Federal, de Estado, de Território, de Município, de empresa pública, sociedade de economia mista, autarquia ou fundação instituída pelo Poder Público;

3.2 EXEMPLOS DE CRIMES DIGITAIS

A Internet trouxe uma quantidade inimaginável de informações para qualquer pessoa que esteja interessada em pesquisar sobre um determinado assunto. Essa facilidade é apenas uma dentre tantas outras que esse meio de comunicação nos oferece. Esse é o lado bom da Internet. Existe um outro lado, não tão agradável como o anterior, que são os crimes praticados por meio dessa magnífica ferramenta de informação disponível para a população em geral.

Esse tipo de conduta utilizando-se da Internet para que seja realizada, está ferindo direitos de terceiros e conflitando a todo instante com o interesse

[9] BITENCOURT, 2004, op-cit, p.18.
[10] BITENCOURT, 2004, op-cit, p.20.

comum da sociedade.

Dentre os ilícitos cometidos estão, por exemplo: a exposição de sites na Internet com pornografia infantil, que se enquadra no art 241 do Estatuto da Criança e do Adolescente – pedofilia; também o plágio de textos de terceiros que se enquadra no art 184 do Código Penal – violação de direito de autor.

Inúmeros crimes podem acontecer no meio cibernético, como: calúnia, difamação, injúria, ameaça, divulgação de segredo, furto, dano, apropriação indébita, estelionato, violação do direito autoral, escárnio por motivo de religião, favorecimento da prostituição, ato obsceno, escrito ou objeto obsceno, incitação ao crime, apologia ao crime ou criminoso, falsa identidade, inserção de dados falsos em sistemas de informações, adulteração de dados em sistemas de informações, falso testemunho, exercício arbitrário das próprias razões, jogo de azar, crime contra a segurança nacional, preconceito ou discriminação de raça/cor/etnia/etc, pedofilia, crime contra a propriedade industrial, interceptação de comunicações de informática, lavagem de dinheiro e pirataria de software.

Para os tipos de crimes citados anteriormente, não existe a necessidade de uma nova legislação específica, pois, já estão sob o controle da legislação atual. Alguns necessitam apenas de algumas pequenas mudanças para se adaptarem à consumação na Internet.

As condutas que lesam direito relativo a bens ou dados de informática não encontram nenhum tipo de punição dentro da nossa legislação, essas condutas são chamadas de crimes digitais, também conhecidos como crimes informáticos, crimes da Internet, crimes cibernéticos, ou cybercrimes.

4 MODALIDADES DE CRIMES PRATICADOS NA REDE

Os crimes digitais podem ser de várias espécies e praticados de muitas maneiras, e para melhor esclarecer os tipos de crimes citados no capitulo anterior que podem ser cometidos através da Internet, há de se fazer um estudo mais aprofundado sobre alguns mais comuns em nossa sociedade a fim de abolir eventuais dúvidas a respeito de punição, ou seja, saber se o delito cometido possui ou não previsão de pena em nosso ordenamento jurídico, e se possuir, qual será a punição, ou, caso ainda não esteja relacionado dentre os crimes que sofrerão uma sanção como resolver essa situação, nem todas as infrações poderão se encaixar no Código Penal brasileiro, desta forma, o que fazer com os crimes que fogem das

previsões dos legisladores, permanecerão inimputáveis? Para os crimes que nossa lei ainda não possui uma previsão, apesar da freqüência com que vem sendo praticados, seja necessário a criação de um novo ramo do direito chamado direito informático, ou, direito da Internet dentre outras definições existentes para essa nova área.

Existe em tramitação no Congresso Nacional o Projeto de Lei n° 84/99 (VER ANEXO 1), que tipifica os delitos que o nosso Código Penal não é competente para prover uma sanção. Esse tipo de crime ainda estão impunes, apesar da freqüência com que vem sendo praticados a todo instante.

Por se tratar de um artigo e não de uma monografia, e para ficar mais claro o entendimento, serão apresentados por meio de exemplos fictícios, algumas formas que os delitos poderiam ser praticados para depois informar a sanção sofrida.

