FACULDADES SENAC DE CIÊNCIAS EXATAS E TECNOLOGIA

Savio Talamoni Vallochi

Tipificação dos Crimes de Informática, métodos de combate e prevenção

São Paulo
2004

SAVIO TALAMONI VALLOCHI

Tipificação dos Crimes de Informática, métodos de combate e prevenção

Trabalho de conclusão de curso apresentado as Faculdades Senac de Ciências Exatas e Tecnologia, como exigência parcial para obtenção do grau de pós-graduação em Segurança de Sistemas em Redes.

Orientador Prof. Dr. Volnys Borges Bernal

São Paulo
2004

Vallochi, Savio Talamoni
Tipificação dos Crimes de Informática, métodos de combate e prevenção / Savio Talamoni Vallochi. – São Paulo, 2004.
80 f.

Trabalho de Conclusão de Curso – Faculdade Senac de Ciências Exatas e Tecnologia.
Orientador: Prof. Dr. Volnys Borges Bernal

Palavras-chave: Crimes de Informática – *Cyber crimes* – Crimes Digitais – Prevenção – Combate

Aluno: Savio Talamoni Vallochi
Título: Tipificação dos Crimes de Informática, métodos de combate e prevenção.

A banca examinadora dos Trabalhos de Conclusão em sessão pública realizada em 23/02/2005, considerou o candidato:

(X) aprovado ( ) reprovado

1) Prof. Dr. Volnys Borges Bernal
2) Prof. Marcelo Lau
3) Prof. Dr. Pedro Luís Próspero Sanchez

Dedico meu trabalho a todas as pessoas que contribuíram direta ou indiretamente para a minha formação, em especial a amada Silvana Chmelyk e a minha querida família.

AGRADECIMENTO

Agradeço a todos os professores do curso de Pós-Graduação em Segurança de Sistemas em Redes do SENAC por estarem sempre dispostos a transmitir o melhor aos alunos, especialmente ao Professor Doutor Volnys, orientador deste trabalho.

RESUMO

Com o avanço tecnológico, e o nascimento da Internet, surgiram novas modalidades criminosas que ainda não estão previstas em nosso ordenamento jurídico, o que acaba impossibilitando a punição dos delinqüentes, visto que nossa lei não permite que seja aplicada nenhuma pena sem que antes haja uma previsão legal. Também surgiram novas formas de praticar os já conhecidos crimes, abrindo caminho à criatividade dos infratores que invadiram o mundo virtual assegurando-se da dificuldade de identificação e conseqüente falta de punição pelos atos praticados.

Este trabalho visa apresentar alguns dos crimes que são praticados através e contra a informática, assim ditos Crimes de Informática e, também, formas de proteção que a ciência tecnológica criou e tem criado com a finalidade de minimizar a possibilidade da ocorrência destes crimes nas empresas e residências.

Então, o objetivo é apresentar um conteúdo simplificado de tipificações e maneiras de amenizar a prática destes delitos, tendo em vista a falta de previsão legal em alguns casos, e o pouco combate contra estes crimes de ordem tecnológica.

ABSTRACT

With technological advance, and the origin of Internet, new criminal modalities that are not still foreseen in our legal system, precluding the delinquent punishment, inasmuch as our law does not allow any penalty be done before there is a legal prevision. New ways of practicing the known crimes have aroused too, making way to the infringer creativity that trespassed the virtual world making sure of the difficulties of identification and the consequent lack of punishment by the acts done.

These papers focuses the demonstration of some of the crimes that are done through and against the information technology, known as Web Crimes and also present the protection ways that the technological science created and has created with a view to lower the possibility of occurrence of these crimes in the companies and residences.

Then, the aim is to present simplified contents of illegal facts and ways of soothing the practice of these wrongs, with a view to the lack of legal prevision in some cases, and the little combat against these crimes of technological order.

SUMÁRIO

1 INTRODUÇÃO

São indiscutíveis os benefícios que o avanço da tecnologia, o uso de computadores, e o avanço das comunicações mundiais, em especial a Internet, trouxeram para a sociedade Brasileira. As facilidades alcançadas pelo uso do computador transformaram a vida moderna. É a era da Informática. (1)

As inovações na área tecnológica propiciaram o aparecimento de novos tipos de crimes ou novas formas de praticar os já conhecidos tipos penais. Conseqüentemente também surgiram formas de tentar amenizar, neutralizar ou prevenir a prática destes crimes.

Este trabalho tem por objetivo conceituar, classificar, descrever e analisar os crimes de informática no Brasil, e apresentar formas tecnológicas de tentar prevenir a prática destes crimes, como por exemplo, a implementação de rotinas que permitam conferir autenticidade, integridade, confidencialidade e irretratabilidade para as informações e dados que transitam em meios telemáticos.

---

1 - CASTRO, Carla Rodrigues Araújo de. **Crimes de Informática e seus Aspectos Processuais**. Rio de Janeiro: Lumen Juris, 2003.

2 CRIMES DE INFORMÁTICA

2.1 Conceito

Crimes de Computador [2], Crimes via Internet [3], Crime Informático [4], Delitos Praticados por Meio da Internet [5], Crimes Tecnológicos [6], Crimes na Internet [7] e Crimes Digitais [8], entre outros. Não há um consenso quanto ao nome genérico dos delitos que ofendem interesses relativos ao uso, à propriedade, à segurança ou à funcionalidade de computadores e equipamentos periféricos (hardwares), redes e programas de computadores. Dentre essas designações, as mais comumente utilizadas têm sido as de crimes de informática ou crimes informáticos.

'Crimes de Informática' possui um sentido mais amplo, pois engloba todo o sistema de informática, não apenas aqueles crimes praticados através da Internet, sendo este uma espécie dos crimes de informática.

---

2 - BRASIL, Ângela Bittencourt. **Crimes de Computador**. Disponível em: <www.ciberlex.adv.com>. Acesso em: 20 nov. 2004.
3 - MIRANDA, Marcelo Baeta. **Uma abordagem dinâmica aos crimes via Internet. direitos difusos, instrumentalidade e antecipação prática. Prevenção e Reprresão. Iniciativas no Brasil e principiologia**. Disponível em: <www.jusnavegandi.com.br>. Acesso em: 20 nov. 2004.
4 - RODRIGUES, Miguel Ángel Davara. **Crime Informático**. Disponível em: <www.jusnavegandi.com.br>. Acesso em 23 nov. 2004.
5 - MARTINELLI, João Paulo Orsini. **Aspectos relevantes da Criminalidade na Internet.** Disponível em: <www.jusnavegandi.com.br>. Acesso em 23 nov. 2004.
6 - MACHADO, Eduardo de Paula. **Novas Fronteiras da Criminalidade:** Os crimes Tecnológicos, in Boletim IBCCrim, nº81, ano 7, agosto de 1999.
7 - BRITO, Eduado Valadares de. **Crimes na Internet.** Disponível em: <www.infojus.com.br>. Acesso em 23 nov. 2004.
8 - CORREIA, Gustavo Testa. **Aspectos Jurídicos da Internet**, p.42.

Da mesma forma que divergem as nomenclaturas, também divergem os conceitos de Crimes de Informática entre diversos autores.

Para IVETTE SENISE FERREIRA, “crime de informática é toda ação típica, antijurídica e culpável contra ou pela utilização de processamento automático e/ou eletrônico de dados ou sua transmissão”. (9)

Para o Professor JOÃO MARCELLO DE ARAÚJO JUNIOR, “crime de informática é uma conduta lesiva, dolosa, a qual não precisa, necessariamente, corresponder à obtenção de uma vantagem ilícita, porém praticada, sempre, com a utilização de dispositivos habitualmente empregados nas atividades de informática”. (10)

ÂNGELA BITTENCOURT BRASIL não vê diferença no conceito de crime comum e crime de informática; salienta, todavia, que a fronteira que os separa é a utilização do computador para alcançar e manipular o seu sistema em proveito próprio ou para lesionar outrem. (11)

Podemos observar que apesar do bem jurídico protegido ser o sistema informático, alguns autores utilizam um conceito mais restrito, considerando como crimes de informática apenas aqueles praticados contra dados, informações ou software. Já a Professora CARLA RODRIGUES ARAÚJO DE CASTRO prefere um conceito mais amplo, abrangendo a totalidade dos equipamentos utilizados na informática, como também os crimes cometidos através deste sistema. (12)

Acredito que a definição mais completa seria uma mescla da definição de IVETTE SENISE FERREIRA com a do Professor JOÃO MARCELLO DE ARAÚJO JUNIOR e a de CARLA RODRIGUES ARAÚJO DE CASTRO, sendo crime de informática toda

---

9 - **Os Crimes da Informática**, in Estudos em Homenagem a Manoel Pedro Pimentel, São Paulo: RT, 1992, pp. 141-142.
10 - **Computer Crime**, in Anais da Conferência Internacional de Direito Penal, 1988. Rio de Janeiro: PGDF, 1998, p.461.
11 - **Informática Jurídica** - O Ciber Direito, pp. 133-134.
12 - CASTRO, Carla Rodrigues Araújo de. **Crimes de Informática e seus Aspectos Processuais**. Rio de Janeiro: Lumen Juris, 2003.

ação típica, antijurídica, dolosa, a qual não precisa, necessariamente, corresponder à obtenção de uma vantagem ilícita, porém praticada, sempre, com a utilização de dispositivos habitualmente empregados nas atividades de informática ou contra eles. Esta mescla se explica pelos seguintes fatores: para que ocorra a constituição de um crime de informática a ação deve ser típica, pois o crime deve ser descrito na lei penal do contrário feriria o princípio da legalidade que diz: Artigo 5º, inciso XXXIX, Constituição federal Brasileira, “não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal”. A ação deverá ser antijurídica, pois deve ferir o ordenamento jurídico, do contrário seria uma ação legal, não constituindo crime. Para a prática deste crime, necessariamente a conduta deverá dolosa, pois não há que se falar em crime de Informática sem que haja intenção ou o risco do autor na prática do delito. Ao meu ver, não existe crime de Informática na modalidade culposa. Não há necessidade de obtenção de vantagem para a tipificação do crime de informática, visto que certas condutas danosas, como pichação de um SITE, podem não render vantagem, porém, podem provocar danos. Para a configuração de crime de informática há que se considerar sempre a utilização de dispositivos habitualmente empregados nas atividades de informática ou que o crime seja praticado contra estes dispositivos.

2.2 Classificação

Não há consenso na classificação dos delitos de informática. Todavia, a taxonomia mais aceita é a propugnada por HERVÉ CROZE e YVES BISMUTH [13], que distinguem duas categorias de crimes informáticos:

a) os crimes cometidos contra um sistema de informática, seja qual for a motivação do agente;

b) os crimes cometidos contra outros bens jurídicos, por meio de um sistema de informática.

No primeiro caso, temos o delito de informática propriamente dito, aparecendo o computador como meio e meta, podendo ser objetos de tais condutas o computador, seus periféricos, os dados ou o suporte lógico da máquina e as informações que guardar. No segundo caso, o computador é apenas o meio de execução, para a consumação do crime-fim, sendo mais comuns nesta espécie as práticas ilícitas de natureza patrimonial, as que atentam contra a liberdade individual e contra o direito de autor. [14]

Para LUIZ FLÁVIO GOMES, os crimes informáticos dividem-se em crimes contra o computador; e crimes por meio do computador [15], em que este serve de instrumento para atingir a meta. O uso indevido do computador ou de um sistema informático servirá de meio para a consumação do crime-fim. O crime de fraude eletrônica de cartões de crédito serve de exemplo.

---

13 - Citados por Ivette Senise Ferreira, p. 214-5.
14 - Citados por Ivette Senise Ferreira, p. 214-5.
15 - GOMES, Luiz Flávio, Atualidades criminais (1). Disponível em: <www.direitocriminal.com.br>. Acesso em 30 nov. 2004.

Outra classificação é aquela que divide os crimes de informática em próprios ou impróprios. Próprios são aqueles que só podem ser praticados através da informática. Estes são os ditos crimes novos, que surgiram com a inovação tecnológica, muitas vezes podem não ser punidos por não existir legislação específica a respeito. São exemplos de crimes próprios: violação, interceptação e violação de e-mail, pirataria, pichação de páginas entre outros.

Já os crimes de informática impróprios são aqueles que podem ser praticados ou não através da informática. Exemplos: crimes de ameaça, estelionato, calúnia e pedofilia.

Existem outras classificações, como a de IVETTE SENISE FERREIRA que divide os crimes de informática em duas categorias: na primeira, os atos são dirigidos contra o sistema de informática, divididos em atos contra o computador e atos contras os dados ou programas de computador. Na segunda categoria estão os atos cometidos por intermédio do sistema de informática, que podem ser contra o patrimônio, contra a liberdade individual e contra a propriedade imaterial.(16)

2.3 Lugar do Crime de Informática

A determinação do lugar de um crime é fundamental para a aplicação ou não da lei brasileira e também para a definição da competência para o julgamento do delito.

