FACULDADES INTEGRADAS
"ANTÔNIO EUFRÁSIO DE TOLEDO"

FACULDADE DE DIREITO DE PRESIDENTE PRUDENTE

DA CRIMINALIDADE INFORMÁTICA

Lígia Yumi Hikawa

Presidente Prudente/SP
2008

FACULDADES INTEGRADAS
"ANTÔNIO EUFRÁSIO DE TOLEDO"

FACULDADE DE DIREITO DE PRESIDENTE PRUDENTE

DA CRIMINALIDADE INFORMÁTICA

Lígia Yumi Hikawa

Monografia apresentada como requisito parcial de Conclusão de Curso para obtenção do Grau de Bacharel em Direito, sob orientação do Professor Mário Coimbra.

Presidente Prudente/SP
2008

DA CRIMINALIDADE INFORMÁTICA

Monografia aprovada como requisito parcial para obtenção do Grau de Bacharel em Direito

_____

Mário Coimbra
Orientador

_____

Cláudio José Palma Sanchez
Examinador

_____

Paula Akemi Kikushi
Examinador

Presidente Prudente/SP, 22 de novembro de 2008.

Dedico o presente trabalho a meus pais Antônio e Armelinda, que de maneira única souberam e sabem guiar minha vida da melhor forma possível, com uma inigualável dedicação, educação, amor; aos meus queridos irmãos Renato e Rafael, que juntos me mostraram exatamente como verdadeiros irmãos devem conviver; e ao meu namorado André Parangaba, que em todos esses anos esteve presente, com demonstrações de muito amor, respeito, carinho e sinceridade, sempre me apoiando e lutando pelos mesmos objetivos, na espera de alcançar o máximo de felicidade e sucesso juntos.

AGRADECIMENTOS

Meus agradecimentos a Deus primeiramente, que é digno de toda minha adoração, de todo meu saber, de todo o meu querer, da minha salvação.
Agradeço ao admirável professor, promotor e orientador Mário Coimbra, que por seu vasto conhecimento jurídico soube, com muita paciência, ensinar a todos nós, durante a fase acadêmica e a mim, em especial, na conclusão do presente trabalho.
E a todos que participaram de alguma forma, nessa minha caminhada até os dias de hoje.

RESUMO

O presente trabalho é uma análise de uma modalidade criminosa que vem crescendo surpreendentemente nos últimos anos, qual seja: o crime informático. O estudo mostra as várias formas que se tem utilizado este sistema, seja como objeto material da conduta, ou então como um instrumento essencial para determinado delito ou ainda, somente mais um mecanismo à disposição dos criminosos. Busca-se identificar as peculiaridades necessárias para formação de uma nova figura típica, ou para se adequar às disposições já existentes. Verificam-se como os invasores podem agir através desse meio, os sujeitos envolvidos, qual o bem jurídico atingido, e algumas das possibilidades de prática delituosa na utilização desse sistema.

Palavras–chave: Sistema Informático. Crimes Informáticos. Criminalidade Informática.

ABSTRACT

The present research is an analysis about a criminal modality that is surprisingly growing up in the lasts years, called: informatics crimes. This study shows a lot of forms that this system is used, as a conducts´ material object, or as a substantial instrument for determined crime or just more one mechanism for criminals´ disposition. Search for identify the needful singularity to form a new typical figure, or to adapt on the dispositions that already exist. Establish how the invaders can act using this way, the involved guys, what is the frail law, and some possibilities of wrongful practices using this system.

Key-Words: Computerized System. Computer Science Crimes. Informatics Criminality.