4.1 CRIMES PRATICADOS CONTRA A PESSOA

Homicídio (art 121 CP) - Fulano invade o banco de dados do CTI de um hospital e altera a lista de remédios que serão aplicados em Ciclano. Uma enfermeira, induzida ao erro pela falsa receita que Fulano modificou, acaba matando Ciclano com uma superdosagem de medicação. A pena que Fulano esta sujeito é de: detenção, de 6 (seis) a 20 (vinte) anos, não levando em conta agravantes e atenuantes;

Crimes contra a honra (art 138 até art 145 CP) – Fulano cria uma página na Internet com o sugestivo título “Eu odeio Ciclano” na qual, além de insultá-lo, descreve ações e fatos caluniosos e/ou difamantes que Ciclano supostamente realiza; as penas para essa conduta variam de acordo com o fato, se for calunia pode chegar a 2 (dois) anos de detenção não levando em conta agravantes e atenuantes; se for difamação pode chegar a 1 (um) ano de detenção sem considerar agravantes e atenuantes;

Induzimento, Instigação ou auxílio a suicídio (art 122 CP) – Fulano e Ciclano conheceram-se pela Internet em uma sala de bate-papo e nunca se viram pessoalmente, passaram a trocar e-mails. Ciclano revela a Fulano uma tragédia ocorrida em sua vida. Este começa a incentivá-lo freqüentemente para que se suicide e até manda uma fórmula de um poderoso veneno para o e-mail de Ciclano, que é encontrado morto ao lado do seu computador e ao ser feito o exame de corpo

de delito fica constatado que Ciclano morreu devido ao veneno que é o mesmo descrito por Fulano em um dos e-mails que enviou a Ciclano.

Este não é um exemplo absurdo, pois, o jornal O Tempo noticiou em 12/08/1999 um grupo americano que criou uma página na Internet, onde esse grupo era a favor do suicídio. Investigações realizadas sobre três pessoas que colocaram cartas no mural do site constataram que duas obtiveram sucesso na tentativa de tirar a própria vida e a outra foi internada em um hospital psiquiátrico. Pena para essa conduta: reclusão, de dois a seis anos, se o suicídio se consuma; ou reclusão, de um a três anos, se da tentativa de suicídio resulta lesão corporal de natureza grave.

Violação de segredo profissional (art 154 CP) – Dr. Fulano, famoso psicanalista, após enorme sucesso no programa televisivo “Auto Ajuda”, cria uma página na Internet na qual analisa casos de seus clientes, citando inclusive seus nomes, e revela detalhes da vida pessoal obtidos durante as sessões de análise. A pena prevista é detenção, de três meses a um ano, ou multa sem considerar agravantes e atenuantes.

4.2 CRIMES COMETIDOS CONTRA O PATRIMÔNIO

Furto (art 155 CP) – Fulano invade o banco de dados de um importante banco e transfere um centavo da conta de cada cliente para uma conta fantasma. A pena prevista é reclusão, de 1 (um) a 4 (quatro) anos, e multa, fora os agravantes e atenuantes.

Estelionato (art 171 CP) – Fulano utiliza-se de um programa que cria números de CPF e Cartões de credito falsos e de posse desses números, realiza uma série de compras em diversas paginas na Internet debitando a conta no cartão de crédito falso. Pena prevista de reclusão, de 1 (um) a 5 (cinco) anos, e multa, fora agravantes e atenuantes.

4.3 CRIMES CONTRA A PROPRIEDADE IMATERIAL

Violação de direito autoral (art 12, Lei 9609/98)[11] – Fulano cria uma pagina na Internet e disponibiliza o download de diversos programas completos gratuitamente. Essa é a modalidade de crime mais comum na Internet atualmente.

[11] art 12, lei n° 9.609 de 19 de fevereiro de 1998.

Concorrência desleal (art 195, Lei 9.279/96)[12] – Fulano, dono de uma famosa fábrica de refrigerantes, cria uma página na Internet divulgando que uma pesquisa realizada comprovou que os produtos de seu concorrente possuem substâncias cancerígenas.

4.4 CRIMES CONTRA OS COSTUMES

Pedofilia – divulgação de pornografia infantil (art 241 do Estatuto da Criança e do Adolescente (ECA)[13] – Fulano cria uma página na Internet onde expõe fotos pornográficas de crianças e adolescentes.