Para melhor entendimento da lei penal no espaço há que considerar alguns princípios, conforme abaixo:

---

16 - **Os crimes de Informática**, in Estudos Jurídicos em Homenagem a Manoel Pedro Pimentel, pp. 146-152.

a) Princípio da Territorialidade – aplica-se a Lei do Estado aos fatos ocorridos em território nacional.

b) Princípio da Nacionalidade – aplica-se e Lei do Estado aos seus cidadãos onde quer que eles estejam.

c) Princípio da Defesa – aplica-se a Lei do Estado em razão da nacionalidade do bem jurídico tutelado.

d) Princípio da Justiça Penal Universal – aplica-se a Lei do Estado a qualquer crime, independentemente da nacionalidade do agente, do bem jurídico lesado e do local do fato.

e) Princípio da Representação – aplica-se a Lei do Estado em aeronaves e embarcações privadas, quando realizado o crime no estrangeiro.

O Código Penal Brasileiro adotou em seu artigo 5º, o princípio da territorialidade como sendo regra e os demais princípios (Nacionalidade, Defesa, Justiça Penal Universal e da Representação) como acessórios.

Conforme reza o artigo 6º do Código Penal Brasileiro, “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 devia produzir o resultado”.

Sendo assim, para que seja aplicada a lei brasileira, é necessário que o crime haja tocado o território nacional [(17)]. Há também o crime à distância, onde a conduta é praticada fora do país e o resultado ocorre aqui, ou vice-versa.

Para os crimes de informática, será necessário justamente identificar o local do resultado e da ação, caso algum tenha ocorrido no Brasil, será aplicada a lei brasileira.

---

17 - Nelson Hungria, Comentários ao Código Penal, 1977, pp. 164-165.

Analisando o texto acima, parece simples resolvermos todas as questões de aplicabilidade da lei penal no espaço, porém, existem algumas questões que são colocadas por alguns autores à cerca do assunto que demonstram as dificuldades encontradas, como RICHARD SPINELLO: “a Internet é uma tecnologia global sem fronteiras e sem donos, sendo quase impossível para qualquer nação garantir a execução de leis ou restrições que se busque impor no ciberespaço. Se os Estados Unidos, o México ou o Brasil decidirem proibir a pornografia *online*, esses países podem fiscalizar o cumprimento de tal proibição apenas entre os provedores e usuários em seus territórios. Infratores localizados na Europa ou na Ásia não estariam proibidos de disponibilizar material pornográfico na rede, acessível a qualquer pessoa, em qualquer parte”.(18)

Da mesma forma, CELSON VALIN (19) diz que "o grande problema ao se trabalhar com o conceito de jurisdição e territorialidade na Internet, reside no caráter internacional da rede. Na Internet não existem fronteiras e, portanto, algo que nela esteja publicado estará em todo o mundo. Como, então, determinar o juízo competente para analisar um caso referente a um crime ocorrido na rede?".

Quando um crime é cometido na Internet ou por meio dela, o crime irá se consumar em todos os locais onde a rede seja acessível. Imaginemos um exemplo para o crime de calúnia. Se um sujeito atribui um fato criminoso a alguém inocente e lança essa declaração na Internet, a ofensa poderá ser vista e conhecida em qualquer parte do mundo.

A questão de definição do local de um crime de informática pode facilmente ser

---

18 - SPINELLO. Op. cit., p. 38.

19 - A questão da jurisdição e da territorialidade nos crimes praticados pela Internet. In Direito, sociedade e informática: limites e perspectivas da vida digital. Florianópolis: Fundação Boiteux, 2000, p. 115.

resolvida levando-se em consideração o disposto no Artigo 6º do Código Penal. Já o problema da aplicabilidade da Lei Penal é mais complicado, visto que irá depender muitas vezes, da ratificação e acordos internacionais.

O Artigo 7º traz alguns casos de aplicabilidade da Lei Brasileira mesmo que o crime tenha ocorrido no exterior. É o caso, por exemplo, do crime praticado por brasileiro em outro país.

2.4 Sujeito Ativo e Sujeito Passivo nos Crimes de Informática

Qualquer pessoa pode se tornar um sujeito ativo de um crime de informática. Um estelionato praticado por meio da Internet não requer nenhuma qualidade especial do agente, apenas que tenha um conhecimento específico para a atuação.

Determinados crimes podem ser praticados por representantes legais das pessoas jurídicas relacionadas com a rede. Exemplo: Um provedor de acesso à rede mundial recusar informações diante de uma ordem judicial. Os representantes da empresa poderiam responder por crime de desobediência.

Qualquer pessoa também poderá ser sujeito passivo de um crime de informática, visto que qualquer um pode, por exemplo, receber um vírus destrutivo ou ter os dados de seu computador subtraídos.

Existem muitos empecilhos para se saber quem são os sujeitos ativo e passivo de um crime de informática. Diferentemente do mundo “real”, quando um crime é praticado no ciberespaço o exame da identidade e a autenticação dessa identidade não podem ser feitos visualmente, ou pela verificação de documentos ou de

elementos identificadores já em si evidentes, como placas de veículos ou a aparência física, por exemplo. (20)

Existe também a questão da publicidade. Muitas vezes, no caso das empresas, a vítima preferem arcar com os prejuízos causados por uma infração, do que tornar público o fato de ter sido vítima de um delito. Imagine o exemplo de um banco que teve seu sistema violado e o dinheiro de alguns correntistas tenha sido desviado para contas desconhecidas. Certamente o banco ressarcirá seus clientes, sendo este o prejuízo sofrido. A publicidade do episódio poderá causar prejuízos maiores para a imagem da empresa. Daí que algumas empresas preferem o silêncio.

Uma das soluções para o problema de identificação do sujeito ativo de crimes de informática seria a implementação de rotinas que permitam conferir autenticidade, integridade, confidencialidade e irretratabilidade para as informações e dados que transitam em meios telemáticos. Esta tem sido uma preocupação constante tanto para analistas e cientistas, como para aqueles diretamente envolvidos com o Direito Penal Informático.

---

20 - ARAS, Vladimir. **Crimes de Informática. Uma nova criminalidade**. Disponível em: < www.jus.com.br>. Acesso em: 23 out. 2004.

2.5 Dos crimes

A Polícia Federal (PF) brasileira divulgou dados preocupantes sobre fraudes na rede mundial de computadores, a Internet. As fraudes via e-mail aumentaram 856% no primeiro semestre - passando de 142 nos primeiros seis meses do ano passado para 1.358 no mesmo período deste ano (2004). Na mesma oportunidade, a polícia informou que investigações feitas no País e no exterior mostram que cerca de dois terços das páginas de pedofilia na Internet também têm origem brasileira. [21]

Os dados acima, apesar de preocupantes, são uma pequena parcela dos crimes que podem ser praticados através da Informática e que a cada dia tomam proporções maiores no Brasil e no mundo.

A partir deste momento, passaremos a analisar os tipos penais mais comumente praticados no Brasil e suas implicações legais.

2.6 Crimes Contra a Honra

São três os crimes contra a honra previstos no Código Penal Brasileiro: calúnia, difamação e injúria.

Artigo 138. Caluniar alguém, imputando-lhe falsamente fato definido como crime:

Pena – detenção de 6 (seis) meses a 2 (dois) anos, e multa.

---

21 - URBAN, Aldo. **Dispara número de golpes eletrônicos**. Disponível em: <http://www.an.com.br/2004/out/06/0inf.htm>. Acesso em 01 dez. 2004.

Artigo 139. Difamar alguém, imputando-lhe fato ofensivo a sua reputação:

Pena – detenção, de 3 (três) meses a 1 (um) ano, e multa.

A calúnia e a difamação se diferenciam também através do fato que é imputado a vitima; na calúnia, o fato é definido como crime, na difamação é ofensivo a honra. Em ambos os casos, para que haja consumação do crime é necessário que uma terceira pessoa tome conhecimento do fato. Se apenas o ofendido tomar ciências dos fatos, não há que se falar em crime. Tais crimes podem ser praticados na Internet através de *homepages*, salas de bate-papo entre outros. Exemplos: Se uma determinada pessoa cria uma *homepage* imputando um fato criminoso a outra, e esta página é acessada por terceiros, já haveria a consumação do crime de calúnia. Se em uma sala de bate-papo, uma pessoa atribui um fato ofensivo à honra de outra e todos os demais participantes da sala tomam conhecimento do fato, constituirá crime de difamação. Caso o bate-papo esteja sendo realizado privativamente entre ofensor e ofendido e nenhuma outra pessoa tomar conhecimento da ofensa, o crime não será configurado. (22)

Artigo 140. Injuriar alguém, ofendendo-lhe a dignidade ou o decoro:

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

Neste caso o ofensor não irá imputar à vítima a prática de um fato, como na calúnia e na difamação, mas sim uma característica ou qualidade.

Para configuração do crime de injúria, basta que o ofendido tome conhecimento do fato. Este delito pode ser praticado por e-mail, salas de bate-papo, nas *homepages* e etc.

Além dos crimes contra a honra citados, existem também os crimes contra a honra previstos na lei especial 5.250/67, artigos 20, 21 e 22 que tipifica os crimes de

---

22 - CASTRO, Carla Rodrigues Araújo de. **Crimes de Informática e seus Aspectos Processuais**. Rio de Janeiro: Lumen Juris, 2003.

calúnia, difamação e injúria praticados através de notícias de jornais, publicações, radiodifusão e noticiosos.

Aos jornais e periódicos publicados na Internet aplica-se a Lei Especial.

2.7 Ameaça

Artigo 147. Ameaçar alguém, por palavra, escrito ou gesto, ou qualquer outro meio simbólico, de causar-lhe mal injusto e grave:

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

O sujeito pode utilizar-se de um site para inserir um texto ameaçador, podendo também fazê-lo através de salas de bate-papo ou e-mail. Em todos estes casos o computador é meio para atingir o fim de ameaçar.

Para a configuração do crime de ameaça há que considerar que o agente esteja agindo com dolo. Uma simples brincadeira de mau gosto não configura o crime.

Parte da doutrina e da jurisprudência exige o ânimo calmo e refletido para a configuração do crime de ameaça. Quando o sujeito age com ódio, exaltação, no calor da discussão, não há que se falar em crime. [23]

---

23 - CASTRO, Carla Rodrigues Araújo de. **Crimes de Informática e seus Aspectos Processuais**. Rio de Janeiro: Lumen Juris, 2003.

2.8 Violação e Interceptação de e-mail

Violar e-mail é crime? E se a resposta for afirmativa, qual crime?

O artigo 151 do Código Penal indica o seguinte crime:

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

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

De acordo com DANIEL CHRISTIANINI NERY, pelo tipo penal, não só a violação, mas a devassa, de forma geral, é combatida pelo ordenamento jurídico. Dessa forma, independe de violação, de rompimento ou não de lacres, da publicidade ou não do conteúdo etc. (24)

Mas o que significa devassar? "1. Invadir ou observar (aquilo que é defeso ou vedado); 2. Ter vista para dentro de; 3. Descobrir, penetrar, esclarecer." (25)

O simples fato de ter acesso ao conhecimento que lhe é vedado já constitui uma devassa, passível de penalidade em nosso Código Penal, independente do conteúdo da mensagem ou ainda desse conteúdo ser ou não utilizado posteriormente. Devassar é um gênero, do qual o violar é espécie.

Mas o tipo penal do artigo 151 ainda indica que essa devassa deve ser indevida. Obviamente, se existe o "dever" de se devassar determinada correspondência, não há que se falar em crime, pois a conduta não estará mais tipificada, motivo pelo qual a quebra de sigilo autorizada judicialmente, por exemplo, é válida, não constituindo crime.

---

24 - NOGUEIRA, Fernando Célio de Brito. **Violação de e-mail é crime?**. Disponível em: <www.ibccrim.org.br>. Acesso em 02 dez. 2004.
25 - SILVA, Adalberto Prado e. **Novo Dicionário Melhoramentos**, Volume II - 4ª edição - Ed. Melhoramentos – 1968.

Observadas tais considerações, temos que o crime praticado por um Hacker (pessoas que usam seus conhecimentos de informática para acessar computadores alheios), ao acessar mensagens de terceiros (devassar), sem seu conhecimento (indevidamente), estaria plenamente tipificado no Artigo 151 do Código Penal, independente de chaves, senhas, *firewall*, sistemas de criptografias etc. [26]

O problema agora é a definição de correspondência, conforme abaixo:

A Lei de Privilégio Postal da União (Lei 6.538/78) nos indica, em seu artigo 7º, parágrafo 1º, a seguinte situação:

Art 7º - Constitui serviço postal o recebimento, expedição, transporte e entrega de objetos de correspondência, valores e encomendas, conforme definido em regulamento.

§ 1º - São objetos de correspondência:

a) carta;

b) cartão-postal;

c) impresso;

d) cecograma;

e) pequena-encomenda.

De acordo com o artigo citado, a mensagem de correio eletrônico não poderá ser equiparada à correspondência fechada prevista no tipo penal, pois o conceito de correspondência nos é dado pela mesma Lei nº 6.538/78, em seu artigo 47 (toda comunicação pessoa a pessoa, por meio de carta, através da via postal ou telegrama).