LISTA DE ABREVIATURAS E SIGLAS

ARPA – *Advanced Research Projects Agency*

DATAPREV – Empresa de Processamento de Dados da Previdência Social

ENIAC – *Eletronic Numerical Integrator and Computer*

EDVAC – *Eletronic Discrete Variable Computer*

EDSAC – *Eletronic Delay Storage Automatic Calculator*

FAPESP – Fundação de Amparo à Pesquisa de São Paulo

IBCI – Instituto Brasileiro de Proteção e Defesa dos Consumidores

IBDI – Instituto Brasileiro da Política e do Direito da Informática

LNCC – Laboratório Nacional de Computação Científica

NSFNET – *National Science Foundation Network*

PRODASEN – Centro de Informática e Processamento de Dados do Senado Federal

PRODESP – Companhia de Processamento de Dados do Estado de São Paulo

UNIVAC – *Universal Automatic Computer*

UFRJ – Universidade Federal do Rio de Janeiro

www – World Wide Web

SUMÁRIO

1 INTRODUÇÃO

1.1 Origem do Computador

Pode-se dizer que a necessidade de se criar um Computador, iniciou-se quando o homem percebeu que só os dedos ou pedras já não eram suficientes para contar tudo que desejavam.

"Computador" adveio do latim "computatore", cujo significado Aurélio Buarque de Holanda Ferreira diz que é "Máquina capaz de receber instruções e executá-las sobre dados fornecidos".

Há cerca de 2.500 anos a.C já existia um modelo primitivo do Ábaco no Oriente Médio, utilizado pelos egípcios e romanos para computar as transações. Os números eram representados por pedras de calcário ("*calculi*").

Em 1642 foi criada a primeira máquina de calcular automática, feita por Blaise Pascal. Com o intuito de ajudar seu pai, que era coletor de impostos, inventou tal máquina. Ela conseguia somar e subtrair números de até oito algarismos. Gottfried Leibniz aperfeiçoou a máquina inventada por Pascal em 1673, e, já em 1694, era possível fazer tanto adição, quanto subtração, multiplicação, divisão, e até mesmo raiz quadrada. No entanto, o "computador" era uma simples máquina de calcular.

Houve então necessidade e vontade de se ter mais funções, mais utilidade, que houvesse possibilidade de também programá-la.

Foi então que, por volta de 1822, Charles Babbage, colaborou imensamente para esse objetivo. Considerado hoje como o "pai" do computador atual, ele criou um projeto de máquina para calcular tabelas, conhecida como "Máquina das Diferenças". Pouco tempo depois, em meados de 1833, projetou a "Máquina Analítica", cuja novidade era ser pioneira em poder ser "programada".

Em 1880, Herman Hollerith, criou o sistema de perfuração dos cartões para as operações estatísticas. Para isso, precisou usar máquinas especialmente projetadas.

Porém, no final da década de 1930, na Segunda Guerra Mundial, houve necessidade maior de cálculos precisos, porque procuravam meios eficazes para organização das enormes quantias de materiais bélicos, e ainda para o cálculo das tabelas de artilharia.

O primeiro computador de grande porte, totalmente eletrônico, foi criado por John W. Mauchly e John Presper Eckert, com finalidade de resolução de problemas balísticos. Isso foi entre 1934 e 1946, que recebeu o nome de *Eletronic Numerical Integrator and Computer – ENIAC.* Composto por mais de 17.468 válvulas, com 1.500 relês, 70.000 resistores e ainda 10.000 capacitores. Fabrízio Rosa (2002, p. 26) afirma que "Consumia cerca de 150 KW de potência, ocupava 140 m² aproximadamente e pesava cerca de 30 toneladas".

Após o ENIAC, surgiu o *Eletronic Discrete Variable Computer – EDVAC,* criação de John Von Neumann e, em seguida o *Eletronic Delay Storage Automatic Calculator – EDSAC* e o *Universal Automatic Computer – UNIVAC,* iniciando a primeira geração de computadores, caracterizada pelas válvulas eletrônicas.

A segunda geração aparece no final de 1950. Sua característica foi o uso de uma novidade tecnológica: o uso de transistores, em substituição às válvulas. O computador passou a ser comercializado para civis também.