Favorecimento da prostituição (art 228 CP) – Fulano cria uma página na Internet com fotos e anúncios de prostitutas. Além disso, Fulano envia e-mails a várias garotas convidando-as a publicarem anúncios em sua página se oferecendo como prostitutas. A pena nessa modalidade é reclusão, de 2 (dois) a 5 (cinco) anos, sem considerar agravantes e atenuantes.

Rufianismo (art 230 CP) – Fulano na sua página, possibilita ainda a contratação on-line das garotas, que atendem em domicílio, e a conta pode ser debitada no cartão de credito do "usuário". A pena no caso é reclusão, de 1 (um) a 4 (quatro) anos, e multa, sem levar em conta agravantes e atenuantes.

Esses crimes dos arts. 228 e 230 estão cada vez mais freqüentes, basta apenas uma rápida procura em algum site de busca que se tem uma idéia do tamanho do problema.

4.5 CRIMES CONTRA A INCOLUMIDADE PÚBLICA

Tráfico de drogas (art 12, Lei 6.368/76)[14] e Tráfico de armas (art 10, Lei 9.437/97)[15] – Fulano cria uma página na Internet onde anuncia a venda de armas e drogas em todo o território nacional com entrega a domicilio.

4.6 CRIMES CONTRA ADMINISTRAÇÃO PÚBLICA

Inserção de dados falsos em sistemas de informações (art 313-A CP) –

[12] art 195, lei n° 9.279 de 14 de maio de 1996.
[13] Lei n° 8.069 de 13 de julho de 1990.
[14] art 12, lei n° 6.368 de 21 de outubro de 1976.
[15] art 10, lei n° 9.437 de 20 de fevereiro de 1997.

Fulano, funcionário publico autorizado, acessa o banco de dados do INSS, inseri dados falsos e modifica vários outros que estavam corretos para obter vantagem para ele próprio e para seus familiares. A pena prevista é reclusão, de 2 (dois) a 12 (doze) anos e multa.

Modificação ou alteração não autorizada de sistema de informações (art 313-B CP) – Fulano, funcionário público não autorizado, invade o banco de dados do INSS, altera todo o sistema de informações sem nenhuma autorização de autoridade competente. A pena prevista é detenção, de 3 (três) meses a 2 (dois) anos, e multa.

4.7 OUTRAS FORMAS DE CRIME

Ultraje a culto e impedimento ou perturbação de ato a ele relativo (art 208 CP) – Fulano invade uma página religiosa e deixa mensagens criticando Ciclano, que ele sabe ser freqüentador habitual da página, por estar perdendo tempo visitando uma página religiosa na Internet. A pena será de detenção, de 1 (um) mês a 1 (um) ano, e multa, se considerar agravantes e atenuantes;

Violação de correspondência (art 151 CP) – Fulano usando um programa de computador para descobrir senhas se apodera da senha do e-mail de Ciclano e começa a controlar toda a correspondência eletrônica que é destinada a este, chegando até a apagar alguns e-mails importantes. A pena prevista é detenção de 1 (um) a 6 (seis) meses e multa.

Falsa identidade (art 307 CP) – Fulano, em uma sala de bate-papo, finge ser desafeto de Ciclano para prejudicar-lhe a imagem perante seus amigos ou outras pessoas, xingando-os de várias formas. A pena é detenção, de 3 (três) meses a 1 (um) ano, ou multa, se o fato não constitui elemento de crime mais grave.

Esses são apenas alguns exemplos dos crimes que podem ocorrer na prática e que o nosso sistema jurídico estabelece sanções. Existem vários delitos que não conseguem punição muitas vezes não por falta de legislação para o fato, mas sim, devido às próprias leis que esbarram nas fronteiras dos Países, onde, para que se resolva esse conflito de normas são necessários vários fatores, dentre eles os Tratados Internacionais que regem as leis pelo mundo impossibilitando muitas vezes que uma infração seja devidamente punida, e muitos criminosos sabendo dessas lacunas na legislação se aproveitam para cada vez mais cometerem essa prática de crimes que se torna mais comum a cada dia.