Assim, não poderíamos falar que o e-mail seria uma correspondência, não por não haver semelhança (de fato existe), mas por não constar na letra da Lei. Impossível,

---

26 - NOGUEIRA, Fernando Célio de Brito. **Violação de e-mail é crime?**. Disponível em: <www.ibccrim.org.br>. Acesso em 02 dez. 2004.

devido aos princípios penais, seria interpretar de forma extensiva tal assertiva, em prejuízo ao réu. Chegaríamos ao entendimento de que, por não ser considerada correspondência pela Lei, não poderia a violação de e-mail ser tipificada no artigo 151 do Código Penal, a menos que houvesse uma alteração na Lei 6.538/78, que ampliasse os limites do termo “correspondência”.

Temos agora a seguinte situação: O acesso ao e-mail não seria considerado crime.

Concluindo isso, chegamos a mais uma questão: se o e-mail não é uma correspondência, o que seria? Creio que não haverá nenhuma divergência em dizer que e-mail é, no mínimo, uma forma de comunicação.

O fato é que, diante de tal situação, o Governo editou a Lei 9.296, de 24-7-96, que regulamentou o artigo 5º, XII, parte final de nossa Constituição Federal e tem, em seu artigo 10º, a chave de toda a nossa discussão, indicando:

Art. 10º - 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.

A situação fica muito mais clara. A mera interceptação (independente da intenção do interceptador) de uma com unicação (não é correspondência, pode ser qualquer tipo de comunicação) de informática (uma colocação que incluiu, sem sombra de dúvidas, o e-mail) ou telemática (telefonia + informática) constitui crime.

Percebemos aqui a necessidade de Dolo (intenção) para a consumação do fato típico, o que nos dá margem a dizer que a pessoa que recebe por engano um e-mail dirigido à pessoa outra que não ela, não responde pelo crime descrito na Lei 9.296/96.

Agora temos outra situação complicadora: interceptar não tem necessariamente o sentido de devassar, conhecer, violar o sigilo de, mas o sentido de impedir, deter, conter, cortar a passagem, interromper o curso. Com isso chegamos divergência doutrinária de que, nos crimes de "interceptação" de e-mail (ou seja, ter acesso a uma mensagem antes ou no mesmo momento de seu destinatário final), ocorreria o crime previsto na Lei 9.296/96. Existiria, para alguns estudiosos, uma lacuna jurídica ao se acessar um e-mail após a leitura pelo destinatário.

Portanto, se o destinatário já leu o e-mail, mas o manteve em sua conta no provedor, a leitura por um terceiro não será configurada crime. Eis a falha atual do nosso sistema jurídico. Mas tal posição é passível de inúmeras discussões doutrinárias, e só a união de leis, doutrina e jurisprudência poderão sedimentar o melhor entendimento neste aspecto da interceptação." [27]

2.9 Divulgação de Segredo

Código Penal - Artigo 153. Divulgar alguém sem justa causa, conteúdo de documento particular ou de correspondência confidencial, de que é destinatário ou detentor, e cuja divulgação possa produzir dano a outrem:

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

Parágrafo 1ºA Divulgar, sem justa causa, informações sigilosas ou reservadas, assim definidas em lei, contidas ou não nos sistemas de informações ou banco de dados da Administração Pública:

---

27 - NOGUEIRA, Fernando Célio de Brito. **Violação de e-mail é crime?**. Disponível em: <www.ibccrim.org.br>. Acesso em 02 dez. 2004.

Pena – detenção de 1 (um) a 4 (quatro) anos, e multa.

Parágrafo 1º Somente se procede mediante representação.

Parágrafo 2º Quando resultar prejuízo para a Administração Pública, a ação penal será incondicionada.

Conforme reza o artigo acima, pode dividir este crime em duas modalidades: uma delas, o sujeito passivo, ou seja, “o dono do segredo” pode ser qualquer pessoa; já na segunda modalidade, a vítima será sempre a Administração Pública. Nos dois casos, pune-se a conduta de quem coleta ou capta as informações e as divulga de forma danosa.

Este crime pode ou não ser praticado por meio da informática, uma vez que o artigo prevê que as informações podem ou não estar contidas no banco de dados da Administração.

Este crime pode ser praticado apenas na modalidade dolosa, o agente deverá ter conhecimento, vontade de praticar a conduta e de provocar o resultado.

2.10 Furto

Código Penal - Artigo 155 - Subtrair, para si ou para outrem, coisa alheia móvel:

Pena - reclusão, de 1 (um) a 4 (quatro) anos, e multa.

§ 1º - A pena aumenta-se de um terço, se o crime é praticado durante o repouso noturno.

§ 2º - Se o criminoso é primário, e é de pequeno valor a coisa furtada, o juiz pode substituir a pena de reclusão pela de detenção, diminuí-la de um a dois terços, ou aplicar somente a pena de multa.

§ 3º - Equipara-se à coisa móvel a energia elétrica ou qualquer outra que tenha valor econômico.

Furto qualificado

§ 4º - A pena é de reclusão de 2 (dois) a 8 (oito) anos, e multa, se o crime é cometido:

I - com destruição ou rompimento de obstáculo à subtração da coisa;

II - com abuso de confiança, ou mediante fraude, escalada ou destreza;

III - com emprego de chave falsa;

IV - mediante concurso de duas ou mais pessoas.

§ 5º - A pena é de reclusão de 3 (três) a 8 (oito) anos, se a subtração for de veículo automotor que venha a ser transportado para outro Estado ou para o exterior.

Podemos também dividir o crime de furto em duas modalidades. Se um agente furta o computador ou um de seus acessórios, o crime será contra o sistema de informática. Exemplo: furto de um disquete. Todavia, se um indivíduo utiliza o computador para subtrair valores de uma instituição bancária, ele usa a informática como instrumento para a prática do crime. Exemplo: violação de um sistema bancário para transferência de valores.

Para a configuração do delito de furto será necessário que o objeto subtraído tenha valor econômico. Desta forma se o agente subtrai um arquivo sem valor, como por exemplo, uma foto do cachorro da família, não haverá crime.

O crime de furto privilegiado poderá ser aplicado. Exemplo de um sujeito que subtrai um disquete, ou outro acessório com valor inferior a um salário mínimo.

Com relação ao furto qualificado, nem todas as hipóteses poderão ser aplicadas. No caso do agente que subtrai arquivos confidencias que possuem valor econômico aproveitando-se de uma senha de acesso que adquiriu em razão de ser uma pessoa de confiança do lesado, o crime poderá ser qualificado por abuso de confiança.

O furto de tempo ou furto de uso do computador constitui uma conduta abusiva por parte do agente que utiliza o equipamento sem autorização de seu proprietário. O furto de uso pode ser do computador (hardware) ou de acesso desautorizado na rede (navegar na Internet), ambos os casos são previstos. (28)

Aos demais casos, não se aplica o furto qualificado.

O Crime de furto se difere do crime de Estelionato (Fraude) no seguinte aspecto: No crime de furto a ação de subtração cabe ao próprio agente. Na fraude o agente consegue obter a vantagem induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento.

---

28 - CASTRO, Carla Rodrigues Araújo de. **Crimes de Informática e seus Aspectos Processuais**. Rio de Janeiro: Lumen Juris, 2003.

2.11 Envio de Vírus e Similares

Vírus são programas de informática capazes de multiplicar-se mediante a infecção de outros programas maiores. Tentam permanecer ocultos no sistema até o momento da ação e podem introduzir-se nas máquinas de diversas formas, produzindo desde efeitos simplesmente importunos até altamente destrutivos e irreparáveis. Ao lado dos vírus existem os *Worms* e os *Trojans*.

Worms não necessitam infectar outros arquivos para se multiplicar e normalmente se espalham usando recursos da rede (o e-mail é o seu principal canal de distribuição atualmente).

Trojans ou cavalos de Tróia são programas que podem chegar por qualquer meio ao computador, no qual, após introduzidos, realizam determinadas ações com o objetivo de controlar o sistema. *Trojans* puros não têm capacidade de se auto-reproduzir ou infectar outros programas. O nome cavalo de Tróia deriva do famoso episódio de soldados gregos escondidos em um cavalo de madeira dado como presente aos troianos durante a guerra entre os dois povos. (29)

Os vírus , *trojan* e *worm* são cada vez mais comuns na Internet. Uma das formas mais simples de contaminação é através do e-mail.

Na ausência de legislação específica, é aplicável o tipo penal do dano.

Código Penal – Artigo 163. Destruir, inutilizar ou deteriorar coisa alheia:

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

---

29 - Redação Infoguerra. **O que são vírus, worms e trojans**. Disponível em: www.infoguerra.com.br. Acesso em 08 dez. 2004.

Para a configuração do crime de dano é necessário que provoque prejuízo econômico. Assim, se o agente envia um vírus e destrói dados sem importância sem causar prejuízo, não irá configurar o crime.

Em se tratando de vírus ou similar enviado para computador da União, Estado, Município, empresa concessionária de serviços públicos ou sociedade de economia mista será aplicável o dano qualificado (artigo 163, parágrafo único, III do CP). Assim como se o dano for praticado por motivo egoístico ou com prejuízo considerável para a vítima. O conceito de "prejuízo considerável" terá que ser avaliado em cada caso concreto, levando-se em consideração o patrimônio da vítima.

Não se confunde o crime de dano com o ato pelo qual o agente entra em uma *homepage* e lá deixa mensagens "pichando" a página. Embora a Lei número 9.605/98 tipifique a conduta do "pichador" ou do "grafiteiro", esta só é punível quando o ato de conspurcar é dirigido a edificações ou monumentos urbanos. Em direito penal não é admissível a interpretação extensiva para prejudicar o réu. Assim, a conduta de pichar um *homepage* ainda não é tipificada pela nossa legislação. (30)

2.12 Apropriação Indébita

Para a configuração deste delito é necessário que o agente tenha a posse legítima do bem alheio e, após, passa possuí-la como coisa própria.

Um exemplo a ser citado é no caso de um funcionário receber um computador e uma impressora para uso em sua função de trabalho. Passado algum tempo, este

---

30 - CASTRO, Carla Rodrigues Araújo de. **Crimes de Informática e seus Aspectos Processuais**. Rio de Janeiro: Lumen Juris, 2003.

mesmo funcionário leva esses equipamentos para casa e passa utilizá-los sem a pretensão de devolvê-los. Neste exemplo o agente possuía o bem em nome da empresa e em seguida passa a possuí-lo como sendo seu.

Código Penal - Artigo 168. Apropriar-se de coisa alheia móvel, de que tem a posse ou a detenção:

Pena - reclusão, de 1 (um) a 4 (quatro) anos, e multa.

§ 1º - A pena é aumentada de um terço, quando o agente recebeu a coisa:

I - em depósito necessário;

II - na qualidade de tutor, curador, síndico, liquidatário, inventariante, testamenteiro ou depositário judicial;

III - em razão de ofício, emprego ou profissão.

2.13 Estelionato

Código Penal - Artigo 171. Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento:

Pena - reclusão, de 1 (um) a 5 (cinco) anos, e multa.

O crime de estelionato pressupõe dois resultados: vantagem ilícita e prejuízo alheio [31]. Este resultado deve ser causado mediante artifício, ardil ou qualquer outro meio fraudulento. É exatamente aqui que entra a informática. O agente pode utilizar *homepages*, *sites*, conversas *on line* e e-mail para induzir o lesado a erro, seja mediante ardil, artifício ou qualquer meio. Na lição do mestre Paulo José da Costa Júnior, o ardil se distingue do artifício na medida em que o primeiro opera sobre a realidade externa, criando uma falsa aparência material e o último atua diretamente sobre o psiquismo do enganado. [32]

Uma das fraudes mais utilizadas atualmente, segundo o anuário da empresa de segurança informática MessageLabs, é a batizada de *phishing*. A fraude consiste em utilizar e-mails para encaminhar clientes para sites falsos, com o objetivo de extrair informações pessoais sensíveis como senhas de acesso ou número de cartões de crédito.

---

31 - DELMANTO, **Código Penal Anotado**, p. 356.
32 - Costa Júnior, **Comentário ao Código Penal**, p. 525.

Estes tipos de ataques estão se tornando mais sofisticados. Os primeiros exemplos de *phishing* levavam a vítima a visitar sites falsos. Versões mais modernas buscam roubar detalhes das vítimas logo que elas abrem os e-mails contaminados.

Shipp diz que o Brasil vem sendo vítima, de um novo tipo de golpe, utilizando cartões postais. A vítima recebe um e-mail dizendo que ela ganhou um cartão postal. Quando clica no link que a leva ao site, são instalados bugs na sua máquina que ficam adormecidos até que ela acesse detalhes bancários. A vítima é, então, fraudada. (33)

A "Cartilha de Segurança para Internet" (34) da NBSO (NIC BR Security Office) demonstra também algumas modalidades de fraudes envolvendo o comércio eletrônico e Internet Banking. A maior parte das situações apresentadas, envolvem técnicas de engenharia social, conforme abaixo:

a) O usuário recebe um e-mail, cujo remetente pode ser um suposto funcionário, gerente, ou até mesmo uma pessoa conhecida, sendo que este e-mail contém um programa anexado. A mensagem, então, solicita que o usuário execute o programa para, por exemplo, obter acesso mais rápido a um *site* de comércio eletrônico ou ter acesso a informações mais detalhadas em sua conta bancária.