Foi nessa geração ainda, que surgiram as primeiras linguagens de alto nível - Fortran e Cobol – e a indústria de Software também. Os primeiros sistemas operacionais também surgem nessa época.

Por volta de 1958 aparece a terceira geração, que traz mais um avanço: os circuitos integrados.

Esses avanços foram além do equipamento, atingindo também as técnicas de programação, surgindo a multiprogramação e o teleprocessamento.

A multiprogramação é quando o sistema operacional executa vários processos ao mesmo tempo, enquanto que o teleprocessamento é a capacidade de se ter processamento à distância.

A quarta geração foi caracterizada pelo avanço das técnicas de fabricação dos circuitos integrados, com maior capacidade de armazenamento, mais rapidez. Surgem os microprocessadores e computador de grande porte – mainframe.

A próxima geração caracterizou-se pelos computadores menores e mais simples. Apresentou ainda grandes avanços para o hardware, software e para as telecomunicações.

Nessa evolução tecnológica, não se imaginava que dimensão se tomaria através do computador hoje conhecido, que até então era uma busca pela rapidez, pela simplicidade, facilidade nos cálculos. Enquanto ficou na esfera dos pesquisadores, não se visualizava qualquer prática delitiva. No entanto, a partir do momento que houve fusão para os civis, ou seja, tornando-se de uso comum, o uso ilícito desse equipamento surgiu. E hoje, não se pode pensar somente em evolução tecnológica, mas também em evolução da precaução que se deve ter em razão àquela.

1.2 Breve histórico sobre a Internet

Não muito após o surgimento do Computador, a Internet aparece e uma revolução em nossos meios de comunicação, educação, cultura, entretenimento acompanham-na.

Ela é uma rede mundial de computadores que interliga milhões de usuários. Com tamanho avanço tecnológico, tornou-se um instrumental para as pessoas, que a utilizam da maneira que melhor lhes convir, seja de forma lícita ou não. E é essa que preocupa os operadores do Direito, principalmente do Penal, visto a potencialidade lesiva das atitudes (positivas ou negativas), no âmbito da Rede.

Uma primeira idéia do que hoje conhecemos como internet surgiu durante a Guerra Fria. Paul Baran, buscando encontrar um meio de se manter

interligado com sua base, mesmo que houvesse um ataque. Encontrou uma rede, onde não havia nenhum comando central e os pontos desta se equivaliam, utilizando-se do sistema telefônico. Assim, caso houvesse falha em alguma das redes, haveria uma outra via para se comunicar.

A ARPA (*Advanced Research Projects Agency*) patrocinou algumas empresas com o objetivo de interligar computadores de todo o país, para melhorar a capacidade de armazenagem e uso. Foi criada então, em 1969, a Arpanet, capaz de interligar os laboratórios de quatro universidades. Já em 1985, surge a NSFNET (*National Science Foundation Network*), responsável pela interligação entre os computadores da NSF. Após isso, foram conectadas essas duas grandes redes (NSF e Arpanet). Com essa junção, originou-se finalmente a Internet.

Em 1993, com a criação do *www* (*World Wide Web*), passa a existir o uso comercial da rede Internet.

Ela começou fazer parte da história do Brasil em 1988, com o apoio e iniciativa de alguns órgãos como a FAPESP (Fundação de Amparo à Pesquisa do Estado de São Paulo, a UFRJ (Universidade Federal do Rio de Janeiro) e LNCC (Laboratório Nacional de Computação Científica).

Hoje, ela faz parte do cotidiano de mais de 15 milhões de brasileiros. Estima-se que cerca de 80% dos computadores conectados à rede não estão protegidos o suficiente, passíveis de serem invadidos facilmente; acredita-se que aproximadamente 500 vírus diferentes são espalhados todos os dias; Renato M. S. Opice Blum (2001, p. 41) afirma que “em 1999, os prejuízos decorrentes das fraudes eletrônicas chegaram a mais de US$ 3,2 bilhões”.

