Universidade Presidente Antônio Carlos - UNIPAC

FACULDADE DE DIREITO

BACHARELADO EM DIREITO

VICTOR LIMA FRAIZOLI

CRIMES DIGITAIS

JUIZ DE FORA

2009

Universidade Presidente Antônio Carlos - UNIPAC

FACULDADE DE DIREITO

BACHARELADO EM DIREITO

VICTOR LIMA FRAIZOLI

CRIMES DIGITAIS

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

JUIZ DE FORA

2009

FOLHA DE APROVAÇÃO

VICTOR LIMA SCAIZON

Aluno

CRIMES DIGITAIS

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

CARLOS ANDRÉ TELUSO

LUIS CLÁUDIO ALVES TORRES

FRANCISCO DE ASSIS BELGO

Aprovada em 04 / 11 / 2009.

Agradeço ao professor e orientador Carlos André Peluso, pelo apoio e encorajamento contínuos na pesquisa, aos demais Mestres da casa, pelos conhecimentos transmitidos, e à Diretoria do curso de graduação da Universidade Presidente Antônio Carlos pelo apoio institucional e pelas facilidades oferecidas.

"O mais importante é demonstrar que todo mundo é vulnerável e pode ser manipulado, principalmente os que se julgam mais inteligentes".

Kevin David Mitnick

SUMÁRIO

RESUMO

Nos dias atuais se torna mais comum para o cidadão a convivência com sistemas automatizados, tais como: caixas eletrônicos, urnas eletrônicas, home banking, com a internet em si, computadores no trabalho, em casa, esse trabalho tem como objetivo esclarecer pontos no que cerne os ditos "crimes digitais", objetivando mostrar sua tipificação através da inviolabilidade das informações previstas Carta Magna de 1988, veremos aqui também os sujeitos do delito já que mostraremos também que há uma ofensa a um bem juridicamente tutelado, bem como também abordaremos os tipos de crimes que pode ser cometidos através da internet.

Trabalharemos a idéia de tempo e local do crime, o que hoje ainda gera controvérsias no que tange o tempo e o local e como a lei incidirá sobre o agente, a jurisdição e a competência o que também hoje ainda gera longas discussões sobre quem tem a competência e a jurisdição para poder julgar crimes eletrônicos

Aqui também será demonstrado o *inter criminis*, como e quais são as fases de um delito eletrônico.

Abordaremos os crimes mais comuns praticados pela internet, os crimes contra a honra, e a violação de correspondência eletrônica, o uso de *e-mails* como prova nos processos.

Abordaremos aqui a possibilidade da restrição de direitos no que tange o uso do computador pelo agente que comete um crime digital.

Um breve comparativo das legislações européias, Sul-americana, norte-americana visando uma breve noção de uma futura legislação que hoje se encontra na forma de projeto de lei.

INTRODUÇÃO

Primeiramente teremos de diferenciar as terminologias aplicadas aos "invasores" de sistemas, primeiramente temos os "hackers" nos quais encontramos vários níveis, seguindo a ordem hierárquica do menos para o maior temos: newbie/tool kit, cyberpunks, internals, coders, old guard hackers, professional criminals, cyber terrorist, essas categorias variam de acordo com o nível de conhecimento do hacker, e encontramos também a figura do cracker, que é o pirata digital, no qual se dedica para descobrir como tornar um programa "shareware" uma versão "full" através dos códigos e seriais dos programas, é importante também diferenciarmos hardware e software, hardware é a parte física do computador, composta de processador, memória RAM, HD, placa mãe, outras placas, e software são os programas, a parte lógica do computador, sendo que existem três tipos de software, shareware, freeware, trial version, sendo que os crackers tentam burlar as licenças de uso das versões shareware e trial version dos programas, e agem também nos programas de código fechado, para poderem criar "portas" de entrada no sistema automatizado.

Temos também que diferenciar tipos de redes computacionais, o primeiro tipo são as redes locais (LAN) onde os computadores se encontram fisicamente, próximos uns dos outros e o segundo tipo de rede existente são as redes que os computadores estão fisicamente longe uns dos outros essa é a rede (WAN). É necessário que se faça a diferenciação dos tipos de acesso, primeiramente temo o acesso local ou off line, onde o invasor pratica o delito de invasão no próprio sistema, podendo esse se dar às escondidas ou, mesmo, por grave ameaça à pessoa ou mediante violência, secundariamente temos o acesso remoto ou on line, o acesso remoto é o mais comum nas invasões de sistemas computacionais e o meio mais comum é a internet, não havendo nenhum contato físico do hacker com o computador invadido, mas para facilitar o acesso remoto, nasce a figura do cavalo de tróia, que é um programa que pode vir na forma de um jogo, apresentação de power point, figuras etc, que contém em seu código

fonte uma programação que "abre" as portas suscetíveis de invasão para que o hacker que programou o cavalo-de-tróia tenha o acesso facilitado por meio desse programa.

Antes de vermos qualquer conceito sobre "crimes digitais" que aqui denominaremos delitos informáticos, farei uma análise sobre os vários primas que um delito informático pode ser praticado, tanto socialmente, como tecnicamente.

Em alguns países notaremos que a legislação, protege muito bem as informações nos sistemas automatizados, entenda-se sistemas automatizados como todos os sistemas que não necessitam da interferência humana, sendo essa interferência somente tolerada para iniciar as funções dos sistemas automatizados.

Analisemos a invasão dos sistemas para a simples obtenção de informações ou para tão somente a invasão propriamente dita para obtenção de prestigio junto à comunidade "hacker".

Fazendo uma análise criminológica, não podemos comparar criminosos informáticos, com homicidas, estupradores.

Segundo TÚLIO LIMA VIANNA[1]:

> *"(...) não cremos que os fatores que movam um homicida sejam os mesmos que impulsionam um estuprador. Buscar semelhanças em Iseus comportamentos sobre o pretexto que ambos são criminosos não nos parece ser o melhor método para se trabalhar a criminologia."*

Mas fazendo uma analise vemos que um crime informático antes de ser cometido, tem que ser aprendido, pois diferente de um homicídio ou um estupro que não necessitam há uma primeira vista de nenhum conhecimento específico ou mesmo técnico para a sua execução diferente dos crimes informáticos, nos quais há uma necessidade de profundo conhecimento técnico, para sua execução.

Segundo SUTHERLAND, E. H.[2]:

---

1 LIMA VIANNA, Túlio. Fundamentos de Direito Penal Informático

> *"(...) A hipótese aqui sugerida em substituição das teorias convencionais, é que a delinqüência de colarinho branco, propriamente como qualquer outra forma de delinqüência sistemática, é aprendida; são aprendida em associação direta ou indireta como os que já praticaram o comportamento criminoso, e aqueles que aprendem este comportamento criminosos não tem contatos freqüentes e estreitos com o comportamento conforme a lei. O fato de uma pessoa torne-se ou não um criminoso é determinado, em larga medida, pelo grau relativo de freqüência e de intensidade de suas relações com os dois tipos de comportamento. Isto pode ser chamado de processo de associação diferencial."*

Por mais significativa parcela dos hackers e crackers, afirmarem serem autodidatas, não restam dúvidas que grande parte das técnicas de invasão de computadores são ensinadas por hackers ou crackers mais experientes, na própria internet. Uma breve busca do termo "hacker" nos mecanismos de buscas (Google, altavista, cadê), encontrará centenas de páginas que trazem tanto definições, quanto programas que servem para invadir computadores pela rede entendam-se rede tanto as redes internas 2como as redes externas, bem como a internet.

Temos também a figura da engenharia social praticada pelo famoso hacker Kevin Mitnick, que conseguiu inúmeras senhas para sistemas computacionais através da falha humana, ele se fazia passar por um técnico do departamento de informática. As vítimas inocentemente passavam suas senhas na crença de se tratar de uma pessoa autorizada, para o hacker poder traçar um *"footprint"* (ato de traçar um perfil do sistema a ser invadido, buscado suas fraquezas e defesas contra invasões) de muitos sistemas por ele invadidos.

Existem também os ataques de força bruta onde há uma conferência de uma par ordenado de usuário e senha, ambas as informações são gravadas em um banco de dados, a utilização da força bruta ocorre no sentido de um programa fazer a experimentação de senhas, letras por letras ou sentenças por sentenças, com base no

2 SUTHERLAND, E.H. White-collar crimilality in American sociological Review, V, p. 11, 1940 apud BARATTA, 1999

perfil do usuário, por exemplo, se o usuário a ser invadido é um profissional da área jurídica, o hacker utiliza um banco de dados com palavras e sentenças jurídicas.

Analisaremos também o elemento volitivo dos delitos informáticos, bem como o local e o tempo do crime de acordo com as teorias adotadas pelo Código penal, a competência para julgar os delitos digitais que pode variar de acordo com o meio utilizado para o cometimento do delito, a admissibilidade da tentativa, seus sujeitos passivo e ativo.

CAPÍTULO I – CRIMES DIGITAIS PENALMENTE CLASSIFICADOS

2.1. Conceito

Analisaremos aqui, o crime digital, na forma do acesso não autorizado a sistemas computacionais, o acesso em si não é crime já que não é previsto pelo nosso ordenamento jurídico, já que crime é toda conduta típica, antijurídica e culpável, o acesso não autorizado a computadores, seria uma conduta atípica, uma vez que não está descrita em nenhum do tipos penais existentes, o que nos leva a fazer um comparativo com a doutrina no conceito material de crime segundo Fragoso[3]:

> *"(...)sob o aspecto material é um crime um desvalor da vida social, ou seja, uma ação ou omissão que se proíbe e se procura evitar; ameaçando-a com pena, porque constitui ofensa (dano ou perigo) a um bem, ou valor da vida social."*

Diante do conceito matéria de crime que elege a afetação de um bem jurídico como base da ação típica, somente nos falta definir a conduta de quem acessa indevidamente um computador ofende ou não um bem juridicamente tutelado.

Luis Regis Prado[5] nos ensina que:

"(...) não há delito sem que haja lesão ou perigo de lesão (principio da lesividade ou ofensividade) a um bem jurídico determinado. Sob esta perspectiva, a tutela penal só é legitima quando socialmente necessária (principio da necessidade), imprescritível para assegurar as condições de vida, o desenvolvimento e a paz social, tendo em conta os ditames superiores da dignidade e da liberdade da pessoa humana."

---

3 - Fragoso, 1985, P. 147
5 – Luis Regis Prado, 2000, P. 82

A sociedade tem como valores a honra, a vida, o patrimônio, a liberdade, há de se eleger a privacidade como bem jurídico fundamental e assim foi feito na carta magna de 1988 ao assegurar em seu Art. 5°, X, que

"são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurando o direito a indenização pelo dano material ou moral decorrente de sua violação."