- Teclas digitadas: um programa pode capturar e armazenar todas as teclas digitadas pelo usuário, em particular, aquelas digitadas logo após a entrada em um site de comércio eletrônico ou de Internet Banking. Deste modo, o

---

33 - COELHO, Rodrigo Durão. **Fraude online cresce e vira epidemia mundial.** Disponível em: <http://informatica.terra.com.br/interna/0,,OI434865-EI553,00.html**>.** Acesso em 08 dez. 2004.
34 - NBSO (NIC BR Security Office). **Cartilha de Segurança para Internet**
Parte IV: Fraudes na Internet. Disponível em: < http://www.nbso.nic.br/docs/cartilha/cartilha-04-fraudes.html#sec2>. Acesso em: 08 dez. 2004.

- programa pode armazenar e enviar informações sensíveis (como senhas de acesso ao banco ou números de cartões de crédito) para um atacante;
- Posição do cursor e tela: alguns sites de Internet Banking têm fornecido um teclado virtual, para evitar que seus usuários utilizem o teclado convencional e, assim, aumentar o nível de segurança na realização de transações bancárias via Web. O fato é que um programa pode armazenar a posição do cursor e a tela apresentada no monitor, nos momentos em que o mouse foi clicado. Estas informações permitem que um atacante, por exemplo, saiba qual foi a senha de acesso ao banco utilizada pelo usuário;
- Webcam: um programa pode controlar a Webcam do usuário, direcionando-a para o teclado, no momento em que o usuário estiver acessando um site de comércio eletrônico ou de Internet Banking. Deste modo, as imagens coletadas (incluindo aquelas que contém a digitação de senhas ou número de cartões de crédito) podem ser enviadas para um atacante.

b) Outra situação seria a do atacante que compromete o servidor de nomes do provedor do usuário, de modo que todos os acessos a um *site* de comércio eletrônico ou Internet Banking são redirecionados para uma página Web falsificada, semelhante ao site verdadeiro. Neste caso, um atacante pode monitorar todas as ações do usuário, incluindo, por exemplo, a digitação de sua senha bancária ou do número de seu cartão de crédito. É importante ressaltar que nesta situação normalmente o usuário deve aceitar um novo certificado (que não corresponde ao site verdadeiro) e o endereço mostrado no browser do usuário poderá ser diferente do endereço correspondente ao site verdadeiro;

c) Além das situações citadas, existe também a possibilidade do usuário ser persuadido a acessar um site de comércio eletrônico ou de Internet Banking, através de um link recebido por e-mail ou em uma página de terceiros. Este link pode direcionar o usuário para uma página Web falsificada, semelhante ao site que o usuário realmente deseja acessar. A partir daí, um atacante pode monitorar todas as ações do usuário, incluindo, por exemplo, a digitação de sua senha bancária ou do número de seu cartão de crédito. Também é importante ressaltar que nesta situação normalmente o usuário deve aceitar um novo certificado (que não corresponde ao site verdadeiro) e o endereço mostrado no browser do usuário será diferente do endereço correspondente ao site verdadeiro;

d) Por fim, o usuário, ao utilizar computadores de terceiros para acessar sites de comércio eletrônico ou de Internet Banking, pode ter todas as suas ações monitoradas (incluindo a digitação de senhas ou número de cartões de crédito), através de programas especificamente projetados para este fim.

2.14 Violação de Direito Autoral

Código Penal - Artigo 184. Violar direito autoral:

Pena - detenção, de 3 (três) meses a 1 (um) ano, ou multa.

§ 1º - Se a violação consistir em reprodução, por qualquer meio, com intuito de lucro, de obra intelectual, no todo ou em parte, sem a autorização expressa do autor ou de quem o represente, ou consistir na reprodução de fonograma ou videofonograma, sem autorização do produtor ou de quem o represente:

Pena - reclusão, de 1 (um) a 4 (quatro) anos, e multa, de Cr$ 10.000,00 (dez mil cruzeiros) a Cr$ 50.000,00 (cinqüenta mil cruzeiros).

§ 2º - Na mesma pena do parágrafo anterior incorre quem vende, expõe à venda, aluga, introduz no País, adquire, oculta, empresta, troca ou tem em depósito, com intuito de lucro, original ou cópia de obra intelectual, fonograma ou videofonograma, produzidos ou reproduzidos com violação de direito autoral.

§ 3º - Em caso de condenação, ao prolatar a sentença, o juiz determinará a destruição da produção ou reprodução criminosa.

O crime de Violação de Direito Autoral é de múltipla ação, o agente pode praticá-lo de inúmeras formas, por exemplo, reproduzir, expor à venda, vender, trocar ou copiar a obra com violação do direito do autor. Na Internet é muito comum reproduzir

músicas e livros sem autorização do autor e sem que lhe sejam repassados os valores devidos. (35)

Vale citar que este artigo não se aplica aos programas de computadores, em face da existência de lei específica sobre o assunto (Lei nº 9.609/98).

2.15 Escárnio por Motivo de Religião

Código Penal - Artigo 208. Escarnecer de alguém publicamente, por motivo de crença ou função religiosa; impedir ou perturbar cerimônia ou prática de culto religioso; vilipendiar publicamente ato ou objeto de culto religioso:

Pena - detenção, de 1 (um) mês a 1 (um) ano, ou multa.

Parágrafo único - Se há emprego de violência, a pena é aumentada de um terço, sem prejuízo da correspondente à violência.

Escarnecer nada mais é do que debochar, zombar. O sujeito ativo que zomba de outra pessoa em razão de sua função ou crença religiosa responderá por este crime. Para caracterização do crime, ele deverá ser praticado publicamente, portanto, é possível sua prática em salas de bate-papo, *homepages* e *sites*. Esta prática quando feita por e-mail direcionado a apenas uma pessoa não caracterizará o crime, visto que o ato não se tornou público.

---

35 - CASTRO, Carla Rodrigues Araújo de. **Crimes de Informática e seus Aspectos Processuais**. Rio de Janeiro: Lumen Juris, 2003.

2.16 Favorecimento da Prostituição

Código Penal - Artigo 228. Induzir ou atrair alguém à prostituição, facilitá-la ou impedir que alguém a abandone:

Pena - reclusão, de 2 (dois) a 5 (cinco) anos.

§ 1º - Se ocorre qualquer das hipóteses do § 1º do artigo anterior:

Pena - reclusão, de 3 (três) a 8 (oito) anos.

§ 2º - Se o crime, é cometido com emprego de violência, grave ameaça ou fraude:

Pena - reclusão, de 4 (quatro) a 10 (dez) anos, além da pena correspondente à violência.

§ 3º - Se o crime é cometido com o fim de lucro, aplica-se também multa.

A prostituição é o comércio do corpo, podendo ocorrer em ambos os sexos. A prostituição por si só não constitui crime. A conduta de quem se aproveita ou de alguma forma favorece a prostituição é que constitui.

O código penal apresenta três condutas para o favorecimento: induzir ou atrair, facilitar ou impedir que alguém abandone. Todas as condutas apresentadas podem ser praticadas pela Internet, exceto a conduta de impedir o abandono. Segundo o Professor CELSO DELMANTO, em citação jurisprudencial induzir é persuadir, aliciar ou levar, enquanto facilitar é tornar mais fácil o comércio da prostituta (TJSP, RT 532/328).[36]

---

36 - DELMANTO, Celso. **Código Penal Comentado**. São Paulo: Renovar, 1991.

Qualquer ato tendente a tornar mais fácil o comércio carnal, o que é possível através de *sites* que oferecem nomes, telefones, valores e locais de encontros configura o crime de favorecimento da prostituição.

2.17 Pedofilia

O estatuto da criança e do adolescente, Lei 8.069/90, cuida dos direitos das crianças e dos adolescentes. Criança para o estatuto é a pessoa até doze anos de idade incompletos e adolescente aquela entre doze e dezoito anos (artigo 2º da Lei número 8069/90).

Lei 8069/90 – Artigo 241. Fotografar ou publicar cena de sexo explícito ou pornografia envolvendo criança ou adolescente:

Pena – reclusão de um a quatro anos.

É inaceitável o constrangimento ao qual as crianças e adolescentes são submetidos para saciar o prazer doentio e repugnante destes criminosos. A pedofilia tira da criança o que ela tem de mais valioso, sua inocência, sua infância, e o faz de forma brutal, não lhe permite qualquer possibilidade de defesa. Age o agressor contra aqueles que não concebem a extensão da agressão que estão sofrendo e suas incomensuráveis cicatrizes. Que postura a sociedade adotará para enfrentar esta onda de crimes que violentam tão fortemente a infância e a adolescência?

Publicar é tornar público, divulgar. Quem insere fotos de crianças ou adolescentes

em cena de sexo na Internet está publicando e, assim, cometendo a infração. O crime pode ser praticado através de *sites* e *homepages*. A simples publicidade das fotos já configura o crime. Não importa o número de pessoas que tiveram acesso a elas. Quem envia um e-mail para uma pessoa determinada, com uma foto anexada não esta tornando publico o ato, assim, não há conduta atípica. (37)

Há quem defenda a necessidade da identificação da criança ou adolescente para a configuração do crime, porém, a Lei não faz esta requisição.

Como pudemos observar, as condutas punidas são as de fotografar ou publicar, desta forma, se alguém acessa uma página não esta sujeito à punição.

2.18 Interceptação de Comunicações

Lei número 9296/96 – Antigo 10º. Constitui crime realizar interceptação de comunicação telefônica, de informática ou telemática, ou quebrar segredo fr Justiça, sem autorização judicial ou com objetivos não autorizados em lei.

Pena – reclusão, de 2(dois) a 4(quatro) anos, e multa.

Interceptar é captar, conhecer o conteúdo da comunicação. Nossa lei protege a privacidade das comunicações, constituindo crime a conduta que viola o sigilo. Há necessidade de dolo para a configuração do crime. Neste caso se engloba o sigilo das conversas *on line*, transferência de arquivos entre outros.

---

37 - CASTRO, Carla Rodrigues Araújo de. **Crimes de Informática e seus Aspectos Processuais**. Rio de Janeiro: Lumen Juris, 2003.

2.19 Pirataria de software (38)

Segundo DEANA WEIKERSHEIMER, desde a implantação da política de informática no país, na década de 80, o grande problema visualizado para incremento do segmento na área de prestação de serviços - aí incluídos o desenvolvimento e a comercialização de software, nacional e estrangeiro - sempre foi a forma de proteger a novidade ali contida, evitando que a mesma fosse ilicitamente copiada por terceiros, em detrimento dos direitos dos reais detentores da tecnologia.

Assim, ao se definir a natureza jurídica de software, com a promulgação da lei nº 7646/87 e de seu decreto regulamentador nº 96.036/98, o legislador estabeleceu que o mesmo é obra protegida pelo direito autoral, definindo no próprio texto legal as sanções pela violação de direitos daí decorrentes.

A medida legal existente não evitou a ocorrência da prática do ilícito, de forma bastante corriqueira, principalmente no tocante à multiplicação das licenças sem a pertinente autorização do seu titular, determinando a proposição de algumas ações de indenização, que em face da morosidade da nossa justiça, não encontraram o amparo esperado na solução da pendência.

A legislação de regência foi revogada e substituída pela lei nº 9609/98, que referendou a natureza jurídica do software de direito autoral, fato este consignado de forma inconteste na lei nº 9610/98, que dispõe sobre a proteção aos direitos autorais, uma vez que ali se encontra expressamente previsto no seu art.7º e respectivo parágrafo primeiro tal conceito jurídico.

---

38 – WEIKERSHEIMER, Deana. **Pirataria de Software**. Disponível em: < http://www.modulo.com.br/pt/page_i.jsp?page=3&catid=2&objid=167&pagenumber=1&idiom=0>. Acesso em 15 dez. 2004.

Tal assertiva elimina definitivamente, eventuais dúvidas quanto a forma de proteção do software, garantindo ao titular a prerrogativa de exigir ressarcimento efetivo pela ocorrência da prática de ilícito em relação ao bem que desenvolveu.

Paralelamente à promulgação da legislação vigente, verificou-se, também, o aparecimento da Internet, expandindo de modo avassalador o uso do computador e o licenciamento de ferramentas (software) para dar amparo aos anseios de usuários e internautas que buscam este novo modelo para movimentar seus negócios.

Esta evolução vem determinando outras formas de prática de pirataria, que devem ser ilididas de modo contundente, posto que a sua perpetuação tem trazido um prejuízo incalculável às empresas que destinam forma substancial de investimento para a descoberta de soluções inteligentes, em detrimento daquelas que se aproveitam da criação intelectual disponível para tirar vantagem comercial rápida, praticando de forma efetiva a concorrência desleal.

Toda a movimentação que se tem conhecimento até agora não surtiu os efeitos desejados, uma vez que a solução esbarra, na maioria das vezes em medidas judiciais, que são demoradas e custosas, além do que, os parcos resultados havidos, em sentenças transitadas em julgado, determinam como indenização pelo ilícito, quantias insignificantes que encorajam ainda mais a perpetuação da prática delituosa.