Postas as considerações acima, nota-se cada vez mais a necessidade de proteção tanto às informações quanto ao computador, que vêm sofrendo um crescente controle humano, podendo causar prejuízos gigantes para o convívio social, levando à instabilidade da paz social.

2 RELAÇÃO DO DIREITO COM A INFORMÁTICA

2.1 Direito da informática

A importância da Informática para o Direito pode ser tanto como um meio, quanto um objeto. Assim, novas áreas de estudo passam existir, e é necessário que se identifique qual a aplicabilidade e que influência tem essa nova tecnologia no ordenamento jurídico.

Por volta de 1980, o Conselho da Comunidade Européia reconheceu a existência do Direito da Informática, o qual representa uma reunião de conhecimentos diversos de outras áreas do direito, e acaba influenciando o Direito tradicional.

Há quem diga que com essa nova tecnologia, surge um novo ramo do conhecimento jurídico, advindo da necessidade social frente a essa evolução. Mário Antônio Lobato de Paiva (2002), sócio-fundador do IBDI (Instituto Brasileiro da Política e do Direito da Informática) conceitua o Direito da Informática como sendo:

> Conjunto de normas e instituições jurídicas que pretendem regular aquele uso dos sistemas de computador – como meio e como fim – que podem incidir nos bens jurídicos dos membros da sociedade; as relações derivadas da criação, uso, modificação, alteração e reprodução do software; o comércio eletrônico, e as relações humanas realizadas de maneira sui generis nas redes, em redes ou via internet.

Luiz Fernando Martins Castro (1992, p.19-20) define: “Direito da Informática é o conjunto de leis, normas e princípios aplicáveis aos fatos e atos decorrentes do tratamento automatizado da informação” e que “os fatos são conseqüências aportadas pela informática e não imputáveis a vontade humana, hipótese nas quais estaremos em face dos atos informáticos”.

Há que se destacar que apesar de toda essa evolução, a presença do homem é fundamental para o uso desse sistema informático, o que nos leva concluir que todo ato informático é imputável à vontade do homem.

Não há unanimidade em relação a um possível surgimento de novo ramo do Direito. É claro que se exigem cuidados peculiares, no entanto, não é o suficiente para se reconhecer um novo ramo.

Certamente a Informática está superando todas as fronteiras possíveis, sejam geográficas, políticas ou ainda culturais. Portanto, há a necessidade de leis que punam, previnam qualquer ato ilícito proveniente dessa nova tecnologia.

O surgimento da informática em nosso meio foi muito rápido, e com isso, o Direito não pôde acompanhar com essa mesma velocidade. Assim, não há tutela suficiente para tamanha necessidade. No entanto, é preciso que se tenha cuidado para não criar leis excessivas e desnecessárias.

Poder-se-ia dizer que uma adequação jurídica seria ideal nesse momento, ou seja, utilizar-se de normas já existentes quando estas forem suficientes para as condutas ilícitas que vierem; quanto às outras, que não têm previsão alguma que se possa adequar, seria necessária a criação de novas normas.

Não há possibilidade de o Direito acompanhar todas as evoluções tecnológicas e informáticas que vêm acontecendo, já que para isso, novas normas teriam que ser criadas a todo minuto. Porém, é necessária uma atualização suficiente para garantir o sossego e a paz social.

2.2 Informática Jurídica

A Informática Jurídica não se confunde com o Direito da Informática. Este diz respeito à solução de condutas ilícitas provenientes do uso da Informática, utilizando-se de todo conhecimento jurídico existente; já aquela tutela a aplicação dos computadores na área jurídica. Diz Martinho, Antonio Anselmo (1987, p. 11): “A informática jurídica diz respeito ao emprego da metodologia e das técnicas de processamento de dados na arte e na ciência do direito”.

Com o uso da computação, facilitou-se muito, tanto para a administração da justiça, como também na análise de jurisprudências, informativos, nas atualizações jurídicas.