Sendo assim, a inviolabilidade das informações é decorrência natural do direito a privacidade, devendo por tanto, ser reconhecida como bem juridicamente protegido pela Constituição Federal de 1988, e ainda decorrente desse raciocínio, a inviolabilidade das informações automatizadas, ou seja, daquela armazenadas e ou processadas em sistemas de computadores, faz-se necessário então um novo bem jurídico a ser tutelado pelo direito penal a fim de garantir a privacidade e a integridade dos dados eletrônicos.

CAPÍTULO II – CRIMES PRÓPRIOS

Delitos informáticos próprios são aqueles em que o bem jurídico protegido pela norma penal é a inviolabilidade das informações automatizadas (dados). Além do delito de acesso não autorizado a sistemas computacionais, há ainda outras modalidades de crimes que tem como objeto a inviolabilidade dos dados informáticos e, por tanto, podem ser classificados como delitos informáticos próprios.

A interferência em dados informatizados é uma modalidade de crime informático próprio abrangido pelo acesso não autorizado a sistemas computacionais, porém mais específica do que ele. A hipótese procura prevenir a alteração e destruição de dados armazenados em sistemas computacionais e sua execução implicam necessariamente em um acesso não autorizado.

A lei nº 9.983/2000 acresceu dois tipos penais ao Código Penal Brasileiro prevendo a hipótese da interferência em dados informatizados unicamente quando praticada por funcionário público no exercício da função[6]. Em ambas as condutas prevista não se pune a

---

6 - Art 313-A. Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano: (Inclusão Lei nº 9.983/ 2000)

Pena - reclusão, de 2 (dois) a 12 (doze) anos, e multa. (Inclusão Lei nº 9.983/ 2000)

Modificação ou alteração não autorizada de sistema de informações (Inclusão Lei nº 9.983/ 2000)

Art 313-B. Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente: (Inclusão Lei nº 9.983/ 2000)

Pena - detenção, de 3 (três) meses a 2 (dois) anos, e multa. (Inclusão Lei nº 9.983/ 2000)

Parágrafo único. As penas são aumentadas de um terço até a metade se da modificação ou alteração resulta dano para a Administração Pública ou para o administrado.(Inclusão Lei nº 9.983 /2000)

7- O Draft Convention on Cyber – Crime em seu Art 3º prevê tal conduta

mera leitura dos dados, razão pela qual não se trata do acesso não autorizado a sistemas computacionais, mas crime especial em relação a este.

A interferência não está tipificada no ordenamento jurídico brasileiro.

A interceptação ilegal[7] é um crime informático próprio no qual os dados são capturados durante a transferência de um sistema para outro, sendo que o agente já violou o sistema anteriormente para poder monitorar as atividades do sistema para que possa interceptar a transmissão de dados.

A conduta está tipificada no ordenamento jurídico pátrio na lei 9.296 de 24 de julho de 1996, que em seu Art. 10° dispõe:

"(...)Art. 10. Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei.

Pena: reclusão, de dois a quatro anos, e multa."

Outro importante delito próprio é a falsificação informática, que consiste na adulteração de dados de computador (seja por introdução, supressão ou simples modificação), com fins fraudulentos.

Sendo um exemplo típico dessa adulteração, os softwares que são versões de testes (Trial ou shareware) onde são criados pequenos programas chamados de "cracks" que enganam o programa forjando um registro e possibilitando seu uso sem restrições como se fosse um registro autentico.

Há ainda os delitos informáticos próprios a criação ou divulgação de programas de computadores destrutivos que tem como seu representante mais vigoroso os vírus informáticos.

A palavra vírus deriva do latim e significa originalmente "veneno". O termo acabou sendo usado pelas Ciências Biológicas para definir diminutos agente infecciosos, visíveis apenas em

microscópios eletrônicos, que se caracterizam pela dependência do hospedeiro para sua sobrevivência e têm a capacidade de reprodução apenas no interior de células vivas.

O homem criou os vírus de computador à imagem e semelhança dos vírus biológicos, são pequenos programas, que infectam outros programas causando danos diversos ao sistema, se espalhando com estrema rapidez, em nanos segundos [8], são programa extremamente pequenos normalmente escritos em linguagem de programação tais como: assembly, pascal, Clipper, Delphi.capaz de se reproduzirem através de disquete, pen drives, cd, DVD ou e-mail ou mesmo links na internet.

Nesse caso temos o crime de dano (Art. 163 CP) que prevê:

*"(...)**Art. 163**. Destruir, inutilizar ou deteriorar coisa alheia:*

Pena - detenção, de um a seis meses, ou multa.

Dano qualificado

Parágrafo único. Se o crime é cometido:

I - com violência à pessoa ou grave ameaça;

II - com emprego de substância inflamável ou explosiva, se o fato não constitui crime mais grave;

III - contra o patrimônio da União, Estado, Município, empresa concessionária de serviços públicos ou sociedade de economia mista; (Alteração Lei nº 5.346/1967)

IV - por motivo egoístico ou com prejuízo considerável para a vítima:

Pena - detenção, de seis meses a três anos, e multa, além da pena correspondente à violência"

Entenda-se por coisa tudo aquilo que existe ou pode existir.

---

8 – nano segundo é uma media usada na informática é a milésima parte de um segundo

Apesar de ser perfeitamente aplicável a condenação por dano causado por vírus de computador, melhor seria se houvesse lei específica prevendo a criação e a divulgação de vírus de computador como crime de perigo concreto.

CAPITULO II – CRIMES IMPRÓPRIOS

Os delitos informáticos impróprios são aqueles em que o computador é utilizado como instrumentos para a execução de um crime, não existindo a ofensa ao bem jurídico inviolabilidade da informação automatizada.

Sua prática pode ser facilmente difundida, pois não exige conhecimentos técnicos para sua execução, são exemplos de crimes informáticos impróprios, crimes contra a honra, calúnia (Art. 138 do CP), difamação (Art. 139 do CP), injúria (Art. 140 do CP), que pode ser cometidos com um simples envio de e-mail, com uma comunidade no site de relacionamentos Orkut, o que é bem comum dado a facilidade para que simples usuários possam fazer disso uma prática constante e comum, há também outros crimes que podem ser cometidos através da utilização do computador tais como, induzimento, auxilio instigação ao suicídio (Art. 122 do CP), ameaça (Art. 147 CP), violação de segredo profissional (Art. 154 do CP), incitação ao crime (Art. 286 CP), apologia ao crime ou criminoso, bem como estelionato (Art. 171 CP) no caso dos "bankers" que são um tipo específico de hackers que geram uma boleta com o símbolo de alguma instituição de renome e inserem um código de barras que determina ao computador do caixa o depósito da quantia na boleta numa conta de uma particular e não da instituição utilizada na boleta, além da conduta estelionato, temos várias outras condutas que utilizam o computador como meio para seu cometimento.

Mas é importante lembrar que em nenhum dessas condutas há ofensa, ao bem jurídico inviolabilidade das informações automatizadas, razão pela qual são considerados delitos informáticos impróprios, esses mesmos crimes poderiam ser praticados através de um "chat" ou mesmo através de uma página Web. O que não exige conhecimentos específicos, além dos conhecimentos básicos como manipulação de textos e tabelas.

Essa facilidade aliada com a simplicidade do uso de softwares e da publicação anônima das páginas da Web em serviços gratuitos é responsável por uma expressiva quantidade de casos de publicação de fotos pornográficas de crianças na internet, o que em nossa legislação é crime de pedofilia, previsto no Art. 241 do Estatuto da Criança e do Adolescente (ECA – Lei 8.069 de 13 de julho de 1990).

Dentre os delitos informáticos, previstos na legislação penal extravagante, praticados por meio da internet, através de uma simples publicação em uma página temos concorrência desleal (art. 195 da lei nº 9.279 de 14 de maio de 1996), violação de direito autoral (Art. 12 da lei nº 9.609 de 19 de fevereiro de 1998) e mais uma gama de crimes eleitorais (Art. 337 da lei nº 4.737 de 15 de julho de 1965).

A prostituição é veementemente explorada através da internet onde páginas contêm anúncios de serviços profissionais de sexo, com a exposição de fotos das mulheres e os usuários podem contratar as mulheres "on line" o que, em tese pode caracterizar os delitos de favorecimento da prostituição (Art. 228 CP), já que as páginas facilitam o contato com os "clientes" ou rufianismo (Art. 230 CP), uma vez que o responsável pela página recebe comissão pelos contatos bem sucedidos.

O tráfico de drogas (Art. 12 da Lei 6.368/76) e o tráfico de armas (Art. 10 da lei 9.437/97) também pode facilmente pode ser realizado com a simples criação de uma página na internet.

Todos os casos vistos anteriormente são crimes informáticos impróprios, pois são cometidos com o auxilio de um computador, mas não violam os dados de nenhum sistema computacional.

CAPÍTULO II – CRIMES MISTOS

Delitos Informáticos mistos são crimes complexos em que além da proteção da inviolabilidade dos dados, a norma visa tutelar bem jurídico de natureza diversa.

Segundo Hungria:

"(...) Crimes simples e complexos: simples é o que se identifica com um só tipo legal; complexo, o que representa a fusão unitária de mais de um tipo (ex: roubo, estupro) [9] *"*

São delitos derivados do acesso não autorizado a sistemas computacionais que ganharam o status de delitos *sui generis* dada a importância do bem jurídico protegido diverso da inviolabilidade dos dados informáticos.

No ordenamento jurídico brasileiro paradoxalmente, um delito informático derivado do acesso não autorizado a sistemas computacionais já foi tipificado, enquanto que o delito fundamental ainda aguarda regulamentação.

Trata-se do acesso não autorizado a sistemas computacionais do sistema eleitoral que surgiu como tipo penal no ordenamento jurídico nacional com a lei nº 9.100/95 que em seu art. 67, VII assim o tipificou:

"(...) Obter ou tentar obter, indevidamente, acesso a sistema de tratamento automático de dados utilizado pelo serviço eleitoral, a fim de alterar a apuração ou contagem de votos.

Pena de 1(um) a 2 (dois) anos de reclusão e multa."

---

9 Hungria, Nelson – 1958 p. 53

Dois anos mais tarde veio a Lei nº 9.504/97, em seu Art. 72, I, assim dispôs sobre a matéria:

"(...) Obter ou tentar obter, indevidamente, acesso a sistema de tratamento automático de dados utilizado pelo serviço eleitoral, a fim de alterar a apuração ou contagem de votos.

Pena de 5(cinco) a 10 (dez) anos de reclusão."

Assim sendo, encontra-se parcialmente em vigor o art. 67, VII, da Lei nº 9.100/95, disciplinando exclusivamente os casos de tentativa, pois há a aplicação do Art. 14 do CP, por sua própria disposição é meramente subsidiária e este somente pode ser utilizado quando não há prévia regulamentação da matéria.