3 COMBATE E PREVENÇÃO AOS CRIMES DE INFORMÁTICA

Existem diversas maneiras de combate e prevenção aos crimes de informática.

Combate é a aplicação direta de métodos que eliminem a criminalidade. A prevenção consiste em evitar que o crime ocorra, realizando ações tendentes a interpor obstáculos no caminho da delinqüência, visto que inexiste forma de garantir 100% a ocorrência destes delitos. Além das leis, que não são diretamente formas de prevenção, porém, métodos de intimidação e punição, existe a tecnologia com seus diversos controles de segurança que podem ser empregados com esta finalidade.

3.1 Cooperação policial internacional no combate aos crimes de informática

O mundo está se convencendo de que a cooperação policial internacional para o combate aos crimes de informática, por meio da adoção de mecanismos céleres, é imprescindível para se levar a bom termo a persecução criminal dessa nova modalidade de ilícitos. (39)

As características dos crimes de informática que dificultam seu combate são os fatos de não existem fronteiras em sua consecução e de que as suas evidências podem

---

39 - SILVA, Paulo Quintiliano da. **Cooperação policial internacional no combate aos crimes cibernéticos**. Disponível em: <http://www.modulo.com.br>. Acesso em 16 dez. 2004.

se perder definitivamente em pouco tempo. Assim, a mesma ação criminosa pode ter efeito em vários países, de forma simultânea, podendo atingir até milhões de pessoas, como é o caso da disseminação de programas maliciosos. As evidências que poderiam permitir a identificação e a localização dos autores desses crimes podem se perder em pouco tempo.

Dadas as características dessa ação criminosa, em que muitas vezes as suas provas são perdidas definitivamente em poucos meses ou em poucas semanas, para o combate efetivo é necessária a cooperação internacional entre os agentes públicos encarregados desta missão, que deve ser feita por meio de grupos organizados e estruturados em cada um dos países, objetivando adotar imediatamente todas as medidas necessárias, sem burocracias. (40)

Dessa forma, em se tratando de crimes de informática, é imprescindível que as ações sejam tomadas de forma extremamente rápida, pois, de outra forma, poderia perder definitivamente todas as evidências, impossibilitando o trabalho da investigação policial.

De acordo com o Serviço de Perícias em Informática (SEPINF) do Departamento de Polícia Federal em investigações de crimes cibernéticos com efeitos em mais de um país, pode-se constatar que, na grande maioria das vezes, tornam-se inócuos todos os esforços empreendidos pelos policiais, em decorrência da morosidade e, às vezes, da impossibilidade de se conseguirem informações armazenadas em Provedores de Serviços de Internet localizados em outros países.

Nos procedimentos normais, são necessárias Cartas Rogatórias para se possibilitar o afastamento dos sigilos telemáticos e a obtenção dos dados das pessoas

---

40 - SILVA, Paulo Quintiliano da. **Cooperação policial internacional no combate aos crimes cibernéticos**. Disponível em: <http://www.modulo.com.br>. Acesso em 16 dez. 2004.

investigadas junto aos Provedores de Serviços de Internet localizados no exterior. Devido à grande morosidade desses procedimentos, quando eles são concluídos os Provedores de Serviços de Internet responsáveis pela guarda dos dados já liberaram as mídias magnéticas que continham dos dados de interesse, tendo as evidências sido perdidas definitivamente.

Sabe-se que grande parte dos Provedores de Serviços de Internet mantém as suas cópias com os “logs” dos acessos e demais evidências por, no máximo, 90 (noventa) dias e às vezes por período ainda menor, visto que ainda não existem leis que regulamentam as atividades dos Provedores de Serviços de Internet, obrigando-os a preservarem os dados por mais tempo. (41)

Considerando-se a atual forma de trabalho, com a necessidade de Cartas Rogatórias e demais procedimentos, este prazo acaba não sendo suficiente, o que inviabiliza todo o trabalho de investigação.

3.1.1 Proposta brasileira de cooperação policial internacional

Existe uma proposta brasileira (projeto de cooperação policial internacional na “V Reunião de Ministros da Justiça das Américas (REMJA V)” da Organização dos Estados Americanos (OEA), realizada em Washington, DC, de 28 a 30 de abril de 2004) que consiste no estabelecimento de cooperação hemisférica, por meio da adoção de mecanismos ágeis no combate aos delitos cibernéticos, especialmente aos que têm repercussão internacional. Os mecanismos propostos procuram evitar, sempre que possível, todos os procedimentos burocráticos e morosos, incompatíveis

---

41 - SILVA, Paulo Quintiliano da. **Cooperação policial internacional no combate aos crimes cibernéticos**. Disponível em: < http://www.modulo.com.br >. Acesso em 16 dez. 2004.

com a velocidade que experimentam os crimes de informática e com a agilidade dos criminosos do espaço cibernético. (42)

A cooperação internacional para o combate aos crimes de informática, proposta pelo Brasil, tem como pressuposto a existência de Grupos Técnicos formados por policiais especializados na investigação desses crimes, estruturados e organizados em cada um dos países participantes.

Esta cooperação pode e deve se estender aos demais países não membros da OEA, de forma que se torne universal e possa alcançar todas as localidades conectadas na Internet.

Sabe-se da existência da "Rede de Emergência 24 horas/7dias", organizada e administrada pelo G8, da qual o Brasil é membro, sendo que o ponto de contato brasileiro é o Serviço de Perícias em Informática (SEPINF) da Polícia Federal. Esta Rede, também conhecida como "G8 24/7 *Computer Crime Networ*k", já possui pontos de contatos e está estruturada em diversos países, e pode e deve ser utilizada na implantação da proposta, com as devidas estruturações e adequações em alguns de seus pontos de contatos, quando for o caso.

A proposta de cooperação considera duas vertentes distintas: inversão da persecução penal e fornecimento de evidências para serem utilizadas em processos penais de outros países.

a) Inversão da persecução penal

Esta vertente se aplica nos casos em que indivíduos residentes no país A, agindo dentro do território de seu próprio país, cometem crimes que surtem efeitos no país B, e em outros.

---

42 - SILVA, Paulo Quintiliano da. **Cooperação policial internacional no combate aos crimes cibernéticos**. Disponível em: <http://www.modulo.com.br>. Acesso em 16 dez. 2004.

Neste caso, o país onde reside os criminosos cibernéticos se torna o responsável por toda a persecução penal, com base no pedido de cooperação e nas evidências recebidas do exterior.

b) Fornecimento de evidências para outros países

Esta vertente se aplica nos casos em que indivíduos residentes no país A, agindo dentro do território de seu país, cometem crimes que surtem efeito dentro de seu próprio país, mas as evidências comprobatórias da ocorrência dos crimes estão armazenadas em computadores localizados no país B, e em outros.

Os crimes cibernéticos estão experimentando um grande crescimento nos últimos anos. Se tais atividades criminosas não forem combatidas com o devido vigor, pode haver grande prejuízo nas atividades sérias que vêm sendo conduzidas por meio do espaço cibernético, tanto as atividades governamentais, como as comerciais e as científicas. (43)

Nos casos em que as atividades criminosas ultrapassam as fronteiras do país, é imprescindível que haja a cooperação internacional, por meio dos grupos de cooperação, de modo a ser possível enfrentarmos com eficácia essa nova face do crime que o século XXI nos apresenta.

Em se tratando de crimes de informática praticados a partir de ou com efeitos em vários países, em grande parte das vezes, um país atuando isoladamente não consegue fazer praticamente nada em termos de investigação, visto que as evidências que poderão comprovar a autoria do crime estão armazenadas fora do país, sob proteção de sigilo. Além disso, os criminosos também residem no exterior, longe do alcance das leis e do poder coercitivo do país ofendido. Assim, para se

_____

43 - SILVA, Paulo Quintiliano da. **Cooperação policial internacional no combate aos crimes cibernéticos**. Disponível em: <http://www.modulo.com.br>. Acesso em 16 dez. 2004.

lograr êxito no combate a esses crimes, é imprescindível que haja o estabelecimento de uma cooperação internacional, de forma compromissada e célere. (44)

3.2 Prevenção à Engenharia Social

Engenharia Social é o termo utilizado para a obtenção de informações importantes de uma empresa, através de seus usuários e colaboradores. Essas informações podem ser obtidas pela ingenuidade ou confiança. Os ataques desta natureza podem ser realizados através de telefonemas, envio de mensagens por correio eletrônico, salas de bate-papo e até mesmo pessoalmente.

As empresas investem na modernização de seus parques tecnológicos, em segurança da informação, porém, acabam deixando de lado o fator humano. A engenharia social explora essa vulnerabilidade. Os ataques de engenharia social não possuem fórmula nem método definido. Eles podem ter aspectos físicos e psicológicos. No físico, exploram o local de trabalho, vasculham lixeiras, e por telefone se passam por outra pessoa. No psicológico, exploram o lado sentimental das pessoas. (45)

Para conseguir persuadir as pessoas, o Engenheiro Social utiliza artimanhas com a finalidade de explorar algumas características humanas, tais como solidariedade, Instinto de sobrevivência, ambição, curiosidade e confiança, exercendo a influência acima de tudo, enganando muitas vezes, misturando pequenas mentiras em grandes verdades. O objetivo do Engenheiro Social é alcançado após conquistar a confiança do usuário. (46)

---

44 - SILVA, Paulo Quintiliano da. **Cooperação policial internacional no combate aos crimes cibernéticos**. Disponível em: <http://www.modulo.com.br>. Acesso em 16 dez. 2004.
45 - BRIGNOLI, Juliano Tonizetti e POPPER, Marcos Antonio. **ENGENHARIA SOCIAL**: Um perigo eminente. Disponível em: <http://www.modulo.com.br>. Acesso em 16 dez. 2004.
46 - SANTOS, Rafael Cardoso dos. **Engenharia social:** atacando o elo mais fraco – parte 1. Disponível em: < http://www.modulo.com.br/ >. Acesso em 16 dez. 2004.

Segundo RAFAEL CARDOSO DOS SANTOS, a Segurança da Informação é sempre associada a uma corrente e a escolha do elo mais fraco desta corrente é uma unanimidade: o usuário. Para conseguir mitigar o risco da Engenharia Social é necessário combatê-la como ameaça grave, fortalecendo o elo mais fraco. (47)

Para alcançar o objetivo de fortalecimento deste elo, podemos recorrer a ISO/IEC 17799:2000. Em suas primeiras páginas são encontradas dicas importantíssimas que se forem seguidas fortalecerão as empresas no combate à Engenharia Social. Vejamos então os controles considerados essenciais:

- Proteção de dados e privacidade de informações pessoais;
- Salvaguarda de registros organizacionais;
- Direitos de propriedade intelectual;
- Política de Segurança da Informação;
- Definição de Responsabilidades;
- Educação e Treinamento em Segurança da Informação;
- Relatório dos incidentes de segurança;
- Gestão da Continuidade do Negócio;
- Comprometimento e apoio visível da alta administração;
- Divulgação eficiente da segurança para todos os funcionários;
- Distribuição das diretrizes sobre as normas e política de segurança da informação para todos os funcionários e parceiros;
- Proporcionar educação e treinamento adequados.

Observando as diretrizes apontadas, podemos ter uma boa noção de como fortalecer o elo mais fraco: através da arte da conscientização. Conscientizar é criar

---

47 - SANTOS, Rafael Cardoso dos. **Engenharia social:** fortalecendo o elo mais fraco – parte 2. Disponível em: < http://www.modulo.com.br/ >. Acesso em 16 dez. 2004.

uma consciência. É ganhar a confiança do usuário a fim de fazê-lo colaborar com a segurança das informações.

Cardoso diz ainda que a melhor ferramenta de segurança é o usuário. Transformar o usuário em um agente de segurança, em um "Policial Corporativo" é um grande desafio. Desafio este que se conseguido trará bons frutos. O prêmio é um ambiente infinitamente mais seguro. Se a equipe de Segurança da Informação conseguir ganhar um funcionário de cada setor, aumentará e muito o nível de segurança da corporação. Vai conseguir multiplicar as informações de forma muito mais proveitosa e a consciência de segurança estará fazendo parte do dia-a-dia. (48)

Com base na ISO, Cardoso faz uma proposta de um modelo simples e que pode variar de corporação para corporação. Este modelo precisa de alguns requisitos fundamentais:

- Política de segurança bem definida;
- Processos críticos mapeados;
- Análise de risco concluída;
- Seleção de controles aplicada;
- Definição clara das responsabilidades.

Com estes passos concluídos é preciso expandir a equipe de segurança. Isso se iniciará quando a Política de Segurança começar a ser divulgada.

O maior objetivo do Engenheiro Social é fazer com que o usuário seja uma porta de acesso que burle todos os controles tecnológicos de segurança implementados. Passam pelo *Firewall*, enganam o IPS, não tomam conhecimento do Antivírus e tudo isso porque utilizam acessos válidos. Concedidos gentilmente pelo usuário.

---

48 - SANTOS, Rafael Cardoso dos. **Engenharia social:** fortalecendo o elo mais fraco – parte 2. Disponível em: < http://www.modulo.com.br/ >. Acesso em 16 dez. 2004.