5 LEGISLAÇÃO MUNDIAL

A Internet facilita o desenvolvimento cultural e social da sociedade, permitindo que um número ilimitado de pessoas tenha acesso a essa tecnologia todos os dias.

Paralelamente a este avanço surgiram novas formas de conduta anti-social transformando os equipamentos de informática em meios de delinqüência e infrações.

Como esse tipo de crime ocorre no mundo inteiro, é necessário que todos os países imponham leis específicas tratando desse assunto, que a cada dia atormenta mais a vida, principalmente, das grandes empresas.

A Organização das Nações Unidas (ONU), reconheceu que esse tipo de delito é um grande problema, já que vários países ainda não adequaram suas legislações mediante a criação de novos tipos penais e procedimentos investigativos, que pudessem ser colocados em prática para coibir o crescimento dos crimes digitais.

Já os Países membros da União Européia, possuem uma regulamentação mais abrangente no campo da informática, incluindo a segurança de dados, as criações intelectuais relativas à informática, defraudação informática, entre outros. Contudo, estabelecem como condição de acesso aos seus arquivos policiais que o país solicitante tenha legislação protetora da privacidade informática.

Países como a Alemanha, a França, a Itália e a Áustria já criaram uma lei específica quanto à privacidade de dados e informações, enquanto que a Argentina e a Espanha optaram pela inclusão em seus Códigos Penais, da tipificação de delitos ligados ao sigilo de dados e a privacidade de informações.

5.1 LEGISLAÇÃO ESPECÍFICA DE ALGUNS PAÍSES[16]

A Alemanha promulgou em 1986, lei tratando da criminalidade econômica na qual estão previstos os crimes de espionagem e de sabotagem de dados.

Na Áustria está previsto o crime de destruição de dados no Código Penal.

[16] http://www.america-net.com.br/bussines_segurança_contexto.asp

Na França a Lei 88/19 de 1988 dispõe sobre crimes de informática, tais como destruição de bases de dados, acesso fraudulento e falsificação de documentos informatizados.

Nos Estados Unidos há lei federal de abuso computacional promulgada em 1994.

5.2 NECESSIDADE DE REGULAMENTAÇÂO INTERNACIONAL

A tipificação desse tipo de delito pelas legislações de todos os Países é de extrema urgência, visto que as relações negociais no âmbito realizadas através da Internet crescem rapidamente e, movimentam anualmente bilhões de dólares entre as diferentes nações.

Devido a esse crescimento, em reunião extraordinária do "Conselho da Europa", realizada em Bruxelas, foi aprovada a primeira convenção internacional sobre os "cybercrimes".

A medida adotada por este organismo internacional, que integra a União Européia, pretende definir uma forma de política criminal comum a todos os Estados-Membros, sobre a utilização de redes de dados e de informações eletrônicas para atividades ilegais e/ou terroristas.

Dentre as atividades consideradas criminosas, e que são abrangidas pelo "Tratado Internacional sobre o Cybercrime", encontram-se: a distribuição de pornografia infantil na Internet; a violação das leis do copyright; a violação dos sistemas de segurança e, uma série de fraudes relacionadas com computadores. Deverá ainda, ser objeto de inclusão, um protocolo adicional, que caracterizará a publicação de material racista na Internet, como uma forma de "ofensa criminal".

É de bom dizer, que a União Européia, vem trabalhando a cerca de 04 (quatro) anos, na redação deste Tratado Internacional, juntamente com os Estados Unidos, Canadá e Japão, o objetivo maior é a criação de um instrumento que estabeleça regras e condições, para que se possa proteger a sociedade mundial das práticas de crimes eletrônicos.

A tendência mundial está sendo direcionada para a criação de uma legislação padrão, que deverá ser adotada por todos os Países participantes, devido ao ilimitado alcance que a Internet possui, superando as fronteiras territoriais e os limites geográficos entre as nações.

Para exemplo de como se faz necessário esse Tratado, basta lembrar

a invasão dos principais "websites" da rede mundial de computadores (Internet), pela impiedosa ação dos "hackers", que propositalmente tiraram inúmeros portais do ar, impedindo a oferta de bens e serviços aos usuários da rede.