Destaque-se ainda que no Art. 107 da Lei 9.504/97 enumera taxativamente os dispositivos por esta revogados e em seu rol não há qualquer menção ao art. 67, VII, da Lei 9.100/95.

Podemos notar uma demasiada ânsia em punir as tentativas e as consumações de crimes contra o sistema informático eleitoral pelo fato da política de segurança do TST (Tribunal Superior Eleitoral)

Segundo Túlio Vianna:

"(...) A política de segurança do TST parece se basear somente no sigilo da fonte. Tal opção é profundamente temerosa, pois um único dos programadores que se corrompesse poderia colocar em risco a legitimidade de uma eleição inteira. Não sendo os códigos públicos, os partidos não tem como saberem se o programa que está sendo usado no dia das

eleições está mesmo cumprindo sua função de coletar e totalizar os votos sem alterações, pois poderiam facilmente ser alterados para garantir a vitória de um determinado candidato.[10]"

10- LIMA VIANNA, Túlio. Fundamentos de Direito Penal Informático – Ed. Forense - 2003

CAPÍTULO II – CRIMES FORMAIS, MATERIAIS E DE MERA CONDUTA

Vistos os tipos de crimes, procuraremos agora determinar o tempo e o local do crime, baseando-nos no direito Penal e no Direito Processual Penal.

Para tanto buscaremos definir, *ab initio,* qual o resultado no meio, produzido por um acesso não autorizado a sistemas computacionais.

Crimes materiais, formais e de mera conduta

Todo crime, por sua própria definição, te como resultado jurídico a ofensa a algum bem penalmente tutelado, no acesso não autorizado a sistemas computacionais, é a inviolabilidade dos dados.

Além do resultado jurídico, temos também os resultados no mundo fenomênico, no caso de uma calúnia, injúria, difamação e diversos outros delitos que podem ter o computador como meio de execução e também podemos ter um crime eleitoral bem como uma apropriação indébita no caso do desvio de dinheiro de instituições bancárias.

Muitos doutrinadores classificam os crimes quanto ao resultado matéria que produzem em delitos materiais, formais e de mera conduta.

Segundo tais autores, delitos materiais são aqueles em que ocorrem resultado no mundo fenomênico penalmente relevante, delitos formais são aquele em que ocorrem resultados no mundo fenomênico penalmente irrelevantes e delitos de mera conduta são aqueles em que não ocorre resultado no mundo fenomênico.

Segundo Zaffaroni e Pierangeli [11] :

---

11 ZAFFARONI, Eugenio Raúl e PIERANGELI, José Henrique. *Manual de Direito Penal Brasileiro Parte – Geral.* 2ª.ed., São Paulo: Revista dos Tribunais, 1999.

"(...) O que ocorre é que todos os tipos requerem um resultado, só que os individualizaram de maneiras distintas: alguns os mencionam expressamente, outros vinculam-nos inseparavelmente à conduta, outros preferem limitar-se ao puro resultado da conduta desinteressando de qualquer outro que possa causar."

Todo crime há um resultado fático, buscaremos agora o resultado material produzido pelo acesso não autorizado a sistemas computacionais e se ele é relevante ou não para a caracterização da tipicidade da conduta.

Vimos que o acesso é a conduta de ler, escrever ou processar dados em sistemas computacionais. Há três modalidades distintas do delito de acesso não autorizado a sistemas computacionais sendo que em cada uma delas encontraremos uma relação ordenada de ação e resultado.

Nas três modalidades a ação será sempre um comando emitido pelo agente, geralmente digitado em um teclado, podendo ser emitido também através do mouse, um microfone ou qualquer dispositivo de entrada de dados. Este comando processará uma série de instruções que cominará em um dos três resultados que caracterizam a modalidade do acesso.

Quando alguém emite um comando para que um editor de textos ou outro programa de edição abra um arquivo, e esse comando culminará na abertura de um arquivo na tela do computador, da mesma forma a exibição de uma foto ou a execução de um arquivo de som, esta é a modalidade de leitura de dados.

Quando alguém emite um comando para que um editor de textos abra um arquivo ou salve as alterações nele efetuadas também ocorrerá uma seqüência ordenada de instruções que gerarão uma modificação nos dados originalmente armazenados no sistema. Esta é a modalidade de escrita de dados

Quando alguém emite um comando para que o computador feche o editor de textos e abra outro programa qualquer, o que culminará na execução de outro programa, esta é a modalidade de processamento de dados.

Constata-se claramente que a proteção penal incidira sobre a leitura, escrita e processamento de dados e não sobre a emissão de comando sem a ocorrência de resultado.

Em uma analogia com o crime de homicídio, poderíamos afirmar que digitar o comando ou clicar do mouse seria o disparo de uma arma e a leitura, escrita ou processamento de dados seriam a morte da vítima.

Assim como matar equivale semanticamente a produzir lesões corporais em outrem, causando-lhe o resultado morte, acessar significa emitir comandos a um sistema computacional, causando-lhe leitura, escrita ou processamento de dados.

O delito do acesso não autorizado a sistemas computacionais é crime material, já que o resultado fático da conduta é penalmente relevante, está conclusão e fundamental para que possamos delinear a tentativa, bem como o tempo e o local do delito e identificar a co-autoria e a participação.

CAPÍTULO II – DO TEMPO E DO LOCAL DOS CRIMES

A determinação do exato momento da ocorrência do crime é importante na aplicação da norma para a solução de conflito temporal de normas, aferição da imputabilidade do agente, aplicação da anistia e da prescrição e análise das circunstâncias do crime.

Temos três teorias doutrinárias a este respeito, a teoria da atividade ou ação, segundo a qual o crime é praticado no momento da execução da conduta; a teoria do resultado pela qual o crime considera-se realizado no momento de seu resultado; a teoria mista ou da ubiqüidade em que o crime é considerado cometido tanto no momento da conduta como no momento do resultado.

O Art. 4° do CP adotou a teoria da ação ou da atividade e estabeleceu que:

"considera-se praticado o crime no momento da ação ou omissão, ainda que outro seja o momento do resultado"

Antônio José Fabrício Leiria diz que[12]:

"É exatamente no instante da ação que a inteligência que pensa e a vontade que quer se manifestam no mundo exterior: tornando-se relevantes ao direito. É este o momento da ação ou omissão que se objetiva o querer do agente, portanto, revela-se a sua rebeldia ao comando da lei. Logo, aqui é que se deve situar o tempos delict"

Observemos que o lapso temporal entre a ação e o resultado nos crimes informáticos pode ser muito grande, pois ao digitarmos um comando ou clicarmos para que o computador faça esse comando, se o computador do agente estiver em rede poderão passar-se alguns minutos para que o comando seja executado em sua totalidade, mas no caso da transferência de arquivos de uma rede remota para uma rede local (*download)* esse lapso temporal entre a

---

12 LEIRIA, Antônio José Fabrício. Teoria e prática da lei penal. 1981. PP. 93-94 apud FRANCO ET AL., 1987. p.13

ação e o resultado pode ser maior ainda, poderá ser de horas, talvez dias dependendo de uma séries de fatores externos.

È perfeitamente possível ainda que o acesso não autorizado a sistemas computacionais seja praticado como delito permanente. Basta que o agente, ao obter o acesso, troque a senha do sistema, impedindo o acesso dos usuários autorizados e garantindo assim seus acessos futuros até que uma providência seja tomando. Neste caso a ação e o resultado vão se postergar no tempo até que o usuário autorizado consiga reaver o controle do sistema.

CAPÍTULO II – DO LOCAL DO CRIME

Os posicionamentos doutrinários a cerca do *locus commissi delicti* são vários. Luis Regis Prado13 diz:

"a) teoria da ação ou da atividade: local do delito é onde se realizou a ação ou omissão típica; b) teoria do resultado ou do efeito: local do delito é aquele em que ocorreu o evento ou resultado; c) teoria da intenção: lugar onde deveria ocorrer o resultado, segundo intenção do autor; d) teoria do efeito intermédio ou do efeito mais próximo: local do delito é aquele em que a energia movimentada pela atuação do agente alcança a vítima ou o bem jurídico; e) teoria da ação a longa distância ou da longa mão: lugar do delito é aquele em que se verificou o ato executivo; f) teoria limitada da ubiqüidade: lugar do delito tanto pode ser da ação como pode ser do resultado; e g) teoria pura da ubiqüidade, mista ou unitária: lugar do delito pode ser o da conduta como o do resultado ou o lugar do bem jurídico atingido"

O código Penal Brasileiro consagrou a teoria pura da ubiqüidade ao dispor em seu Art. 6º que:

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

A aplicação desta norma aos casos de acesso não autorizado a computadores cometidos através da internet em que o computador do agente encontra-se em um pais diferente é bem simples quando em ambos os países a conduta do acesso não autorizado a sistemas computacionais é fato típico.

Nestes casos, supondo que na nossa legislação atual já houvesse a figura do acesso não autorizado a sistemas computacionais, tanto o acesso de um computador do Brasil a um sistema computacional estrangeiro, seria punido aqui no Brasil, quando o acesso de um computador localizado no estrangeiro a um sistema computacional aqui no Brasil seria punido

13 PRADO, Luis Regis. Curso de Direto Penal volume I. São Paulo. Editora Revista dos Tribunais

no estrangeiro se lá houvesse a figura do acesso não autorizado a sistemas computacionais como fato típico.

O verdadeiro problema ocorre quando apenas um dos países tem em sua legislação a figura do acesso não autorizado a sistemas computacionais com fato típico.

Pode ocorrer que a conduta seja típica no local onde foi dado o comando, mas atípica no local onde se dá o resultado fático. Ou ao contrário ser atípica onde o comando foi dado e típica onde ocorre o resultado fático.

Para tentarmos encontrar uma solução para isso devemos parti do pressuposto que a interpretação da lei penal deve ser restritiva, aplicando-se também no caso de duas interpretações a menos danosa a liberdade do cidadão.

Em seu art. 6º nosso Código penal traz em sua redação a palavra "crime" e não "ação" ou "conduta". Se o crime será considera praticado tanto no lugar da conduta quanto no lugar do resultado, é necessário que o fato seja considerado crime nos dois locais, tanto o local da conduta quando no local do resultado.

É de extrema importância a tipificação da conduta acesso não autorizado a sistemas computacionais nas duas legislações para, que não ocorra a ofensa do principio constitucional do nullum crimen sine lege.

CAPITULO II – JURISDIÇÃO E COMPETÊNCIA

A jurisdição é o poder de legislar e governar, a expressão da soberania de um estado. Este poder é uno, mas é dividido em vários órgãos do corpo estatal.