Muitas tecnologias podem fortalecer a segurança das empresas. Hoje em dia uma ferramenta cada vez mais útil para este tipo de defesa são os filtros de conteúdo, tanto de *web* quanto de e-mail. Outra ferramenta importante é o anti-spam. Além de ferramentas computacionais, recursos como identificador de chamadas podem ajudar e muito no combate à Engenharia Social. A implementação de controles como ligação de retorno para identificar se a origem é verdadeira podem ser muito úteis.

Nenhuma delas terá o efeito esperado, caso o profissional de segurança não tenha a mais importante delas: o usuário. Por isso algumas técnicas de Engenharia Social devem ser empregadas para que o usuário mude de lado.

A Política de Segurança deve ser divulgada para todos os funcionários da empresa. Assim como o Engenheiro Social que está tentando atacar, a empresa deverá identificar os diferentes tipos de usuário, seja por personalidade, seja por função, seja por nível hierárquico. Saber com quem está lidando é fundamental para conseguir dar o recado. Transformá-lo em uma ferramenta de apoio.

A Implementação de seminários periódicos, onde sejam apresentados novos ataques, estatísticas e muita informação também será muito útil. Todo seminário deve ter sua lista de presença e um termo de compromisso. O usuário deve sair dali compromissado com a segurança das informações a que tem acesso.

Treinamentos para todos funcionários que forem contratados. Todos devem ter conhecimento de suas responsabilidades, direitos e deveres. “Se um usuário descumpriu algum ponto da Política de Segurança, mostre a ele os motivos que fizeram a empresa criar a política de segurança e os perigos a que ele e a empresa estão sujeitos com o descumprimento. Documente o incidente e se comprometa a

não levar o incidente à frente caso o funcionário se comprometa com a segurança das informações". [49]

3.3 Prevenção do SPAM

Pesquisas realizadas pela empresa Message Labs indicaram que hoje cerca de 80% dos e-mails circulados na Internet são *spam* e que isto já causa de grandes prejuízos. [50]

Alguns países (Argentina, Austrália, Coréia e outros) já têm leis contra isso, mas a maioria das nações (inclusive o Brasil) ainda não tem legislação específica para coibir essas práticas. Essas regulamentações são necessárias, pois o *spam* é atividade lucrativa para quem a pratica e é preciso estabelecer punições para aqueles que obtém vantagens financeiras com propaganda massiva quase de graça e promovem fraudes através de correio eletrônico.

Entretanto, as regulamentações não são suficientes para erradicá-los. São também necessárias melhores soluções tecnológicas para enfrentar esses desafios. Embora os procedimentos técnicos de barrar as mensagens indesejáveis não tenham sido suficientes até hoje para interromper o crescimento do problema, já existem novas soluções que, aplicadas internacionalmente, serão capazes de combatê-lo com mais eficácia.

---

49 - SANTOS, Rafael Cardoso dos. **Engenharia social:** fortalecendo o elo mais fraco – parte 2. Disponível em: < http://www.modulo.com.br/ >. Acesso em 16 dez. 2004.
50 - Faulhaber, Henrique. **O combate à praga do SPAM**. Disponível em: <http://www.modulo.com.br>. Acesso em: 16 dez. 2004.

Os criadores de "spam" se utilizam, principalmente, do anonimato na Internet. Hoje é possível fraudar facilmente a identidade do emitente de um correio eletrônico, pois não existe nenhum mecanismo automático capaz de verificar se o remetente é realmente quem alega ser.

Para resolver esta insegurança intrínseca da Internet atual foram propostos alguns esquemas, como por exemplo o sistema de identificação de e-mails CALLER ID, da Microsoft, e o Sender Policy Framework, de Meng Wong (co-fundador da Pobox.com), permitem que provedores de Internet chequem se uma mensagem enviada por joão@exemplo.com realmente foi enviada pelo endereço numérico usado pelo *site* "exemplo.com". Mensagens que não recebem essa confirmação são rejeitadas como *spam*. "O que estamos tentando fazer é dizer se um e-mail está realmente vindo de onde diz que vem", afirmou Wong.

As propostas de autenticação de e-mails têm sido divulgadas desde 1998, mas os especialistas começaram a prestar mais atenção a elas no ano passado, depois que o volume de *spam* chegou a limites inaceitáveis.

O sistema da Pobox está sendo testado pela America Online, Earthlink e outras empresas de Internet que têm seus domínios freqüentemente falsificados por *spammers*. Enquanto isso, o Yahoo apóia outra estratégia, conhecida como DomainKeys, que usa assinaturas eletrônicas para autenticar os e-mails. (51)

---

51 - REUTERS LIMITED. SPAM**: MS se une à empresa de software para combater spam**. Disponível em: <http://www.terra.com.br>. Acesso em: 17 dez. 2004.

3.4 Assinatura digital, certificado digital e criptografia

Outros elementos tecnológicos de fundamental importância dentro do campo da prevenção e combate aos crimes de informática são a assinatura digital, o certificado digital e a criptografia. Com eles, podemos implementar serviços de segurança como: autenticidade, confidencialidade, integridade, irretratabilidade e outros.

3.4.1 Assinatura Digital

A assinatura digital é uma modalidade de assinatura eletrônica, resultado de uma operação matemática que utiliza algoritmos de criptografia assimétrica e permite aferir, com segurança, a origem e a integridade do documento.

A assinatura digital fica de tal modo vinculada ao documento eletrônico "subscrito" que, ante a menor alteração neste, a assinatura se torna inválida. A técnica permite não só verificar a autoria do documento, como estabelece também uma "imutabilidade lógica" de seu conteúdo, pois qualquer alteração do documento, como por exemplo a inserção de mais um espaço entre duas palavras, invalida a assinatura. (52)

---

52 – Instituto Nacional de Tecnologia da Informação. **O que é assinatura digital**. Disponível em: <http://www.iti.br>. Acesso em 18 dez. 2004.

Necessário distinguir assinatura digital da assinatura digitalizada. A assinatura digitalizada é a reprodução da assinatura autógrafa como imagem por um equipamento tipo scanner. Ela não garante a autoria e integridade do documento eletrônico, porquanto não existe uma associação inequívoca entre o subscritor e o texto digitalizado, uma vez que ela pode ser facilmente copiada e inserida em outro documento. (53)

Através da assinatura digital podemos obter os seguintes serviços de segurança: autoria, irretratabilidade de geração, integridade, aceite e garantia de que o certificado não tenha sido revogado nos casos de assinatura com garantia de data.(54)

Entre as diversas aplicações possíveis, encontram-se as seguintes:

- comércio eletrônico;

- processos judiciais e administrativos em meio eletrônico;

- facilitar a iniciativa popular na apresentação de projetos de lei, uma vez que os cidadãos poderão assinar digitalmente sua adesão às propostas;

- assinatura da declaração de renda e outros serviços prestados pela Secretaria da Receita Federal;

- obtenção e envio de documentos cartorários;

- transações seguras entre instituições financeiras, como já vem ocorrendo desde abril de 2002, com a implantação do Sistema de Pagamentos Brasileiro - SPB;

- Diário Oficial Eletrônico;

---

53 – Instituto Nacional de Tecnologia da Informação. **O que é assinatura digital**. Disponível em: <http://www.iti.br>. Acesso em 18 dez. 2004.

54 - GUELFI, Adilson Eduardo; BERNAL, Volnys Borges. **Sistemas Criptográficos**: Assinatura Digital (1999-2003). 2004. 10 f. – Apresentação (Pós-Graduação em Segurança de Sistemas em Rede) – Faculdade Senac de Ciências Exatas e Tecnologia, Faculdades Senac, 2004.

- identificação de sítios na rede mundial de computadores, para que se tenha certeza de que se está acessando o endereço realmente desejado;

3.4.2 Certificado Digital

O certificado digital é um documento eletrônico assinado digitalmente por uma autoridade certificadora, e que contém diversos dados sobre o emissor e o seu titular. A função precípua do certificado digital é a de vincular uma pessoa ou uma entidade a uma chave pública. (55)

Quando você envia um e-mail importante, seu aplicativo de e-mail pode utilizar seu Certificado Digital para assinar "digitalmente" a mensagem. Uma assinatura digital faz duas coisas: informa ao destinatário que o e-mail é seu e indica que o e-mail não foi adulterado entre o envio e o recebimento deste.

Um Certificado Digital normalmente contém as seguintes informações: (61)

- Sua chave pública (nome e endereço de e-mail do proprietário do certificado);
- A validade da chave pública;
- O nome da empresa (a Autoridade Certificadora - CA) que emitiu seu Certificado Digital;
- O número de série do Certificado Digital;
- A assinatura digital da CA.

---

55 – Instituto Nacional de Tecnologia da Informação. **O que é certificado digital**. Disponível em: <http://www.iti.br>. Acesso em 18 dez. 2004.

3.4.3 CRIPTOGRAFIA

Criptografia é um conjunto de técnicas empregadas com a finalidade de ocultar informações. Isso ocorre em função de um conjunto de operações matemáticos que transformam um texto claro em um texto cifrado. O emissor do documento envia o texto cifrado, que será reprocessado pelo receptor, transformando-o, novamente, em texto claro, igual ao emitido. (56)

A criptografia permite a implementação de alguns serviços de segurança, como: irretratabilidade, integridade, autenticação e confidencialidade.

3.5 Prevenção de crimes nas empresas

As empresas no Brasil e no mundo tem sido vítimas de crimes como: Fraudes, Interceptação de comunicação, vírus, invasões entre outros. A prevenção destes e de outros crimes somente será necessária mediante a definição de uma política de segurança eficiente e a implementação de controles diversos que possam contribuir diretamente para a continuidade do negócio.

Há que se considerar os seguintes fatores (57):

---

56 – Instituto Nacional de Tecnologia da Informação. **O que é criptografia**. Disponível em: <http://www.iti.br>. Acesso em 18 dez. 2004.
57 - Foco Security. **Como anda a segurança da informação na sua empresa**. Disponível em: <http://www.focosecurity.com.br>. Acesso em 18 dez. 2004.

3.5.1 Análise de Risco

A Análise de Risco tem por objetivo identificar os riscos de segurança presentes na sua Empresa, fornecendo conhecimento para que sejam implementados controles eficazes de Segurança.

Fazem parte de uma Análise de Risco:

- Processos de Negócio: Identificar junto aos gestores e colaboradores os Processos de Negócio existentes na Empresa.
- Ativos: Identificar os ativos que serão considerados na Análise de Risco: Pessoas, Infra-estrutura, Aplicações, Tecnologia e informações.
- Vulnerabilidades: Identificar as vulnerabilidades existentes nos ativos que possam causar indisponibilidade dos serviços ou serem utilizadas para subtração das suas informações.
- Ameaças: Identificar os agentes que podem vir a ameaçar a Empresa.
- Impacto: Tendo identificado as vulnerabilidades e ameaças, haverá possibilidade de identificar o impacto que estes podem causar na Empresa. Como subtração de informação, paralisação de serviços, perdas financeiras entre outros.

Uma Análise de Risco bem realizada dará informações à sua Empresa para garantir a confidencialidade, disponibilidade e Integridade da suas informações.

- Confidencialidade: Garantir que apenas pessoas autorizadas tenham acesso às informações.
- Disponibilidade: Garantir que a sua Empresa tenha acesso a informação sempre que necessário.

- Integridade: Garantir que haja controle quanto a alteração das informações.

Benefícios

- Conhecimento dos riscos da Empresa;

- Otimização de recursos;

- Ter subsídios para um Plano de Ação.

3.5.2 Classificação da Informação

Um dos principais fatores para o sucesso da sua implantação é ter o conhecimento das informações que circulam na sua Empresa. Definir pode acessar, modificar ou excluir determinada informação.

Identificação e classificação das informações quanto ao nível de sensibilidade: confidencial, restrito, uso interno, pública, secreta e ultra-secreta.

Definição do grau de criticidade: alto, médio, baixo e nenhum.

Definição de políticas: armazenamento, manuseio, transporte e descarte.

3.5.3 Plano de Continuidade (Contingência)

De acordo com a Análise de Risco é possível elaborar o Plano de Continuidade para a Empresa. O objetivo é minimizar as interrupções das atividades dos colaboradores, protegendo também a perda das informações causadas por possíveis ameaças.

Deverão ser estabelecidos os seguintes planos:

-Plano de Continuidade Operacional

-Plano de Recuperação de Desastres

-Plano de Administração de Crise

-Plano para realização de Teste

O Plano de Continuidade deve ser testado periodicamente a fim de garantir que sua informação seja recuperada dentro de um tempo máximo permitido

3.5.4 Criação do Comitê Corporativo de Segurança da Informação

Já no inicio dos serviços, haverá necessidade de se estabelecer os responsáveis pelo Comitê Corporativo de Segurança da Informação.

O Comitê, basicamente, tem o objetivo de atuar com as áreas associadas, definir indicadores e metas, coordenar as medidas de segurança, avaliar os resultados, promover palestras (conscientização e manutenção da Política de Segurança), conduzir ações de auditoria e monitoramento, entre outras responsabilidades.

3.5.5 Teste de Invasão

O Teste de Invasão tem o objetivo de avaliar o grau de segurança oferecido pelos controles de segurança implementados na Empresa. Funcionando também, como um complemento à Análise de Risco, pois identifica as vulnerabilidades.