Uma primeira preocupação para os juristas se voltava para análise da informática como um utilitário para o Direito na pesquisa e criação de banco de dados. Com isso, foram surgindo centros de processamentos de dados como, por exemplo, o Tribunal de Alçada Criminal de São Paulo, e o Sistema de Protestos.

No Brasil, tivemos a criação, entre 1965 e 1975, do Centro de Informática e Processamento de Dados do Senado Federal (Prodasen), Empresa de Processamento de Dados da Previdência Social (Dataprev), Companhia de Processamento de Dados do Estado de São Paulo (Prodesp), dentre outros.

Antonio Chaves (1982, p. 7) dizia: “a influência da informática pesaria sobre o equilíbrio econômico e modificaria o pacto do poder colocando em questão a soberania nacional, pois funciona como amplificador, introduzindo desequilíbrios que devem ser avaliados e corrigidos”.

Está claro que a informática influencia várias atividades que o homem realiza. Para o Direito, tal influência se vê tanto para ações criminosas, como para evoluções de conhecimentos, ou ainda para informatizações de dados, processos.

2.3 Direito e Informática

Com os avanços da Informática, o Direito vem sofrendo mutações. Estudiosos vêm desenvolvendo novas normas, na tentativa de coibir qualquer ação ilícita advindo do uso em massa dessa nova tecnologia.

No entanto, há dificuldades enormes. Dentre elas, pode-se citar a linguagem diferenciada contida na Informática. Novas palavras foram aparecendo, e uma linguagem característica que não pertencia ao conhecimento da ciência até então. Assim, é preciso que o jurista entenda os termos dessa “nova” linguagem, para que as normas sejam precisas, e também que a delimitação de sua incidência seja acertada.

O ambiente virtual é um assunto desconhecido para o Direito. A internet, por exemplo, não é de ninguém. E como impor regulamentações para essa situação?

Para o Direito Constitucional, é imprescindível que as normas sejam baseadas no Estado de Direito Democrático, ou seja, como prescreve o artigo 1º, da Constituição Federal:

> A república Federativa do Brasil, formada pela união indissolúvel dos Estados e Municípios e do Distrito Federal, constitui-se em estado Democrático de Direito e tem como fundamentos: I – a soberania; II – a cidadania; III – a dignidade da pessoa humana; IV – os valores sociais do trabalho e da livre iniciativa; V – o pluralismo político.

É preciso que se reflita em proteção aos direitos fundamentais, tais como a liberdade de informação (direito de informar e informar-se), liberdade da atividade intelectual, artística, científica e de comunicação, conforme o artigo 5º, inciso IX e 220 da Constituição Federal.

Artigo 5º, IX, Constituição Federal estabelece: “É livre a expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença”.

Artigo 220, Constituição Federal: “A manifestação do pensamento, a criação, a expressão e a informação, sob qualquer forma, processo veículo não sofrerão qualquer restrição, observado o disposto nesta Constituição”.

Há que se dizer ainda que, como a Internet não pertence a ninguém, havendo interconexão de fichários, não existe a privacidade que se espera com o uso da Informática, pois é possível obter informações de cada indivíduo, ainda que este não permita ou se quer saiba.

Outra questão que se deve discutir é o avanço nas vendas on-line, que envolve tanto venda, quanto troca, compras, etc. Isso gera reflexo claro no Direito do Consumidor, Comercial, do Trabalho, dentre outros.

Como exemplo do que cerca o Direito do Consumidor, cita-se a identidade real de quem está fornecendo os produtos ou a qualidade que estes se encontram, se suas ofertas estão adequadas de acordo com os procedimentos

legais e várias indagações caso o produto esteja com vício, ou insatisfação quanto a ele. Ainda pode-se falar que não há definições conclusivas quanto aos recursos cabíveis para sanar os prejuízos decorrentes dessas ações por meio da Informática.