Ensina Mirabete[13] que:

"Como poder soberano do Estado, a jurisdição é uma e, investido do poder de julgar; o juiz exerce a atividade jurisdicional. Sendo evidente, porém que um juiz não pode julgar todas as causas e que a jurisdição não pode ser exercida ilimitadamente por qualquer juiz, o poder de julgar é distribuído por lei entre os vários órgãos do poder judiciário, através da competência. A competência é assim, a medida e o limite da jurisdição"

A competência é o limite do poder de cada órgão jurisdicional. A distribuição dos poderes jurisdicionais se dá de acordo com a natureza do crime praticado (*ratione materiae*), com a qualidade das pessoas incriminadas (*rationae personae*) e com o local onde o crime foi praticado ou consumou-se ou ainda com o local da residência do autor (*ratione loci*).

Aqui iremos nos basear na razão do local e em razão da matéria do delito.

Com base na carta magna de 1988 em seu art 109, IV:

"crimes políticos e as infrações penais praticadas em detrimento de bens, serviços ou interesse da União ou de suas entidades autárquicas ou empresas públicas, excluídas as contravenções e ressalvada a competência da Justiça Militar e da Justiça Eleitoral."

Baseando-se que a internet é um serviço público de telecomunicação e como tal sujeita-se as normas da ANATEL (agência Nacional de Telecomunicações), sendo interesse da união em sua proteção jurídica incontestável. A Constituição Federal de 1988 em seu art. 21, XI determina que:

---

13 MIRABETE, Julio Fabbrini. Código penal interpretado. São Paulo: atlas 1999

"compete à união explorar, diretamente ou mediante autorização, concessão ou permissão, os serviços de telecomunicações, nos termos da lei, que disporá sobre a organização dos serviços, a criação de um órgão regulador e outros aspectos institucionais."

Então quando do acesso não autorizado a sistemas computacionais, quando o agente praticar por meio da internet será de competência federal, devendo ser conhecidos e julgados pela justiça federal, devido à internet ser uma serviço da união.

Mas se o agente não utilizar-se da internet para o cometimento do crime, será conhecido e julgado este pela justiça comum.

Observando o Art. 70 do Código de Processo Penal adotou a teoria do resultado, assim sendo a competência *ratione loci* para se julgar o delito de acesso não autorizado a computadores será fixada pelo local onde se encontra o sistema acessado indevidamente.

Nos casos em que o sistema computacional invadido se encontrar no Brasil a competência será no local onde o sistema acessado indevidamente se encontra, aplicando-se oi que se encontra disposto no Art. 70, §1°, do Código de Processo Penal que dispõe:

"A competência será, de regra, determinada pelo lugar em que se consumar a infração, ou, no caso de tentativa, pelo lugar em que for praticado o último ato de execução."

A tentativa vai ser tratada da mesma forma como previsto no At. 70, §1° do Código de Processo Penal, se consumará a tentativa no caso do comando ser dado no Brasil, não tendo se consumado por fatos alheios a vontade do agente no caso do comando ser dado no Brasil e não ter sido consumado no estrangeiro:

Como disposto no Código de Processo Penal:

"Se, iniciada a execução no território nacional, a infração se consumar fora dele, a competência será determinada pelo lugar em que tiver sido praticado, no Brasil, o último ato de execução."

Para o caso de o comando ser dado no estrangeiro e o resultado ocorrer no Brasil aplicar-se-á o disposto no Art. 70;§2° do Código de Processo Penal que dispões em sua redação:

"Quando o último ato de execução for praticado fora do território nacional, será competente o juiz do lugar em que o crime, embora parcialmente, tenha produzido ou devia produzir seu resultado."

Nesses casos a competência será do juizo onde estiver localizado o sistema computacional que foi ameaçado pela tentativa proveniente do estrangeiro.

CAPÍTULO II – DO *ITER CRIMINIS*

Os doutrinadores conceberam que a conduta criminosa é um caminho percorrido pelo agente (*iter criminis*). Assim em toda conduta criminosa é possível vislumbrar as seguintes fases; cogitação (*cogitatio*), preparação (*conatus remotus*), execução (*conatus proximus*) e consumação (*meta optata*).

Cogitação

Evidente mente a fase da cogitação é uma fase subjetiva, desta forma não podendo ser punida, pois dessa forma estaríamos admitindo a punição pelos pensamentos do agente, desta forma o delito do acesso não autorizado a sistemas computacionais, não poderia ser punido tão somente pela manifestação da vontade de invadir um determinado sistema, ainda que o agente forneça detalhes de sua intenção de lograr êxito com sua ação.

Preparação

É nessa fase que o agente colherá informações sobre o sistema a ser invadido que é chamada de *footprint*, o que lhe possibilitará uma mais chance de lograr êxito em sua tentativa de acesso não autorizado a sistemas computacionais, podendo direcionar um ataque no local onde o sistema computacional for mais frágil em termos de segurança.

Diz Mcclure[13]:

"O footprint de uma organização permite que invasores criem um perfil completo da postura de segurança dessa organização. Usando uma combinação de ferramentas e técnicas, atacantes podem empregar um fator desconhecido (a conexão a internet da empresa X) e convertê-lo em um conjunto específico de nomes de domínio, blocos de rede e endereços IP individuais de sistemas conectados diretamente a internet."

Essa seria a fase de seleção do sistema computacional a ser invadido, pode-se assemelhar com a conduta de um agente andando pela rua procurando uma bolsa para

13 MCCLAURE, Stuart, SCAMBRAY, Joel, KURTZ, George. Hackers expostos: segredos e soluções para a segurança de redes. São Paulo: Makron Books, 2000.

facilmente poder subtraí-la de seu dono. Nota-se que ainda não há uma ameaça concreta ao bem jurídico, dessa forma o footprint não pode ser punido.

Posteriormente ao footprint temo a fase de varredura do sistema, onde o agente vai procurar os sistemas alcançáveis a partir da internet e ativos, procurando encontrar portas abertas (brechas na programação do sistema computacionais ou mesmo falhas na segurança do sistema)

Mcclure afirma que[14]:

"a varredura de portas (port scanning) é o processo de se conectar a portas TCP e UDP do sistema alvo, para determinar quais serviços estão em execução ou em estado de escuta. Identificar portas escutando é crucial para determinar o tipo de sistema operacional e aplicativos em uso. Serviços ativos ouvindo podem permitir a um usuário não autorizado ter acesso a sistemas mal configurados ou que estejam executando determinado software com falhas de segurança conhecidas"

Essa é a fase de avaliação da vítima. Após ter selecionado a vítima através do footprint, o agente procurará avaliar agora a probabilidade de êxito no seu ataque. Seria o caso de após selecionar a casa a ser roubada o agente tocar a campainha para ver se há alguém no interior da casa.

Não poderá ser punida a varredura já que o bem juridicamente protegido a inviolabilidade de dados ainda não teve ofensa concreta.

Inicia-se agora a etapa onde prepara-se a invasão, verifica-se quais são os usuários cadastrados no sistema e quais são seus privilégios junto a este, como um usuário de leitura, um usuário de processamento, um usuário de escrita ou um administrador do sistema no qual é o mais visado neste tipo de delito.

Segundo Mcclure[15]:

---

14 MCCLAURE, Stuart, SCAMBRAY, Joel, KURTZ, George. Hackers expostos: segredos e soluções para a segurança de redes. São Paulo: Makron Books, 2000.

"em geral, uma vez que um nome de usuário ou de compartilhamento válido seja enumerado, normalmente é só uma questão de tempo antes do invasor adivinhe a senha correspondente ou identifique algum ponto fraco associado ao protocolo de compartilhamento do recurso."

Essa fase serve para determinar os pontos mais frágeis do sistema a ser invadido, assemelha-se a um agente pretendendo seqüestrar uma pessoa traçar todos os horários e locais onde a vítima freqüenta e quis os horário em que ela está sozinha passando por lugares pouco movimentados facilitando a conduta do agente.

O próximo passo do agente é o acesso não autorizado ao sistema computacional previamente avaliado, mas ainda não temos a lesão ao bem jurídico, se o agente desistir da sua conduta, a mesma só terá existido subjetivamente, sem causar nenhuma alteração no mundo fenomênico.

Da execução e da consumação

Vimos que o delito do acesso não autorizado a sistemas computacionais é um crime material, somente se consumando se ocorrer um resultado no mundo fenomênico. Iremos agora determinar quando se inicia a conduta do agente que terminará com este resultado no mundo fenomênico:

Segundo Fragosso[16]:

"tendo em vista o sistema da nossa lei, prevalece na doutrina um critério objetivo de distinção, sendo irrelevante, em princípio, o plano delituoso do agente. Materialmente constitui ato de execução aquele que inicia o ataque ao bem juridicamente tutelado; formalmente, tal ato distingue-se pelo início de realização da ação típica prevista pela lei"

A ação de acessar dados implica em um comando ou uma série de comandos dados e a sua consumação dá-se quando no momento da leitura, escrita ou execução de dados.

---

15 MCCLAURE, Stuart, SCAMBRAY, Joel, KURTZ, George. Hackers expostos: segredos e soluções para a segurança de redes. São Paulo: Makron Books, 2000.
16 FRAGOSO, Heleno Cláudio. Lições de Direito Penal: a nova parte Geral. 8ª Ed. Rio de Janeiro: Forense.

A forma que este comando é dado pode variar pode ser *online* e *offline*, e também pode ser dado como uma única instrução ou como várias instruções seqüenciais que geram o resultado pretendido pelo agente, isto é o acesso ao sistema computacional.

O momento do inicio da execução de um acesso não autorizado dar-se-á no momento em que é emitido pelo agente o primeiro comando de uma série de comandos que irão cominar na obtenção do acesso ou da informação contida no sistema computacional.

No caso em grande parte dos sistemas o acesso é protegido por senha, sendo neste caso então o primeiro comando uma autenticação indevida.

O acesso a qualquer sistema dá-se por meio de um banco de dados onde são gravados os nomes de usuários e senha destes, o agente simplesmente vai até este banco de dados e insere um usuário e uma senha para que tenha o acesso ao sistema.

Tentativa

Essa ocorrerá toda vez que um comando for dado com a intenção de obter o acesso não autorizado a sistemas computacionais, for emitido pelo agente e este não ocorrer por fatos alheios a vontade do agente.

Mesmo obtendo o acesso, mas o agente não conseguir ler, modificar, executar, apagar, copiar os dados por fatores alheios a sua vontade, teremos a figura da tentativa.

Se os dados estiverem em um idioma ou código em eu o agente não consegue fazer a leitura dos dados ou se os dados estiverem criptografados e o agente não conseguir "quebrar" a criptografia isso configurará crime impossível.