Os testes de invasão são divididos em:

a) Teste de invasão Interno: Como o próprio nome diz, é feito no ambiente interno da Empresa, levantando possíveis vulnerabilidades internas. Simulando o que seria possível realizar atuando como participante do ambiente.

Verificar falhas de segurança nas estações de trabalho, servidores, roteadores e aplicações internas entre outros.

b) Teste de Invasão Externo: Tem o objetivo de verificar o grau de segurança a tentativas externas de invasão. Visando principalmente conexões com a Internet e acesso remoto.

Em ambos os testes, haverá de se utilizar técnicas de Engenharia Social, simulando de forma real as técnicas utilizadas por pessoas que buscam coletar informações confidenciais do ambiente.

Características do relatório Teste de Invasão

- Informar detalhadamente as vulnerabilidades encontradas (Quais e como foram encontradas).
- Sugestões para correção das vulnerabilidades.

3.5.6 Campanha de Divulgação da Política de Segurança

A Campanha de Divulgação da Política de Segurança é uma das ferramentas responsáveis pelo sucesso da implantação.

Seu objetivo é divulgar a Política de Segurança da Informação na Empresa, conscientizando os colaboradores e prestadores de serviço para a Política de Segurança que está sendo implantada.

São desenvolvidas palestras de conscientização, cartas, e-mails, cartilhas e eventos objetivando o sucesso da implantação.

3.5.7 Treinamento

Como a campanha de divulgação, o treinamento também tem o objetivo de divulgar a Política de Segurança, conscientizar os colaboradores e treinar a equipe técnica. Podendo ser mais especifica de acordo com a necessidade da Empresa.

- Treinamento geral para colaboradores
- Treinamento para auditores da Empresa
- Treinamento para equipe de TI

3.5.8 Gerenciamento e Manutenção da Segurança

De nada adianta ter implantado a Política de Segurança sem garantir que esta vai realmente ser absorvida pela Empresa a longo prazo.

Na grande maioria das vezes a política de segurança tende a perder sua eficiência. Por este fator, há que se considerar o serviço de Gerenciamento e Manutenção da Segurança, onde são implementadas medidas que visam monitorar o ambiente, identificar tentativas de invasão, garantir atualização da política de segurança e disponibilidade da informação.

3.6 Dicas de prevenção para os usuários domésticos

Como forma de tentar prevenir os crimes apresentados, a NBSO oferece algumas dicas que podem ser utilizados por usuários em suas residências a fim de minimizar a possibilidade de serem vítimas dos crimes de informática, conforme abaixo [58]:

Senhas

- Elaborar sempre uma senha que contenha pelo menos oito caracteres, compostos de letras números e símbolos;
- Jamais utilizar como senha seu nome, sobrenome, números de documentos, placas de carros, números de telefones, datas que possam ser relacionadas com você ou palavras constantes em dicionários;
- Utilizar uma senha diferente para cada serviço;
- Alterar a senha com freqüência.

Vírus e cavalos de tróia

- Instalar e manter atualizado um bom programa antivírus;
- Desabilitar no seu programa de e-mail a auto-execução de arquivos anexados às mensagens;
- Não executar ou abrir arquivos recebidos por e-mail, mesmo que venham de pessoas conhecidas, mas caso seja inevitável, certifique-se que o arquivo foi verificado pelo programa antivírus;

---

58 - NBSO (NIC BR Security Office). **Cartilha de Segurança para Internet**
Parte IV: Fraudes na Internet. Disponível em: < http://www.nbso.nic.br/docs/cartilha/cartilha-04-fraudes.html#sec2>. Acesso em: 08 dez. 2004.

- Não abrir arquivos ou executar programas de procedência duvidosa ou desconhecida e mesmo que você conheça a procedência e queira abri-los ou executá-los, certifique-se que foram verificados pelo programa antivírus;
- Procurar utilizar, no caso de arquivos de dados, formatos menos suscetíveis à propagação de vírus, tais como RTF, PDF ou PS;
- Procurar não utilizar, no caso de arquivos comprimidos, o formato executável. Utilize o próprio formato compactado, como por exemplo ZIP ou GZ;
- Procurar instalar um firewall pessoal, que em alguns casos pode bloquear o recebimento de um cavalo de tróia.

Vulnerabilidades

- Manter o sistema operacional e demais softwares sempre atualizados;
- Visitar regularmente os sites dos fabricantes de software para verificar a existência de vulnerabilidades nos softwares utilizados;
- Aplicar todas as correções de segurança (patches) disponibilizadas pelo fabricante.

Worms

- Instalar e manter atualizado um bom programa antivírus;
- Manter o sistema operacional e demais softwares sempre atualizados;
- Corrigir eventuais vulnerabilidades existentes nos softwares utilizados;
- Procurar instalar um firewall pessoal, que em alguns casos pode evitar que uma vulnerabilidade existente seja explorada ou que o worm se propague.

Backdoors

- Seguir as recomendações para prevenção contra infecções por vírus;
- Não executar ou abrir arquivos recebidos por e-mail, mesmo que venham de pessoas conhecidas;
- Não executar programas de procedência duvidosa ou desconhecida;
- Procurar instalar um firewall pessoal, que em alguns casos pode evitar o acesso a um backdoor já instalado em seu computador;
- Corrigir eventuais vulnerabilidades existentes nos softwares utilizados.

Firewall

- Instalar um firewall pessoal em todos os computadores que tiverem acesso à Internet;
- Verificar os registros de eventos (logs) para identificar possíveis ataques.

E-mail

- Manter sempre a versão mais atualizada do seu programa de e-mail;
- Desligar as opções que permitem abrir ou executar automaticamente arquivos ou programas anexados às mensagens;
- Desligar as opções de execução do JavaScript, de programas Java e, se possível, o modo de visualização de e-mails no formato HTML.
- Evitar abrir arquivos ou executar programas anexados aos e-mails, sem antes verificá-los com um antivírus;
- Desconfiar de e-mails pedindo urgência na instalação de algum aplicativo ou correções de determinados defeitos dos softwares que você utilize.

Browser

- Manter o seu browser sempre atualizado;
- Desativar a execução de programas Java na configuração de seu browser, a menos que seja estritamente necessário;
- Desativar a execução de Javascripts antes de entrar em uma página desconhecida e, então, ativá-la ao sair;
- Permitir que programas ActiveX sejam executados em seu computador apenas quando vierem de sites conhecidos e confiáveis.
- Manter maior controle sobre o uso de cookies, caso você queira ter maior privacidade ao navegar na Internet;
- Certificar-se da procedência do site e da utilização de conexões seguras ao realizar transações via Web;
- Utilizar supervisor de conteúdo para as crianças e adolescentes.

Programas de Troca de Mensagens

- Manter seu programa de troca de mensagens sempre atualizado;
- Não aceitar arquivos de pessoas desconhecidas, principalmente programas de computadores;
- Evitar fornecer muita informação, principalmente a pessoas que você acabou de conhecer;
- Não fornecer, em hipótese alguma, informações sensíveis, tais como senhas ou números de cartões de crédito;
- Configurar o programa para ocultar o seu endereço IP.

Programas de Distribuição de Arquivos

- Manter seu programa de distribuição de arquivos sempre atualizado e bem configurado;
- Ter um bom antivírus instalado em seu computador mantê-lo atualizado e utilizá-lo para verificar qualquer arquivo obtido, pois eles podem conter vírus ou cavalos de tróia;
- Certificar-se que os arquivos obtidos ou distribuídos são livres, ou seja, não violam as leis de direitos autorais.

Compartilhamento de Recursos

- Ter um bom antivírus instalado em seu computador, mantê-lo atualizado e utilizá-lo para verificar qualquer arquivo ou programa compartilhado, pois eles podem conter vírus ou cavalos de tróia;
- Estabelecer senhas para os compartilhamentos, caso seja estritamente necessário compartilhar recursos do seu computador.

Cópias de Segurança

- Procurar fazer cópias regulares dos dados do computador;
- Criptografar dados sensíveis;
- Armazenar as cópias em local acondicionado, de acesso restrito e com segurança física;
- Considerar a necessidade de armazenar as cópias em um local diferente daquele onde está o computador.

Privacidade

E-mails

- Utilizar criptografia sempre que precisar enviar um e-mail com informações sensíveis;
- Certificar-se que seu programa de e-mail grava as mensagens criptografadas, para garantir a segurança das mensagens armazenadas no disco.

Cookies

- Desabilitar cookies, exceto para sites confiáveis e onde sejam realmente necessários;
- Considerar o uso de softwares que permitem controlar o envio e recebimento de informações entre o browser e o site visitado.

Privacidade na Disponibilização de Páginas Web

- Evitar colocar seus dados pessoais (e-mail, telefone, endereço, etc) em páginas Web ou blogs;
- Evitar colocar dados sobre o seu computador ou sobre os softwares que utiliza em páginas Web ou blogs;
- Evitar fornecer informações sobre o seu cotidiano (como, por exemplo, hora que saiu e voltou para casa, data de uma viagem programada, horário que foi ao caixa eletrônico, etc) em páginas Web ou blogs.

Cuidados com seus Dados Pessoais

- Procurar não fornecer seus dados pessoais (como nome, e-mail, endereço e números de documentos) para terceiros;
- Nunca fornecer informações sensíveis (como senhas e números de cartão de crédito), a menos que esteja sendo realizada uma transação (comercial ou financeira) e se tenha certeza da idoneidade da instituição que mantém o site.

Cuidados com os Dados Armazenados em um Disco Rígido

- Criptografar todos os dados sensíveis, principalmente se for um notebook;

- Sobrescrever os dados do disco rígido antes de vender ou se desfazer do seu computador usado.

Fraude

Engenharia social

- Não fornecer dados pessoais, números de cartões e senhas através de contato telefônico;
- Ficar atento a e-mails ou telefonemas solicitando informações pessoais;
- Não acessar sites ou seguir links recebidos por e-mail ou presentes em páginas sobre as quais não se saiba a procedência;
- Sempre que houver dúvida sobre a real identidade do autor de uma mensagem ou ligação telefônica, entrar em contato com a instituição, provedor ou empresa para verificar a veracidade dos fatos.

Cuidados ao realizar transações bancárias ou comerciais

- Seguir todas as recomendações sobre utilização do browser de maneira segura;
- Estar atento e prevenir-se dos ataques de engenharia social;
- Realizar transações somente em sites de instituições que você considere confiáveis;
- Certificar-se de que o endereço apresentado em seu browser corresponde ao site que você realmente quer acessar, antes de realizar qualquer ação;
- Antes de aceitar um novo certificado, verificar junto à instituição que mantém o site sobre sua emissão e quais são os dados nele contidos;
- Procurar sempre digitar em seu browser o endereço desejado. Não utilize links em páginas de terceiros ou recebidos por e-mail;

- Certificar-se que o site faz uso de conexão segura, ou seja, que os dados transmitidos entre seu browser e o site serão criptografados e utiliza um tamanho de chave considerado seguro;
- Verificar o certificado do site, para assegurar-se que ele foi emitido para a instituição que se deseja acessar e está dentro do prazo de validade;
- Não acessar sites de comércio eletrônico ou Internet Banking através de computadores de terceiros;
- Desligar sua webcam (caso vecê possua alguma), ao acessar um site de comércio eletrônico ou Internet banking.

Boatos

- Verificar sempre a procedência da mensagem e se o fato sendo descrito é verídico;
- Verificar em sites especializados e em publicações da área se o e-mail recebido já não está catalogado como um boato.

Banda Larga e Redes Sem Fio

Proteção de um computador utilizando banda larga

- Instalar um firewall pessoal e ficar atento aos registros de eventos (logs) gerados por este programa;
- Instalar um bom antivírus e atualizá-lo freqüentemente;
- Manter o seu software (sistema operacional, programas que utiliza, etc) sempre atualizado e com as últimas correções aplicadas;
- Desligar o compartilhamento de disco, impressora, etc;
- Mudar a senha padrão do seu equipamento de banda larga (modem ADSL, por exemplo) pois as senhas destes equipamentos podem ser facilmente

encontradas na Internet com uma simples busca. Esse fato é de conhecimento dos atacantes e bastante abusado.

Proteção de uma rede utilizando banda larga

- Instalar um firewall separando a rede interna da Internet;
- Caso seja instalado algum tipo de proxy (como AnalogX, wingate, WinProxy, etc) configurá-lo para que apenas aceite requisições partindo da rede interna;
- Caso seja necessário compartilhar recursos como disco ou impressora entre máquinas da rede interna, devem-se tomar os devidos cuidados para que o firewall não permita que este compartilhamento seja visível pela Internet.

Cuidados com um cliente de rede sem fio (wireless)

- Possuir um firewall pessoal;
- Possuir um antivírus instalado e atualizado;
- Aplicar as últimas correções em seus softwares (sistema operacional, programas que utiliza, etc);
- Desligar compartilhamento de disco, impressora, etc;
- Desabilitar o modo ad-hoc. Utilize esse modo apenas se for absolutamente necessário e desligue-o assim que não precisar mais;
- Usar WEP (Wired Equivalent Privacy) sempre que possível;
- Considerar o uso de criptografia nas aplicações, como por exemplo o uso de PGP para o envio de e-mails, SSH para conexões remotas ou ainda o uso de VPNs;
- Habilitar a rede wireless somente quando for usá-la e desabilitá-la após o uso.