Economicamente, não é fácil quantificar a dimensão dos prejuízos causados por uma invasão desta e mesmo de outras modalidades de ataques, como as que foram realizadas por criminosos eletrônicos chineses, que invadiram as páginas do governo dos Estados Unidos, para protestar contra o bombardeio da Embaixada da China em Belgrado, ou em face da suspensão das atividades do Lloyds em Londres, e ainda a constatação da American Express e da Discover que vários números de seus cartões haviam sido descobertos e publicados ensejando sua substituição.

Exemplos como estes, demonstram que os Países necessitam urgentemente de mecanismos tecnológicos e legislativos, voltados para a aplicação das conseqüentes sanções aos delitos eletrônicos, para que de maneira firme e impiedosa, os criminosos virtuais, sejam desencorajados a execução de tais condutas ilegais, mostrando a esses delinqüentes que a sua identificação na rede não é uma tarefa de muita dificuldade, ou até mesmo para os que não acreditam, considerada como impossível.

6 CONCLUSÃO

È certo que nosso ordenamento jurídico precisa de mudanças e soluções rapidamente para tentar deter essa prática de crimes que a cada dia aumenta sem que haja punição, ou melhor, punição adequada para esses delitos. Uma legislação específica aos crimes da Internet, no meu entender, é a melhor solução, pois, além de evitar lacunas na lei, facilita para que as pessoas envolvidas na resolução dos problemas consigam de forma mais clara e rápida uma solução competente e eficaz.

As pessoas envolvidas na área da computação também necessitam fazer a sua parte para estar sempre um passo à frente dos criminosos digitais, evitando assim, ter que esperar que esses invasores pratiquem seus atos ilícitos para que, apenas após o fato consumado, venha surgir uma solução na área da segurança.

Os próprios hackers que, na maior parte, possuem uma inteligência

acima da média e que não possuem o propósito de prejudicar a vida alheia[17], devem fazer parte dos projetos a serem elaborados para garantir maior segurança, tanto para grandes e pequenas empresas, ao governo federal, até aos usuários caseiros, pois todos correm os mesmos riscos em se tratando de crimes praticados pela Internet, claro que sites como o do governo e de grandes empresas possuem uma segurança extremamente superior à de usuários caseiros, mas mesmo assim não afasta o risco de invasão e se tornam os alvos prediletos dos criminosos.

Esses hackers podem ajudar na elaboração de programas que ajudam a protegerem-se de outros hackers com fins maldosos, podem colaborar no estudo de técnicas avançadas sobre segurança em rede e banco de dados, pois é indiscutível o conhecimento cientifico e tecnológico que algumas dessas pessoas possuem, dentre tantas outras formas de ajuda que venham a oferecer. E então porquê não usá-las para praticar o bem ao invés do mal? Isso já vem ocorrendo há algum tempo em algumas grandes empresas, estas contratam os hackers para trabalharem na área da segurança em informática e estão pagando uma boa remuneração para a prestação desses serviços.

Os Países do mundo necessitam entrar em acordo para eliminar fronteiras quando se tratar de crimes digitais, como vimos no estudo, para esses delitos não é tão difícil achar o culpado, desde que se descubra logo sobre a ocorrência do crime.

Os projetos de lei em curso nas nossas casas legislativas deveriam ser vistos com um maior interesse pelos congressistas, para inserir rapidamente em nosso ordenamento leis que inibam a prática dessas infrações, reduzindo assim os riscos de prejuízos a todos que utilizam dessa ferramenta de informação tão poderosa e ao mesmo tempo tão perigosa.

A Internet é um caminho sem volta, e quem precisa se adaptar a ela é o Direito e não o contrário.

Como trabalhos futuros, podem ser realizadas pesquisas sobre jurisprudências para analisar situações (cenários) reais.

REFERÊNCIAS BIBLIOGRÁFICAS

BITENCOURT, Cezar Roberto. *Código Penal comentado*. 2. ed. atual. São Paulo:

[17] Existem os Hackers que são os indivíduos com intenção de prejudicar a outras pessoas e existem os Crackers que apenas invadem os computadores alheios por pura diversão e sem nenhum propósito de prejudicar outras pessoas, fazem isso apenas pelo desafio de conseguirem “furar” a segurança dos computadores.