A escrita de dados tem por seu objetivo a alteração de informações dentro do sistema, sendo assim poderá o agente se arrepender e restaurar os *status quo ante*, figurando assim o arrependimento eficaz previsto no Art. 15 do Código Penal Brasileiro.

A modalidade de processamento de dados de como objetivo a execução da ordem dada, mas se por algum motivo interno no sistema computacional, há o retorno de uma

mensagem de erro, isso configurará crime impossível pela absoluta impropriedade do objeto e o agente não será punido conforme consta no Art. 17 do Código Penal Brasileiro.

CAPÍTULO II – SUJEITOS DO DELITO

Sujeitos ativos e passivos

Sujeito Passivo no delito do acesso não autorizado a sistemas computacionais será qualquer pessoa física ou jurídica proprietária dos dados armazenados no sistema.

Sujeito ativo será a pessoa humana responsável pela emissão do comando causador da leitura, escrita ou processamento de dados para os quais não possuía privilégios junto ao sistema computacional.

Nada impede o empregador de ser sujeito ativo quando acessar o e-mail pessoal de seus funcionários ou seus arquivos pessoais armazenados no sistema computacional. O fato de o empregador ser o proprietário do sistema não o exime da infração uma vez que se protege juridicamente a inviolabilidade dos dados informáticos e estes sendo de cunho pessoal são propriedades do empregado, mas há uma ressalva neste caso, se o empregador designar um e-mail e um local onde o empregador deverá acessar e salvar suas informações tão somente profissionais e pactuar em contrato que esse e-mail e este espaço são para uso profissional e que a empresa tem total e livre acesso as informações ali contidas devido ao seu cunho profissional, o empregador não ocorrerá em crime algum, pois ele é o proprietário das informações ali contidas.

O cônjuge também pode figurar como sujeito ativo do delito do acesso não autorizado a sistemas computacionais uma vez que o Art. 5º; X da Constituição federal de 1988 garante a intimidade e a vida privada, direitos individuais do cidadão que são essência da tutela penal à inviolabilidade dos dados informáticos.

O casamento não elimina dos cônjuges o

Direito individual a privacidade, pois há em cada individuo uma necessidade natural de manter determinados segredos só para si, um cônjuge que acessa sem autorização os dados

informáticos do outro, estará cometendo acesso não autorizado a sistemas computacionais, pois a lesão ao bem jurídico privacidade individual é evidente.

A união, Estados, Distrito Federal e Municípios, quando sujeitos passivos do acesso não autorizados a sistemas computacionais, deverão ter uma proteção maior dado à extensão da lesividade de um acesso não autorizado, pois não será apenas um individuo lesado, mas sim uma coletividade, razão pela qual o crime deverá ser qualificado.

Ainda sim temos a figura de sujeitos ativos aos quais são imputadas facilidades para o cometimento do delito acesso não autorizado a sistemas computacionais, como funcionários que tem conhecimento do funcionamento técnico do sistema, funcionários públicos responsáveis pelo processamento de dados sigilosos. A estes certamente deverá ser imputada uma pena mais severa quando em razão dos seus cargos, obtiverem acesso não autorizado

CAPÍTULO III – CRIMES CONTRA A HONRA

Neste ponto veremos a adequação dos crimes contra a honra cometidos utilizando um computador como meio, primeira mente deveremos avaliar os tipos de crimes contra a honra, temos, calúnia (Art. 138 do CP), difamação (139 do CP), injúria (Art. 140 do CP), no caso dos três tipos, se forem praticados por meio da internet, será aplicada o disposto no art. 141, III do CP.

Que nos diz:

"Art. 141 - As penas cominadas neste Capítulo aumentam-se de um terço, se qualquer dos crimes é cometido:

III - na presença de várias pessoas, ou por meio que facilite a divulgação da calúnia, da difamação ou da injúria."

Neste caso teremos a forma qualificada dos crimes contra a honra, pois facilita a divulgação da calúnia, injúria ou difamação, tendo em vista que a internet é mundial e é considerado um meio de ampla divulgação.

Já temos casos de crimes contra a honra utilizando o site de relacionamentos Orkut para sua divulgação.

Reportagem da Folha Online[17] diz:

"pós a "Orkut mania", o serviço ultrapassou a fase de boom no Brasil, viveu a temporada de "orkuticídios" e agora, cada vez mais, enfrenta a ira daqueles que tiveram perfis falsos em seus nomes no serviço e comunidades potencialmente ofensivas.

---

17 Disponível em http://www.denunciar.org.br/twiki/bin/view/SaferNet/Noticia20070713005321 às 10:00 de 23/07/2008.

A socialite Yara Baumgart e o bispo Edir Macedo são alguns dos conhecidos que chegaram a processar a companhia por crimes contra a honra.

A temporada de reclamações de crimes contra a honra no Orkut começou com a invasão brasileira no site, que ocorreu maciçamente em 2005. Diversos tribunais brasileiros emitiram decisões responsabilizando a Google do Brasil nestes casos, mas a empresa alega que quem responde pelo Orkut é a matriz da companhia.

Procura

Tiago Bortoletto Vaz, da ONG Safernet, que reúne denúncias de crimes virtuais, disse que a organização não se encarrega de pedidos de crimes contra a honra, mas que fornece orientação em seu site para pessoas que se sintam prejudicadas por perfis ou comunidades.

Vaz afirma que há cerca de 500 processos dessa natureza envolvendo a Google, detentora do Orkut, no país. Ele afirma que a sessão do site com as orientações recebe cerca de 2.000 acessos por dia e que 50 e-mails com dúvidas sobre tais questões são enviadas diariamente sobre como proceder.

Em apenas uma vara cível de São Paulo, a reportagem da Folha Online encontrou mais de 30 procedimentos contra a Google. A maioria referente a Orkut. "Nos tribunais do Rio Grande do Sul e Minas Gerais, por pesquisa eletrônica, é possível ver que a grande maioria das ações ocorre a partir do final de 2005, com um aumento em 2006."

Como dito anteriormente, os crimes contra a honra cometidos por meio da internet terão suas penas aumentadas em 1/3 pelo meio empregado para sua divulgação.

CAPÍTULO III – VIOLAÇÃO DE CORRESPODÊNCIA ELETRÔNICA

Veremos a seguir se a violação de correspondência eletrônica é fato típico ou não, primeira mente analisemos a palavra *e-mail* do inglês *eletronic mail*, segundo o dicionário Micaélis *mail* (1 – correspondência, 2 – correio) temos então correspondência eletrônica, que é protegida por alguns recursos eletrônicos tais como a encriptação de dados do *e-mail*, bem como pode ser protegido por senha ou idiomas cifrados etc.

Vejamos agora o que diz a Constituição Federal de 1988 sobre a correspondência eletrônica:

"Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:

.....

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

Nota-se que a inviolabilidade da correspondência eletrônica é um direito constitucional e ainda uma violação a propriedade da correspondência, dado o exposto a violação de correspondência eletrônica é fato típico previsto pela Constituição Federal devendo ser punido.

Segundo Celso Ribeiro Bastos[18], ao comentar o inciso XII, afirma:

"Dizer que a correspondência assim como as comunicações telegráficas, de dados e telefônicas são invioláveis significa que a ninguém é licito romper o seu sigilo, isto é: penetrar-lhe o conteúdo. Significa ainda mais: implica, por parte daqueles que em função do seu trabalho tenham de travar contato com o conteúdo da mensagem, um dever de sigilo profissional."

Com base no meu conhecimento técnico sobre correspondências eletrônicas pode se interpretar o que consta no Art. 151 do CP, de forma técnica a correspondência eletrônica é fechada com a utilização de *softwares* específicos que cifram a linguagem, encriptam os dados na mensagem contidos ou mesmo bloqueiam com uma senha o acesso a esta mensagem, sendo assim podemos entender que a mensagem eletrônica é uma correspondência fechado o que nos permitirá a aplicação do exposto no art. 151 do CP que diz:

"Violação de correspondência

Art. 151 - Devassar indevidamente o conteúdo de correspondência fechada, dirigida a outrem:

Pena - detenção, de 1 (um) a 6 (seis) meses, ou multa.

Sonegação ou destruição de correspondência

§ 1º - Na mesma pena incorre:

---

18 BASTOS. Celso Ribeiro. Curso de direito constitucional. 19ª Edição. Editora Saraiva: São Paulo. 1998

I - quem se apossa indevidamente de correspondência alheia, embora não fechada e, no todo ou em parte, a sonega ou destrói;

A sonegação ou a destruição de correspondência eletrônica vai constituir em concurso formal, pois haverá uma conduta mais terão sido praticados dois crimes, primeiramente o acesso não autorizado a sistemas computacionais e o segundo a violação de correspondência eletrônica, já que para violar a correspondência eletrônica o agente devera acessar o sistema computacional onde se encontra a correspondência.

CAPÍTULO IV – POVEDORES DE ACESSO

Depois de fazer muito barulho em novembro de 2006 com a idéia de exigir que os internautas tivessem que ter um cadastro completo para acessar a rede, o projeto de lei de crimes digitais volta a provocar polêmica às vésperas de sua votação na CCJ (Comissão de Constituição e Justiça) do Senado.

A nova proposta derrubou a exigência do cadastro, mas agora obriga provedores de Internet a encaminhar denúncias às autoridades sobre possíveis condutas ilegais de seus usuários, considerando mais de 600 tipos de crimes definidos pela legislação brasileira. Além disso, o texto dá amparo legal para que "profissionais habilitados" ou empresas privadas de segurança da informação interceptem dados ou invadam redes em legítima defesa.

O centro da polêmica é uma revisão —chamada de Substitutivo— do senador Eduardo Azeredo (PSDB-MG) ao Projeto de Lei da Câmara nº 89, de 2003, e dos Projetos de Lei do Senado nº 137 e nº 76, ambos de 2000. Segundo a assessoria da CCJ, o projeto pode entrar na pauta de votação a qualquer momento.

Segundo resenha do Substitutivo a que o UOL Tecnologia teve acesso, o projeto prevê que o provedor de Internet tenha de "informar, de maneira sigilosa, à autoridade policial competente, denúncia da qual tenha tomado conhecimento e que contenha indícios de conduta delituosa na rede de computadores sob sua responsabilidade".

Antônio Tavares, representante dos provedores de acesso à Web no Comitê Gestor da Internet —entidade que para coordena e integra todas as iniciativas de serviços Internet no país— questiona este ponto do projeto. "É como a sua namorada resolvesse processar a Telefônica ou uma operadora qualquer porque você usou o telefone para xingá-la ou maldizê-la. Ninguém faz isso, não tem lógica."

José Henrique Portugal, assessor técnico de Azeredo e responsável pela redação do projeto, defende o texto: "Trata-se de tornar oficiais práticas que já são adotadas pelos bons provedores", diz.