Cuidados com uma rede sem fio doméstica

- Mudar configurações padrão que acompanham o seu AP;

- Usar sempre que possível WEP (Wired Equivalent Privacy);
- Trocar as chaves WEP que acompanham a configuração padrão do equipamento. Procure usar o maior tamanho de chave possível (128 bits);
- Desligar seu AP quando não estiver usando sua rede.

SPAM

- Considerar a utilização de um software de filtragem de e-mails;
- Verificar com seu provedor ou com o administrador da rede se é utilizado algum software de filtragem no servidor de e-mails;
- Evitar responder a um SPAM ou enviar um e-mail solicitando a remoção da lista.

Incidentes de Segurança e Uso Abusivo da Rede

Registros de eventos (logs)

- Verificar sempre os logs do firewall pessoal e de IDSs que estejam instalados no computador;
- Verificar se não é um falso positivo, antes de notificar um incidente.

Notificações de incidentes

- Incluir logs completos (com data, horário, timezone, endereço IP de origem, portas envolvidas, protocolo utilizado, etc) e qualquer outra informação que tenha feito parte da identificação do incidente;
- Enviar a notificação para os contatos da rede e para os grupos de segurança das redes envolvidas.

4 CONCLUSÃO

Os meios informáticos, sobretudo a Internet, possibilitam a prática de diversos crimes. O avanço tecnológico tem proporcionado o incremento dos crimes comuns bem como o surgimento de novas condutas ainda não tipificadas no ordenamento jurídico, de tal forma que podemos afirmar, sem sombra de dúvida, que os delitos virtuais crescem na proporção do avanço da tecnologia.

As condutas praticadas que não possuem tipificação legal (exemplo: violação de e-mail) podem ficar impunes, uma vez que a legislação brasileira não admite a aplicação extensiva da lei para prejudicar o réu, apenas para benefício.

O sentimento de anonimato, a impunidade e o alcance global dos meios de comunicação, principalmente na Internet, que sabemos se tornou um mundo sem fronteiras, fazem com que o número de infratores dessa natureza cresça, não obstante a constante preocupação em prevenir e combater tais condutas.

As estatísticas revelam que o Brasil tem sido um grande paraíso para aqueles que utilizam os meios informáticos para a prática de crimes, pois apesar de haver previsão legal para muitos dos crimes de informática, ainda existem grandes dificuldades no esclarecimento.

No campo do combate e prevenção, não podemos deixar de ressaltar a grande importância de se estabelecer acordos de colaboração entre as polícias mundiais no intuito de investigar com maior celeridade os crimes cometidos, visto que alguns crimes atravessam fronteiras de muitos países. A falta de colaboração neste sentido

aumenta ainda mais a sensação de impunidade, trazendo tranqüilidade para os criminosos que se utilizam deste meio.

O Brasil emitiu uma proposta neste sentido (projeto de cooperação policial internacional na “V Reunião de Ministros da Justiça das Américas (REMJA V)” da Organização dos Estados Americanos (OEA), realizada em Washington, DC, de 28 a 30 de abril de 2004), que consiste no estabelecimento de cooperação hemisférica, por meio da adoção de mecanismos ágeis no combate aos delitos cibernéticos, especialmente aos que têm repercussão internacional. Os mecanismos têm por objetivo evitar, sempre que possível, os procedimentos burocráticos e morosos, incompatíveis com a velocidade com que ocorrem os crimes de informática.

A prevenção à engenharia social também é uma grande aliada no combate ao crime de informática, visto que muitas empresas investem milhões em ferramentas tecnológicas e controles de segurança, mas acabam se esquecendo do elo mais fraco da relação, os usuários. Para conseguir reduzir o risco da Engenharia Social é necessário combatê-la como ameaça grave, fortalecendo este elo.

Há que se pensar também no combate a praga dos SPAMS, visto que tem sido a causa de grandes prejuízos no mundo todo. Alguns criminosos estão praticando fraudes através de correio eletrônico para obtenção vantagens financeiras (exemplo: phishing). Existem algumas tentativas de se minimizar este problema, como o sistema de identificação de e-mails CALLER ID, da Microsoft, e o Sender Policy Framework, de Meng Wong, porém, jamais darão uma solução definitiva à questão.

A utilização de assinatura digital, de certificados digitais e da criptografia é de grande valor na prevenção e combate aos crimes de informática. Hoje em dia muitas operações bancárias e de e-commerce utilizam estes recursos e tornam as transações muito seguras, evitando assim a prática de fraudes e de outros crimes.

Para a prevenção de crimes nas empresas, há que se considerar o estabelecimento de uma política de segurança séria, bem como a implementação de controles rigorosos que ao mesmo tempo não venham causar impactos e atravancar as atividades dos colaboradores.

Acredito que os crimes de informática, assim como os crimes comuns, são um reflexo do momento político e social que o Brasil e o mundo estão vivendo.

A época de desemprego, desigualdade social, falta de oportunidades e perspectivas com o futuro fazem com que a prática de crimes aumente, como justificativa de busca de uma vida melhor.

A prática de crimes de informática trouxe à criminalidade uma massa de pessoas que em outros meios talvez não fossem capazes de atuarem. A sensação de estar anônimo e impune faz com que muitas pessoas utilizem-se deste meio para obtenção de vantagens que podem não estar diretamente ligados ao mesmo instinto para a prática de crimes no mundo físico.

O surgimento da Internet trouxe uma facilidade muito grande de acesso e disseminação das informações, criação de empregos diretos e indiretos em todo o mundo, o que sem dúvida nenhuma foi uma grande vitória social e tecnológica, mas com ela também um mundo obscuro de criminalidade diversa que ao meu ver foi apenas uma expansão do mundo real.

5 REFERÊNCIAS BIBLIOGRÁFICAS

CASTRO, Carla Rodrigues Araújo de. **Crimes de Informática e seus Aspectos Processuais**. Rio de Janeiro: Lumen Juris, 2003.

BRASIL, Ângela Bittencourt. **Crimes de Computador**. Disponível em: <www.ciberlex.adv.com>. Acesso em: 20 nov. 2004.

MIRANDA, Marcelo Baeta. **Uma abordagem dinâmica aos crimes via Internet. direitos difusos, instrumentalidade e antecipação prática. Prevenção e Reprresão. Iniciativas no Brasil e principiologia**. Disponível em: <www.jusnavegandi.com.br>. Acesso em: 20 nov. 2004.

RODRIGUES, Miguel Ángel Davara. **Crime Informático**. Disponível em: <www.jusnavegandi.com.br>. Acesso em 23 nov. 2004.

MARTINELLI, João Paulo Orsini. **Aspectos relevantes da Criminalidade na Internet.** Disponível em: <www.jusnavegandi.com.br>. Acesso em 23 nov. 2004.

MACHADO, Eduardo de Paula. **Novas Fronteiras da Criminalidade:** Os crimes Tecnológicos, in Boletim IBCCrim, nº81, ano 7, agosto de 1999.

BRITO, Eduado Valadares de. **Crimes na Internet.** Disponível em: <www.infojus.com.br>. Acesso em 23 nov. 2004.

CORREIA, Gustavo Testa. **Aspectos Jurídicos da Internet**, p.42.

Os Crimes da Informática, in Estudos em Homenagem a Manoel Pedro Pimentel, São Paulo: RT, 1992, pp. 141-142.

Computer Crime, in Anais da Conferência Internacional de Direito Penal, 1988. Rio de Janeiro: PGDF, 1998, p.461.

Informática Jurídica - O Ciber Direito, pp. 133-134.

Citados por Ivette Senise Ferreira, p. 214-5.

Citados por Ivette Senise Ferreira, p. 214-5.

GOMES, Luiz Flávio, Atualidades criminais (1). Disponível em: <www.direitocriminal.com.br>. Acesso em 30 nov. 2004.

Nelson Hungria, Comentários ao Código Penal, 1977, pp. 164-165.

A questão da jurisdição e da territorialidade nos crimes praticados pela Internet. In Direito, sociedade e informática: limites e perspectivas da vida digital. Florianópolis: Fundação Boiteux, 2000, p. 115.

ARAS, Vladimir. **Crimes de Informática. Uma nova criminalidade**. Disponível em: < www.jus.com.br>. Acesso em: 23 out. 2004.

URBAN, Aldo. **Dispara número de golpes eletrônicos**. Disponível em: <http://www.an.com.br/2004/out/06/0inf.htm>. Acesso em 01 dez. 2004.

NOGUEIRA, Fernando Célio de Brito. **Violação de e-mail é crime?**. Disponível em: <www.ibccrim.org.br>. Acesso em 02 dez. 2004.

SILVA, Adalberto Prado e. **Novo Dicionário Melhoramentos**, Volume II - 4ª edição - Ed. Melhoramentos – 1968.

Redação Infoguerra. **O que são vírus, worms e trojans**. Disponível em: www.infoguerra.com.br. Acesso em 08 dez. 2004.

COELHO, Rodrigo Durão. **Fraude online cresce e vira epidemia mundial.** Disponível em: <http://informatica.terra.com.br/interna/0,,OI434865-EI553,00.html**>.** Acesso em 08 dez. 2004.

DELMANTO, Celso. **Código Penal Comentado**. São Paulo: Renovar, 1991.

WEIKERSHEIMER, Deana. **Pirataria de Software**. Disponível em: < http://www.modulo.com.br/pt/page_i.jsp?page=3&catid=2&objid=167&pagenumber=1&idiom=0>. Acesso em 15 dez. 2004.

SILVA, Paulo Quintiliano da. Cooperação policial internacional no combate aos crimes cibernéticos. Disponível em: <http://www.modulo.com.br>. Acesso em 16 dez. 2004.

BRIGNOLI, Juliano Tonizetti e POPPER, Marcos Antonio. ENGENHARIA SOCIAL: Um perigo eminente. Disponível em: <http://www.modulo.com.br>. Acesso em 16 dez. 2004.

SANTOS, Rafael Cardoso dos. Engenharia social: fortalecendo o elo mais fraco – parte 2. Disponível em: < http://www.modulo.com.br/ >. Acesso em 16 dez. 2004.

Faulhaber, Henrique. O combate à praga do SPAM. Disponível em: <http://www.modulo.com.br>. Acesso em: 16 dez. 2004.

REUTERS LIMITED. SPAM**: MS se une à empresa de software para combater spam**. Disponível em: <http://www.terra.com.br>. Acesso em: 17 dez. 2004.

Instituto Nacional de Tecnologia da Informação. O que é assinatura digital. Disponível em: <http://www.iti.br>. Acesso em 18 dez. 2004.

GUELFI, Adilson Eduardo; BERNAL, Volnys Borges. Sistemas Criptográficos: Assinatura Digital (1999-2003). 2004. 10 f. – Apresentação (Pós-Graduação em

Segurança de Sistemas em Rede) – Faculdade Senac de Ciências Exatas e Tecnologia, Faculdades Senac, 2004.

Instituto Nacional de Tecnologia da Informação. O que é certificado digital. Disponível em: <http://www.iti.br>. Acesso em 18 dez. 2004.

Instituto Nacional de Tecnologia da Informação. O que é criptografia. Disponível em: <http://www.iti.br>. Acesso em 18 dez. 2004.

Foco Security. Como anda a segurança da informação na sua empresa. Disponível em: <http://www.focosecurity.com.br>. Acesso em 18 dez. 2004.

NBSO (NIC BR Security Office). Cartilha de Segurança para Internet Parte IV: Fraudes na Internet. Disponível em: < http://www.nbso.nic.br/docs/cartilha/cartilha-04-fraudes.html#sec2>. Acesso em: 08 dez. 2004.

GLOSSÁRIO

Autoridade Certificadora – Uma Autoridade Certificadora é uma entidade de confiança que administra a gestão de certificados digitais através da emissão, revogação e renovação dos mesmos por aprovação individual.

Crime consumado – crime realizado. Quando as condutas necessárias à pratica do crime já foram realizadas.

Crime culposo – aquele onde o sujeito ativo não desejou o resultado.

Crime doloso – aquele onde o sujeito ativo desejou o resultado ou assumiu o risco de produzi-lo.

Direito Penal Informático – Área do direito que trabalha diretamente com crimes de informática.

WEP (Wired Equivalent Privacy) – protocolo de criptografia

PGP (Pretty Good Privacy) – é um programa que faz a criptografia altamente segura de dados.

VPN (Virtual Private Network) – é uma rede privativa (com acesso restrito) construída sobre a infra-estrutura de uma rede pública, geralmente a Internet.

SSH (Secure Shell) – é um programa de acesso a computadores no ambiente de rede, para execução de comandos e transferências de arquivos de um computador para outro. O SSH tem um sistema seguro de autenticação de senhas, permitindo um canal seguro entre duas máquinas remotas.

AP (Access Point) – é o ponto central do sistema de rádio banda larga

IDS (Intrusion Detection System) – realiza análise de trafego de rede com a finalidade de detectar intrusões.