Saraiva, 2004.

GRECO, Rogério. *Curso de direito penal*. 5. ed. Rio de Janeiro: Impetus, 2005.

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

Disponível em: http://www.navedapalavra.com.br/resenhas/ainformatica.htm

Acesso em: 01/03/2005

Disponível em: http://www.alfa-redi.org/revista/data/32-5.asp

Acesso em: 01/03/2005.

Disponível em: http://www.falke.com.br/estadodeminas.htm

Acesso em: 24/02/2005

Disponível em: http://www.aldemario.adv.br/infojur/conteudo6texto.htm

Acesso em: 02/03/2005.

Disponível em: http://www1.jus.com.br/doutrina/texto.asp?id=3271

Acesso em: 24/02/2005.

Disponível em: http://www.paremasmaquinas.com.br/et007.htm

Acesso em: 24/02/2005

Disponível em: http://nvdark.vilabol.uol.com.br/submundodosHackers.htm

Acesso em: 24/02/2005

Disponível em: http://www1.jus.com.br/doutrina/texto.asp?id=1828

Acesso em: 25/05/2005

Disponível em: http://www.inlimine.hpg.ig.com.br/crimesvirtuais.htm

Acesso em: 25/05/2005

Disponível em: http://www.advogadocriminalista.com.br/home/cybercrimes/0011.html

Acesso em: 18/05/2005

ANEXO 1

Projeto de Lei n° 84/99 – Deputado Luiz Piauhylino

Dispõe sobre os crimes cometidos na área de informática, suas penalidades e dá outras providências.

O Congresso Nacional decreta:

CAPÍTULO I

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

Art. 1° - O acesso, o processamento e a disseminação de informações através das redes de computadores devem estar a serviço do cidadão e da sociedade, respeitados os critérios de garantia dos direitos individuais e coletivos e de privacidade e segurança de pessoas físicas e jurídicas e da garantia de acesso às informações disseminadas pelos serviços da rede.

Art 2° - É livre a estruturação e o funcionamento das redes de computadores e seus serviços, ressalvadas as disposições específicas reguladas em lei.

CAPÍTULO II

DO USO DE INFORMAÇÕES DISPONÍVEIS EM COMPUTADORES OU REDES DE COMPUTADORES.

Art. 3° - Para fins desta lei, entende-se por informações privadas aquelas relativas a pessoa física ou jurídica identificada ou identificável.

Parágrafo único. É identificável a pessoa cuja individuação não envolva custos ou prazos desproporcionados.

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

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

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

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

CAPÍTULO III

DOS CRIMES DE INFORMÁTICA

Seção I

Dano a dado ou programa de computador

Art 8° - Apagar, destruir, modificar ou de qualquer forma inutilizar, total ou parcialmente, dado ou programa de computador, de forma indevida ou não autorizada.

Pena: detenção, de um a três anos e multa.

Parágrafo único. Se o crime é cometido:

I – contra o interesse da União, Estado, Distrito Federal, Município, órgão ou entidade da administração direta ou indireta ou de empresa concessionária de serviços públicos;
II – com considerável prejuízo para a vítima;
III – com intuito de lucro ou vantagem de qualquer espécie, própria ou de terceiro;
IV – com abuso de confiança;
V – por motivo fútil;
VI – com o uso indevido de senha ou processo de identificação de terceiro, ou
VII – com a utilização de qualquer outro meio fraudulento.
Pena: detenção, de dois a quatro anos e multa.

Seção II

Acesso indevido ou não autorizado

Art 9° Obter acesso, indevido ou não autorizado, a computador ou rede de computadores.

Pena: detenção, de seis meses a um ano e multa.

Parágrafo primeiro. Na mesma pena incorre quem, sem autorização ou indevidamente, obtém, mantém ou fornece a terceiro qualquer meio de identificação ou acesso a computador ou rede de computadores.