Mas nesse caso poderemos ter um entrave para que essa prática dos provedores seja válida, temo hoje no nosso código penal cerca de 600 previsões de fatos típicos de condutas ilícitas, isso dificulta o trabalho por parte dos provedores, pois os mesmo não dispõem de conhecimento técnico para avaliar as condutas dos internautas. Pois o provedor de acesso não são policiais disse Eduardo Parajo [19]:

"A adoção de um código de ética e de auto-regulamentação seria a melhor saída para que a Internet brasileira fosse mais segura. Esta pelo menos é a idéia da Abranet (Associação Brasileira dos Provedores de Acesso, Serviços e Informações da Rede Internet).

"Nós não somos polícia e não podemos assumir responsabilidades que não são nossas", diz Eduardo Parajo, presidente da entidade. Segundo ele, o código de ética é uma preocupação de todos os associados.

"Temos interesse em colaborar para a segurança da rede, que é importantíssima, e estamos buscando esse tipo de investimento, como o combate à pedofilia, ao racismo, ao neonazismo. Também cumprimos todas as solicitações do Ministério Público", afirma.

Para Thiago Tavares, presidente da SaferNet Brasil, organização não-governamental responsável pela central nacional de denúncias de crimes cibernéticos, a medida põe um poder indesejado na mão dos provedores.

---

19 – Eduardo Parajo – Presidente da ABRANET - http://safernet.org.br/twiki/bin/view/SaferNet/Noticia20070521123629?sortcol=0;table=2;up=0 em 23/07/2008 as 13h18min

"Uma coisa é um crime na sociedade, um cidadão tomar conhecimento de um crime e levar ao conhecimento da Justiça que aquele crime está sendo praticado, principalmente em se tratando de crimes contra a vida, como pornografia infantil ou racismo, cuja ação é pública e incondicionada a representação", diz.

Ele não concorda com a ação dos provedores como intermediários de uma denúncia. "Agora, crimes patrimoniais são classificados como crimes de ação penal privada, em que somente o ofendido pode provocar o Estado. E cabe ao Estado o direito exclusivo de investigar e punir.

A partir deste ponto vemos que a lei existe, mas não há como cumpri-la, devido ao aumento do escopo de abrangência das denuncias dos provedores sobre os internautas que estiverem incorrendo em alguma conduta delituosa, por falta de conhecimento técnico por parte dos provedores de acesso, mas essa prática da denuncia dos usuários que de certa forma cometer algum delito já é feita por força de um acordo feito entre o ministério público de São Paulo e os principais provedores brasileiros.

CAPÍTULO IV – E-MAILS SUA ADIMISSIBILIDADE COMO PROVA DOCUMENTAL

O Projeto de Lei 6693/06 estabelece que o e-mail (mensagem de correio eletrônico) apresentado em juízo é, presumidamente, autêntico, servindo como prova da data de seu envio e do recebimento pelo destinatário. A proposta, da deputada Sandra Rosado (PSB-RN), iguala o e-mail ao telegrama e ao radiograma, considerados prova documental pelo Código de Processo Civil. A autora destaca que as novas relações sociais decorrentes da utilização da internet exigem a adaptação do ordenamento jurídico. De acordo com a parlamentar, se a legislação estabelece a presunção de autenticidade de telegramas, deveria prever a mesma prerrogativa para o e-mail. Ela lembra que essa presunção é relativa e admite prova em contrário. A deputada informou que a proposta foi sugestão do advogado e professor Leandro Vieira, de Blumenau (SC). O projeto será analisado em caráter conclusivo pela Comissão de Constituição e Justiça e de Cidadania.

Como visto há um projeto de lei que irá igualar o *e-mail* a uma carta ou telegrama, o tornando assim uma prova documental, mas com a atual legislação fazendo-se uma interpretação literal do texto disposto no art. 197, poderemos vislumbrar a possibilidade de aceitação do *e-mail* como prova se seu conteúdo corroborar com outras provas já constadas nos autos.

Rege o Código de Processo Penal:

"Art. 197. O valor da confissão se aferirá pelos critérios adotados para os outros elementos de prova, e para a sua apreciação o juiz deverá confrontá-la com as demais provas do processo, verificando se entre ela e estas existe compatibilidade ou concordância"

No *e-mail*, não há assinaturas reais dos seus remetentes, mas há uma assinatura digital que é única, assim como nossas impressões digitais, há também um endereço eletrônico que é composto por uma série de números que recebe o nome de *internet protocol* comumente conhecido como IP, esse número também é único na internet seria equivalente ao nosso RG, com esse conhecimento, é totalmente possível rastrear um e-mail até seu remetente, tornando assim possível sua punição e seguindo o exposto no Art. 197 do CPP a possibilidade de admissão do *e-mail* como prova.

CAPÍTULO IV – POSSIBILIDADE DA RESTRIÇÃO DE DIREITOS

A restrição de um direito, que é assegurado na Carta Magna de 1988, pode ser restringido quando o agente que comete um delito eletrônico é obrigado por sentença a não se aproximar de sistemas computacionais, seja esse sistema um computador (*notebook*, computadores comuns, *palm tops*, celulares ou outros tipos de sistemas computacionais, isso é possível quando o agente afeta a intimidade, a vida privada, a honra ou a imagem das pessoas.

No entanto a restrição desse direito gera uma grande discussão no que tange a dignidade da pessoa humana, mas visto que ao restringir um direito de uma pessoa para proteger uma coletividade é perfeitamente concebível a Idea da restrição de direitos.

Segundo Carlos José de Andrade[20]:

"Poder-se-á invocar a liberdade religiosa para efetuar sacrifícios humanos ou para casar mais de uma vez? Ou invocar a liberdade artística para legitimar a morte de um ator no palco, para pintar no meio da rua, ou para furtar o material necessário à execução de uma obra de arte? Ou invocar o direito de propriedade para não pagar impostos, ou o direito de sair do país para não cumprir o serviço militar, ou o direito de educar os filhos para espancá-los violentamente? Ou invocar a liberdade de reunião para utilizar um edifício privado sem autorização, ou a liberdade de circulação para atravessar via pública sem vestuário, ou o direito à greve para destruir ou danificar equipamentos da empresa (...)"

Como podemos observar, para se proteger uma coletividade ou um bem maior, podem-se restringir direitos, mas essa restrição não se baseia somente nas ordenações jurídicas, mas também na livre convicção do Juiz, que deve dar uma resposta no embate de regras e princípios, visando proteger uma coletividade, no caso de uma agente que usa o

---

20 ANDRADE, José C. Vieira de. **Os Direitos**. P. 216.

computador e a internet para cometer delitos contra a honra, contra o patrimônio e outras espécies de delitos, deve-se restringir o direito no que cerne o uso de equipamentos eletrônicos que possam permitir ou facilitar o cometimento de mais delitos.

Segundo Canotilho[21]:

"para comprovar a validade de uma restrição, julga necessário determinar o âmbito de proteção do direito, averiguar a finalidade da lei, tipo e natureza da restrição e observar se há respeito aos limites impostos pela Constituição. A metodologia impõe as seguintes indagações: a) trata-se de efetiva restrição do âmbito de proteção (bens jurídicos protegidos e a extensão da proteção) de norma consagradora de direito fundamental? b) a Constituição autoriza a restrição? c) a restrição tem como finalidade salvaguardar outros direitos ou interesses constitucionalmente protegidos? d) a lei restritiva cumpriu os requisitos prescritos expressamente pela constituição?"

Por isso deve-se o Juiz observar a proteção de algo maior ou mesmo de outro direito constitucionalmente protegido.

---

21 -CANOTILHO. **Direito**. P. 602.

CAPÍTULO V – LEGISLAÇÃO INTERNACIONAL

Legislação Européia de Crimes Digitais

Atualmente a União Européia tem rígidas leis para combater os *cybercrims*, ao mesmo tempo tem uma lei flexível que pode ser modificada de acordo com a evolução do *cybercrime*, o que facilita e deveria ser utilizado pelos nossos legisladores ao se tratar da lei de crimes digitais, uma das mais recentes alterações na legislação da União Européia é a punição a incitação ao terrorismo tendo a internet como meio de divulgação.

Segundo a reportagem Estadão.com.br :

"Os países da União Européia fecharam acordo na sexta-feira para a adoção de leis severas contra o incitamento ao terrorismo, a fim de reprimir o uso da Internet por grupos militantes.

Os ministros do Interior e da Justiça da União também concordaram, em reunião no Luxemburgo, em um plano de ação para tentar impedir que esses grupos obtenham explosivos.

A polícia afirma que a Internet assumiu grande importância para os militantes, permitindo que eles compartilhem know-how, planejem operações e difundam propaganda para uma audiência de massa.

"A Internet está sendo usada para inspirar e mobilizar terroristas locais... e funciona como um campo virtual de treinamento", afirma o texto do acordo entre os ministros.

Cada país membro deve tomar as medidas necessárias para garantir que as violações relacionadas ao terrorismo incluam provocação a cometer delitos terroristas, recrutamento para o terrorismo e treinamento para o terrorismo.

Os Estados também podem considerar tentativas de recrutar e treinar como crimes de terrorismo, mas não serão obrigados a fazê-lo, disse um funcionário da União.

Julio Perez Hernandez, secretário espanhol da Justiça, recebeu o acordo positivamente.

A batalha para antecipar (atos de terrorismo) é crucial para a Espanha", disse ele a repórteres. "Não devemos esperar pela fumaça para saber que existe terrorismo.

Em um esforço por acalmar os defensores dos direitos civis, a lei dispõe que a nova medida não poderá ser usada para restringir a liberdade de expressão e a liberdade de imprensa.

Antes de entrar em vigor, ela precisa ainda ser confirmada pelos ministros, depois que diversos Legislativos nacionais a debateram.

Um funcionário da Comissão Européia disse que países como Espanha e Itália já punem a incitação pública ao terrorismo, mas que outros, como os países escandinavos, teriam de alterar suas legislações a fim de incorporar o novo texto da União Européia.

Sob o plano de reforço da segurança com relação a explosivos, os ministros concordaram em estabelecer um sistema de alerta antecipado sobre roubos de explosivos e detonadores, até o final do ano."

Como pudemos observar a lei que coíbe os crimes digitais, quando é modificada ou ampliada, todos os países que fazem parte da União Européia têm de se adequar a nova Lei.