Tais questionamentos influenciaram na criação do IBCI (Instituto Brasileiro de Proteção e Defesa dos Consumidores), que impulsionou da criação de um Tribunal Arbitral para solucionar os conflitos das relações de consumo pela internet.

Quanto ao Direito do Trabalho, a análise volta-se para o trabalho *online*, ou seja, o contrato é feito pela internet, sem qualquer entrevista, e é através dela que se executa o trabalho também. Isso gera questionamentos quanto à subordinação, e pessoalidade, as quais são requisitos essenciais para caracterização da relação de emprego. Além disso, tem ainda a questão de horas extras, que poderiam ser apuradas conforme dia e horários acessados.

Como se pode ver, o crescimento rápido dessa tecnologia forçou o homem a adaptar-se. No entanto, para o Direito, o ritmo já não é o mesmo.

3 DIREITO PENAL E INFORMÁTICA – CONSIDERAÇÕES GERAIS

3.1 Direto Penal e Informática

Hoje o que ocorre são inúmeras ações, que prejudicam o convívio da sociedade, sobre as quais se busca saber se há ou não tipos correspondentes em nossa atual legislação. Uma primeira indagação se refere à existência do princípio da legalidade. Isto porque, caso não haja previsão legal sobre determinado fato, não há possibilidade de punição, conforme o princípio acima citado.

Daí então, discute-se a possibilidade de se adequar à legislação já existente nos eventuais delitos.

É preciso que se busque solução para tais indagações, visto que a paz social encontra-se ameaçada pelo rápido aumento das ações ilícitas, desde fraudes milionárias a pornografia infantil.

As ações são contra o sistema informático ou através de sua utilização. Assim, o Direito Penal não pode ficar parado diante dessas transformações, mas isso não significa que seja necessário criar um novo ramo especificamente para tais situações, mas que se busque nas legislações já existentes dispositivos que estejam em consonância com o delito praticado.

Importante ressaltar que em nosso sistema penal não é permitido que se faça analogia. Portanto, é necessário que a prática delitiva esteja em plena consonância com o dispositivo legal. Caso contrário é preciso que novos tipos sejam criados.

Em busca de uma resposta penal para essas indagações acerca da criminalidade informática, projetos de lei têm sido criados, visando uma regulamentação desse tema. Podem ser citados: Projeto nº 597, de 1991; Projeto nº 152 de 1991; Projeto nº 1.713, 1996; Projeto nº 3.943,1997; Projeto de Lei do Senado nº 76, 2000; Projeto de Lei nº 6.210, 2002, dentre outros.

O que se pode ver nesses projetos são expressões vagas, como por exemplo, indevidamente, permissão, as quais podem gerar a uma atipicidade da conduta.

Dentre os crimes possíveis na rede, podemos citar crimes contra honra, de informática, acesso indevido, estelionato, e um dos mais preocupantes, pornografia infantil.

Há que se falar ainda nos ilícitos civis, que ocorrem pela compra *online*, onde não se tem o contato direto com o produto, podendo gerar algumas insatisfações.

E quanto à relação de trabalho? Os empregadores podem ter acesso aos e-mails dos empregados? E às propagandas? Quais seriam seus limites?

Assim, com toda essa evolução espantosa, era, e é clara a necessidade de interferência do Direito para possíveis soluções.

3.2 Conceito

Não há que se confundir delito informático com aqueles delitos cometidos por meio do uso do computador. O delito informático pode ser considerado aquele que tutela a inviolabilidade de dados. Portanto, a utilização do computador pelo agente para o cometimento de crime não é considerada como delito informático.

No entanto, vários autores adotaram essa terminologia para ambos os casos. Hoje é dificilmente ignorada, ainda que não seja tão adequada.

O Doutrinador João Marcelo de Araújo Junior (1988, p. 460) conceitua esse tipo de crime como sendo:

> 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.

Uma outra visão é de Ivette Senise Ferreira (2000, p. 208): “Crime Informático é toda ação típica, antijurídica e culpável cometida contra ou pela utilização de processamento automático de dados ou sua transmissão”.