Parágrafo segundo. Se o crime é cometido:

I – com acesso a computador ou rede de computadores da União, Estado, Distrito Federal, Município, órgão ou entidade da administração direta ou indireta ou de empresa concessionária de serviços públicos;
II – com considerável prejuízo para a vítima;

III – com intuito de lucro ou vantagem de qualquer espécie, própria ou de terceiro;
IV – por abuso de confiança;
V - por motivo fútil;
VI – com uso indevido de senha ou processo de identificação de terceiro; ou
VII – com a utilização de qualquer outro meio fraudulento.

Pena: detenção, de um a dois anos e multa.

Seção III
Alteração de senha ou mecanismo de acesso a programa de computador ou dados

Art 10° - Apagar, destruir, alterar, ou de qualquer fama inutilizar, senha ou qualquer outro mecanismo de acesso a computador, programa de computador ou dados, de forma indevida ou não autorizada.

Pena: detenção de um a dois anos e multa.

Seção IV
Obtenção indevida ou não autorizada de dado ou instrução de computador

Art 11° - Obter, manter ou fornecer, sem autorização ou indevidamente, dado ou instrução de computador.

Pena: detenção, de três meses a um ano e multa.

Parágrafo único. Se o crime é cometido:

I – com acesso a computador ou rede de computadores da União, Estado, Distrito Federal, Município, órgão ou entidade da administração direta ou indireta ou de empresa concessionária de serviços públicos;
II – com considerável prejuízo para a vítima;
III – com intuito de lucro ou vantagem de qualquer espécie, própria ou de terceiro;
IV – por abuso de confiança;
V - por motivo fútil;
VI – com uso indevido de senha ou processo de identificação de terceiro; ou
VII – com a utilização de qualquer outro meio fraudulento.

Pena: detenção, de um a dois anos e multa.

Seção V
Violação de segredo armazenado em computador, meio magnético, de natureza magnética, óptica ou similar

Art 12° - Obter segredos, de indústria ou comércio, ou informações pessoais armazenadas em computador, rede de computadores, meio eletrônico de natureza magnética, óptica ou similar, de forma indevida ou não autorizada.

Pena: detenção, de um a três anos e multa.

Seção VI
Criação, desenvolvimento ou inserção em computador de dados ou programa de computador nocivos

Art 13° Criar, desenvolver ou inserir, dado ou programa em computador ou rede de computadores, de forma indevida ou não autorizada com a finalidade de apagar, destruir, inutilizar ou modificar dado ou programa de computador ou de qualquer forma dificultar ou impossibilitar, total ou parcialmente, a utilização de computador ou rede de computadores.

Pena: reclusão, de um a quatro anos e multa.

Parágrafo único. Se o crime é cometido:

I – com acesso a computador ou rede de computadores da União, Estado, Distrito Federal, Município, órgão ou entidade da administração direta ou indireta ou de empresa concessionária de serviços públicos;
II – com considerável prejuízo para a vítima;
III – com intuito de lucro ou vantagem de qualquer espécie, própria ou de terceiro;
IV – por abuso de confiança;
V - por motivo fútil;
VI – com uso indevido de senha ou processo de identificação de terceiro; ou
VII – com a utilização de qualquer outro meio fraudulento.

Pena: reclusão, de dois a seis anos e multa.

Seção VII
Veiculação de pornografia através de rede de computadores

Art 14° - Oferecer serviço ou informação de caráter pornográfico, em rede de computadores, sem exibir, previamente, de forma facilmente visível e destacada, aviso sobre sua natureza, indicando o seu conteúdo e a inadequação para criança ou adolescentes.

Pena: detenção, de um a três anos e multa.

CAPÍTULO IV

DAS DISPOSIÇÕES FINAIS

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

Art 6° - Nos crimes definidos nesta lei somente se procede mediante representação do ofendido, salvo se cometidos contra o interesse da União, Estado, Distrito Federal, Município, Órgão ou entidade da administração direta ou indireta, empresa concessionária de serviços públicos, fundações instituídas ou mantidas pelo poder público, serviços sociais autônomos, instituições financeiras ou empresas que explorem ramo de atividade controlada pelo poder público, casos em que a ação é pública incondicionada.

Art 17° - Esta lei regula os crimes relativos à informática sem prejuízos das demais comunicações previstas em outros diplomas legais.

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