CAPITULO V – LEGISLAÇÃO AMERICANA

• o Código dos Estados Unidos

• TÍTULO 18 - CRIMES E CRIMINAIS procedimento

• PARTE 1 - CRIMES

• CAPÍTULO 47 - FRAUDE E FALSAS DECLARAÇÕES

Séc. 1030. Atividade relacionada com a fraude e em conexão com computadores

• (a) Quem -

• (1) ter acessado um computador sem o conhecimento ou autorização superior autorizado o acesso, e por meio deste tipo de conduta terem obtido informações de que tenha sido determinado pelo Governo dos Estados Unidos nos termos dos estatutos ou de uma ordem executiva que exigem proteção contra divulgação não autorizada se por razões da defesa nacional ou as relações externas, ou de quaisquer dados restritos, como definido no n. ° y. Da secção 11 da Lei de Energia Atómica de 1954, com razões para acreditar que tais informações assim obtidas poderiam ser utilizadas para o prejuízo dos Estados Unidos, ou com a vantagem de qualquer nação estrangeira premeditadamente comunica, transmite, ou causas de ser

comunicada, entregues, ou transmitida, ou tentativas de se comunicar, entregar, transmitir ou fazer comunicados, entregues, ou transmitida a mesma para qualquer pessoa que não tenha direito a recebê-lo, propositadamente ou mantém o mesmo e não efetuar a entregá-la ao agente ou empregado de untitled os Estados Unidos para recebê-la;

• (2) intencionalmente acede a um computador sem autorização ou superior autorizado o acesso, e, assim, obtém -

• (A) as informações contidas em um registro financeiro de uma instituição financeira, ou de um cartão emitente, tal como definido no ponto (n) do título 15, ou contidos em um arquivo de um organismo consumidor relato sobre um consumidor, como tais termos são definidos no Fair Credit Reporting Act (15U. SC 1681 e segs.);

• (B) informações de qualquer departamento ou agência dos Estados Unidos da América; ou

• (C) a partir de qualquer informação protegida computador, se a conduta envolvida uma comunicação interestaduais ou estrangeiros;

• (3) intencionalmente e sem autorização qualquer acesso nonpublic computador de um serviço ou organismo que seja exclusivamente para a dos Estados Unidos, acede a um

computador de que tal serviço ou organismo que seja exclusivamente para o uso do Governo do Reino Unido, o Governo dos Estados Unidos e que tal comportamento afeta pelo uso ou para o Governo dos Estados Unidos;

• (4) consciente e com intenção de defraudar, acede a um computador protegido sem autorização, ou excede o acesso autorizado, e por meio deste tipo de conduta destinado promove a fraude e obtiver qualquer coisa de valor, a menos que o objeto da fraude e da coisa obtida consiste apenas do uso do computador e do valor de tal utilização não seja superior a $ 5000 em qualquer 1 - anos;

• (5)

• (A) consciente provoca a transmissão de um programa, informações, códigos ou comando, e como resultado de tal conduta, intencionalmente provoca danos sem autorização, a um computador protegido;

• (B) intencionalmente acede a um computador protegido sem autorização, e como resultado de tal conduta, uma imprudência provoca danos; ou

• (C) intencionalmente acede a um computador protegido sem autorização, e como resultado de tal conduta, provoca danos;

• (6) consciente e com intenção de defraudar tráfegos (como definido na seção) em qualquer senha ou similar informações através do qual um computador pode ser acessado sem autorização, se –

• (A) o tráfico de seres humanos afecta comércio interestadual ou estrangeira, ou

• (B) tal computador é utilizado por ou para o Governo dos Estados Unidos;

• (7) com a intenção de extorquir a partir de qualquer pessoa, empresa, associação, instituição educacional, a instituição financeira, entidade governamental, ou outra entidade jurídica, dinheiro ou qualquer outra coisa de valor, transmite no comércio interestadual ou estrangeiro qualquer comunicação contendo qualquer ameaça à causar danos a um computador protegido, deve ser punido de acordo com o disposto na subsecção (c) desta seção.

• (b) quem tenta cometer um delito nos termos da subsecção (a) ou (b) desta seção devem ser punidos de acordo com o disposto na subsecção (c) desta seção.

• (c) Os punidos por uma ofensa na subsecção (a) ou (b) desta seção é –

• (1)

• (A) uma coima ao abrigo do presente título ou a prisão por não mais de dez anos, ou ambos, no caso de uma ofensa na subsecção (a) (1) desta seção, o que não ocorre depois de uma condenação por outro delito no âmbito do presente secção, ou uma tentativa de cometer um delito punível nos termos do presente parágrafo, e (B) uma coima ao abrigo do presente título ou a prisão por não mais de vinte anos, ou ambos, no caso de um dos

Fense na subsecção (a) (1) desta seção, que ocorre uma condenação por outro delito no âmbito desta secção, ou uma tentativa de cometer um delito punível nos termos do presente parágrafo;

• (2)

• (A) uma coima ao abrigo do presente título ou a prisão por não mais de um ano, ou ambos, no caso de uma ofensa na subsecção (a) (2), (a) (3), (a) (5) (C), ou (a) (6) desta seção, o que não ocorre depois de uma condenação por outro delito no âmbito desta secção, ou uma tentativa de cometer um delito punível nos termos do presente parágrafo; e

• (B) uma coima ao abrigo do presente título ou a prisão por não mais de 5 anos, ou ambos, no caso de uma ofensa na subsecção (a) (2), se -

• (i) a infração foi cometida com fins de vantagem comercial ou privado ganho financeiro;

• (ii) a infração foi cometida na promoção de qualquer ato criminoso ou tortuosos, em violação da Constituição ou leis dos Estados Unidos ou de qualquer membro, ou

• (iii) o valor da informação obtida excedem os US $ 5000;

• (C) uma coima ao abrigo do presente título ou a prisão por não mais de dez anos, ou ambos, no caso de uma ofensa na subsecção (a) (2), (a) (3) ou (a) (6) da esta seção, que ocorre após uma condenação por outro delito no âmbito desta secção, ou uma tentativa de cometer um delito punível nos termos do presente parágrafo; e (3) (A) uma coima ao abrigo do presente título ou a prisão por não mais de cinco anos, ou ambos, no caso de uma ofensa na subsecção (a) (4), (a) (5) (A), (a) (5) (B), ou (a) (7) desta seção, o que não ocorre após uma condenação por outro delito no âmbito desta secção, ou uma tentativa de cometer um delito punível nos termos do presente parágrafo, e (B) uma coima ao abrigo do presente título ou a prisão por não mais de dez anos, ou ambos, no caso

de uma ofensa na subsecção (a) (4), (a) (5) (A), (a) (5) (C), ou (a) (7) desta seção, que ocorre após uma condenação por outro delito no âmbito desta secção, ou uma tentativa de cometer um delito punível nos termos do presente parágrafo; e

• (d) O Serviço Secreto dos Estados Unidos devem para além de qualquer outra agência ter autoridade para investigar tais ofensas sob subseções (a) (2) (A), (a) (2) (B),

• () Os Estados Unidos devem Secret, para além de qualquer Serviço Secreto dos Estados Unidos deve ser exercida em conformidade com um acordo que será celebrado pelo secretário do Tesouro e do Procurador-Geral.

• (e) Como utilizado nesta secção -

• (1) o termo "computador" significa uns eletrônicos, magnéticos, ópticos, eletroquímicos, ou outro dispositivo de tratamento de dados de alta velocidade desempenho lógico, aritmética, ou funções de armazenamento, e inclui qualquer instalação de armazenamento de dados ou de comunicações diretamente relacionadas com a instalação ou a funcionar em conjugado com tais dispositivos, mas essa expressão não inclui uma máquina de escrever automáticas ou compositor, uma calculadora portátil mão, ou outro dispositivo semelhante;

(2) o termo "computador protegido", um computador -

• (A) para utilização exclusiva de instituição financeira ou de Governo dos Estados Unidos, ou, no caso de um computador não exclusivamente para esse uso, usado por ou para uma instituição financeira ou de Governo dos Estados Unidos e os comportamentos constitutivos do delito afeta essa utilização por ou para a instituição financeira ou do Governo; ou

• (B) que é usado no comércio interestadual ou estrangeiro ou de comunicação;

• (3) o termo "Estado" inclui o Distrito de Colúmbia, a Commonwealth de Puerto Rico, e de qualquer outra nação, a posse ou território dos Estados Unidos;

• (4) o termo "instituição financeira" significa -

• (A) uma instituição, com depósitos segurados pelo Federal Deposit Insurance Corporation;

• (B) do Federal Reserve ou um membro do Federal Reserve Incluindo todas Federal Reserve Bank;

• (C) uma cooperativa de crédito com contas segurada pela National Credit Union Administração;

• (D) um membro do Federal homo empréstimo bancário e qualquer casa sistema de empréstimo bancário;

• (E) qualquer instituição do Sistema de Crédito Agrícola sob a Farm Credit Act de 1971;

• (F) um broker-dealer registrada na Securities and Exchange Commission nos termos da secção 15 do Securities Exchange Act de 1934;

• (G), a Proteção dos Valores Mobiliários Investidor Corporation;

• (H) agência ou sucursal de um banco estrangeiro (conforme tais termos são definidos nos parágrafos (1) e (3) do ponto 1 (b) da International Banking Act de 1978), e (I) uma organização que operam sob a seção ou secção 25 (a) da Lei Federal Reserve.

• (5) o termo "financeiro recorde", as informações obtidas a partir de qualquer registro detidos por uma instituição financeira referente a um relacionamento com o cliente da instituição financeira;

• (6) o termo "ultrapassa acesso autorizado" significa um computador com acesso à autorização e à utilização desse acesso para obter ou alterar informação no computador que não tem direito a accesser modo a obter ou alterar;

• (7) o termo "ultrapassa acesso autorizado", o ramo legislativo ou judiciário do Governo ou de um dos departamentos executivos enumerados no ponto 5 do título; e

• (8) o termo "dano" significa qualquer prejuízo para a integridade ou a disponibilidade de dados, um programa, um sistema, ou informação, que -

• (A) provoca perda agregando pelo menos R $ 5000 em valor durante qualquer período de 1-ano ou mais pessoas;
(B) altera ou atrapalha, ou potencialmente altera ou atrapalha, o exame médico, diagnóstico, tratamento, cuidados de uma ou mais pessoas;

• (C) provoca danos físicos a qualquer pessoa, ou

• (D) ameace a saúde pública ou de segurança; e (9) o termo "entidade governamental" inclui o Governo dos Estados Unidos, nenhum país estrangeiro, bem como qualquer estado, província, município, ou outras subdivisões políticas de um país estrangeiro.

• (f) Esta seção não proíbe qualquer legalmente autorizado investigativo, protetor, ou uma atividade de inteligência agência de aplicação da lei dos Estados Unidos, um Estado, ou de uma subdivisão política de um Estado, ou de uma agência de inteligência dos Estados Unidos.

• (g) Qualquer pessoa que sofra danos ou prejuízos em razão de violação da presente secção pode manter uma ação cível contra o infrator a obter indenizações compensatórias e medidas cautelares ou reparação justa. Envolvendo violações Indenizações por danos, tal como definido na subseção (e) (8) (A) estão limitados a violações que envolvam danos, tal como definido na subseção (e) (8) (A) são limitados para os danos econômicos. Nenhuma ação pode ser intentada ao abrigo do presente subsecção não ser que tal ação seja iniciada within2 anos da data do ato imputado ou a data da descoberta do dano.

• (h) o Procurador-Geral e o Secretário do Tesouro presta contas anualmente ao Congresso, durante os primeiros 3 anos após a data da promulgação da presente subsecção (a) (5).

CAPITULO V – LEGILAÇÃO PORTUGUESA

Lei da Criminalidade Informática

Criminalidade Informática – Lei n° 109/91, 17 de Agosto

A assembléia da Republica decreta nos termos dos artigos 164°, alínea d), 168°, n° 1, alínea c), e 169°, n° 3, da Constituição, o seguinte:

CAPITULO I – Princípios gerais

Art. 1° Legislação penal

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

Art.2° Definições

Para efeitos de presente lei, considera-se:

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

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

c) Programa informático – um conjunto de instruções capazes, quando inseridos num suporte explorável em maquina, de permitir a maquina que tem por função o tratamento de informações indicar, executar ou produzir determinada função, tarefa ou resultado.

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

e) Produto semicondutor – a forma final ou intermédio de qualquer produto, composto por um substrato que inclua uma camada de material semicondutor e constituído por uma ou varias camadas de matérias condutoras, isolantes ou semicondutoras, segundo uma disposição conforme a uma configuração tridimensional e destinada a cumprir; exclusivamente ou não, uma função eletrônica;

f) Intercepção – o ato destinado a captar informações contidas num sistema automatizado de dados, através de dispositivos eletromagnéticos, acústicos, mecânicos ou outros;

g) Valor elevado – aquele que exceder 50 unidades de conta processual penal avaliada no momento da pratica do fato;

h) Valor consideravelmente elevado aquele que exceder 200 unidades de conta processual penal avaliada no momento da pratica do fato.

Art. 3° Responsabilidade penal das pessoas coletivas e equiparadas

1. As pessoas coletivas, sociedades e meras associações de fato são penalmente responsáveis pelos crimes previstos na lei, quando cometidos em seu nome e no interesse coletivo pelos seus órgãos ou representantes.
2. A responsabilidade é excluída quando o agente tiver atuado contra ordens ou instruções expressas de quem de direito.
3. A responsabilidade das entidades referidas no n° 1 não excluía responsabilidade individual dos respectivos agentes.
4. As entidades referidas no n° 1 respondem solidariamente, nos termos da lei civil, pelo pagamento das multas, indenizações e outras prestações em que forem condenados os agentes das infrações previstas na presente lei.

CAPITULO II – Dos crimes ligados à informática

Art. 4° Falsidade informática

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

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

atuando com intenção de causar prejuízo a outrem ou de obter um beneficio ilegítimo, para se ou para terceiros.

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

Art. 5° Dano relativo a dados ou programas informáticos

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

2. A tentativa e punível.

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

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

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

Art. 6° Sabotagem informática

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

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

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

Art. 7° Acesso ilegítimo

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

2. A pena será ate três anos ou multa se o acesso for conseguido através da violação de regras de segurança.

3. A pena será a de prisão de um a cinco anos quando:

a) Através do acesso, o agente tiver tomado conhecimento de segredo comercial ou industrial ou de dados confidenciais, protegidos por lei;

b) O beneficio ou vantagens patrimoniais obtidos forem de valor consideravelmente elevado.

4. A tentativa é punível.

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

Art. 8° Intercepção ilegítima

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

2. A tentativa é punível.

Art.9° Reprodução ilegítima de programa protegido

1. Quem, sem para tanto autorizado, reproduzir, divulgar ou comunicar ao público um programa informático protegido por lei será punido com pena de prisão ate três anos ou com pena de multa.
2. Na mesma pena incorre quem ilegitimamente reproduzir topografia de um produto semicondutor ou explora comercialmente ou importa. para estes fins, uma topografia ou um produto semicondutor fabricado a partir dessa topografia.
3. A tentativa e punível.

Art. 10° Penas aplicáveis às pessoas coletivas e equiparadas

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

a) Admoestação;
b) Multa;
c) Dissolução.

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

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

4. Cada dia de multa corresponde a uma quantia entre 10.000$ e 200.000$, que o tribunal fixara em função da situação econômica e financeira da pessoa coletiva ou equiparada e dos seus encargos.

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

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

CAPÌTULO III – Penas acessórias

Art. 11° Penas acessórias

Relativamente aos crimes previstos no presente diploma, podem se aplicadas as seguintes penas acessórias: O Comitê Europeu sobre Crime Problemas (CDPC) examinou atentamente as acusações formuladas por algumas delegações federal contra a cláusula contida no artigo 41 ° do projeto de convenção. A inclusão de uma cláusula deste tipo

envolve um equilíbrio delicado entre os diferentes valores da ordem jurídica internacional.

A fim de atender a estas acusações, o CDPC decidiu introduzir as seguintes alterações ao projeto de convenção com vista a restringir a aplicação da cláusula, tanto quanto possível:

• O âmbito de aplicação foi limitado ao disposto no Capítulo II (direito penal material, direito processual e jurisdição). Estados federais que façam uso desta disposição ainda estaria no âmbito da obrigação de cooperar plenamente com as outras partes nos termos do Capítulo III.

• Um novo parágrafo foi acrescentado à cláusula exigindo que o governo federal para se referir às disposições, a implementação dos que estão sob a jurisdição dos Estados constituintes ou outras entidades territoriais semelhantes, para as autoridades de tais entidades com parecer favorável.

• O artigo 46 ° do projeto de convenção multilateral sobre as consultas das partes foi completada. As partes serão obrigadas a examinar regularmente os efeitos de reservas e declarações, incluindo as declarações federais, sobre a Convenção da operação.

CONCLUSÃO

Após exarar o tema pesquisado, podemos avaliar que nossa legislação não tipifica todas as espécies de crimes digitais, mais ainda sim abrange grande parte desses crimes, embora ainda sim nossa legislação preveja o principal, que é a invasão aos sistemas computacionais fechados, pois para a prática de qualquer conduta ilícita os dados terão de ser violados, é claro que se houvesse uma legislação específica para cada tipo de delito informático seria infinitamente mais fácil a coibição destas condutas delituosas.

Ainda sim tramita pelo senado uma proposta de lei versando sobre os delitos cometidos através do computador e da internet que partiu do senador Eduardo Azeredo.

Fazendo uma breve comparação com a legislação Americana e Portuguesa podemos notar claramente que nossa legislação ainda "engatinha" mais aos pouco se aproxima da legislação desses países ditos "de 1° mundo", mais ainda temos muito a trabalhar, pois esse é um território novo para o direito bem como para o legislador. Esse trabalho tem a intenção de elucidar algumas dúvidas quanto ao tema, pois ainda é um tanto nebuloso na esfera jurídica, mas com uma legislação adequada tais crimes poderão ser coibidos com mais eficiência e punidos com mais rigor, pois que se utiliza de meios eletrônicos para o cometimento de tais crimes obrigatoriamente detém um grande conhecimento técnico sobre o funcionamento de sistemas computacionais e se aproveita de tais conhecimentos para obter vantagem frente a outros "leigos" no que tange tal assunto.

No presente trabalho abordamos a classificação penal dos crimes digitais, como crimes próprios, crimes impróprios, crimes mistos, crimes formais, materiais, de mera conduta, bem como abordados o tempo e o local do crime, o inter criminis e os sujeitos do delito.

Ainda abordamos os crimes mais comuns na internet, bem como as provas e as punições, o e-mail sendo aceito como prova, a possibilidade da pena de restrição de direitos.

REFERENCIAS BIBLIOGRAFICAS

http://www.terravista.pt/mussulo1139/crim.html

http://safernet.org.br/twiki/bin/view/SaferNet/Noticia20070521123629?sortcol=0;table=2;up=0 em 23/07/2008 às 13:18

BASTOS. Celso Ribeiro. Curso de direito constitucional. 19ª Edição. Editora Saraiva: São Paulo. 1998

http://www.denunciar.org.br/twiki/bin/view/SaferNet/Noticia20070713005321 às 10:00 de 23/07/2008.

FRAGOSO, Heleno Cláudio. Lições de Direito Penal: a nova parte Geral. 8ª Ed. Rio de Janeiro: Forense

MCCLAURE, Stuart, SCAMBRAY, Joel, KURTZ, George. Hackers expostos: segredos e soluções para a segurança de redes. São Paulo: Makron Books, 2000

MIRABETE, Julio Fabbrini. Código penal interpretado. São Paulo: atlas 1999

PRADO, Luis Regis. Curso de Direto Penal volume 1. São Paulo. Editora Revista dos Tribunais

LEIRIA, Antônio José Fabrício, Teoria e prática da lei penal, 1981, PP. 93-94 apud FRANCO ET AL., 1987, p.13

ZAFFARONI, Eugenio Raúl e PIERANGELI, José Henrique. *Manual de Direito Penal Brasileiro Parte – Geral.* 2ª. ed., São Paulo: Revista dos Tribunais, 1999.

LIMA VIANNA, Túlio. Fundamentos de Direito Penal Informático – Ed. Forense – 2003

BITENCOURT Cezar Roberto - Manual de Direito Penal, Parte Geral, Vol. 1

CAPEZ, Fernando, membro do Ministério Público, *in* "Curso de Direito Penal", Parte Geral, Vol. 1

JUNIOR, Miguel Reale, *in* "Instituições de Direito Penal", Parte Geral, vol. I

HUNGRIA, Nelson, *in* "Comentários ao Código Penal", vol. I Tomo II, Ed. Forense, 4ª edição

SUTHERLAND, E.H. White-collar crimilality in American sociological Review. V, p. 11, 1940 apud BARATTA, 1999

BASTOS. Celso Ribeiro. Curso de direito constitucional. 19ª Edição. Editora Saraiva: São Paulo. 1998

BELMONTE. Alexandre Agra. O Monitoramento da Correspondência Eletrônica nas Relações de Trabalho. São Paulo: LTr. 2004

CANOTILHO, José Joaquim Gomes. Direito constitucional. 5. ed., Coimbra:

Livraria Almedina, 1991.

ANDRADE, José Carlos Vieira de. Os Direitos fundamentais na constituição

Portuguesa de 1976. Coimbra: Almedina, 1998.

GRECO, Rogério - Curso de Direito Penal - Vl. 1 - 10 Ed. 2008 – editora Impetus