Sérgio Marcos Roque (2000, p. 309-333): “É a conduta definida em lei como crime em que o computador tiver sido utilizado como instrumento para a sua perpetração ou consistir em seu objeto material”.

Conceitua ainda Gustavo Corrêa (2000, p. 43) que:

> Todos aqueles relacionados às informações arquivadas ou em trânsito por computadores, sendo esses dados, acessados ilicitamente, usados para ameaçar ou fraudar; para tal prática é indispensável à utilização de um meio eletrônico.

Há ainda uma posição doutrinária de Carla Rodrigues Araújo Castro (2001, p.10) que não se limita tão somente ao computador; abrange o sistema informático geral: “Aquele praticado contra o sistema de informática ou através deste, compreendendo os crimes praticados contra o computador e seus acessórios e os perpetrados através do computador”.

Assim, pode-se ver que ainda não há um conceito unânime sobre tal tema. Parece, então, ser mais coerente um conceito que envolva todo o sistema informático, ou seja, que abranja desde o próprio computador, até todos os meios que possam servir como transmissão de dados, seja uma simples impressora ou então uma rede de comunicação.

É importante lembrar que existem alguns termos muito específicos utilizados na área da informática que não estariam tipificados explicitamente. Dessa forma, tal modalidade não estaria inclusa como um “crime”, já que lhe falta o principal: tipicidade.

Por fim, importante que se analise qual o caminho da conduta do agente. Ou seja, se ele utilizou o sistema informático como um meio, ou se ele visa atingi-lo. Há, portanto, três possíveis ações: aquelas em que o sistema informático é o alvo do ato ilícito; aquelas em que ele é um meio para o cometimento de outros delitos; ou então as que só podem ser alcançadas com seu uso.

3.3 Classificação

Existem várias classificações para esses delitos, já que o sistema informático ora serve como simples meio, onde sua atuação seria dispensável, ora como objeto do crime e ora somente através dele que se conseguiria atingir o fim almejado.

Dentre as diversas classificações, podem ser citados alguns doutrinadores:

Túlio Lima Viana (2003, p. 13), autor da obra “Fundamentos do Direito Penal Informático” faz uma divisão dos delitos em: impróprios, que seriam aqueles praticados pela utilização do computador como instrumento; próprios, seriam considerados aqueles em que houve ataque à inviolabilidade dos dados; Os que além de tutelar a inviolabilidade, também visar outros bens jurídicos, serão denominados de Delitos Informáticos Mistos; e, finalmente, àquele que fora cometido como crime-meio com finalidade de um crime-fim, considerara-se como Delito Informático Mediato ou Indireto.

Pérez Luño (1994, p. 17-18) classifica de acordo com as tendências “objetiva, subjetiva e funcional”. Subjetiva seria a análise de como o autor atua; Para a objetiva, são abrangidos os crimes que foram cometidos pelo computador; E, finalmente, na funcional, observam-se os delitos de programação, processamento de dados, entrada e saída, etc.

Antonio Scarance Fernandes (1999, p. 8), por sua vez, classifica tais crimes em puros, impuros e comuns. Puros seriam aqueles em que o sistema informático é utilizado como meio e também como fim desejado pelo autor do crime; Impuros, aqueles em que não dependem tão somente do sistema, mas foi ele quem contribuiu para a prática do delito (já tipificado pelo Direito Penal), onde o bem jurídico encontra-se armazenado no equipamento virtual; Comuns concentram-se nas ações, onde a informática é um meio para a prática do delito também, mas que nesse caso esta é apenas mais um instrumento.

No meio de tantas classificações, pode-se notar que a informática tem que funcionar como um diferenciador, já que quando é apenas um instrumento para

o cometimento de um delito, a mais adequada tipificação é para os crimes comuns mesmo; enquanto que quando é essencial para alcançar o objetivo traçado pelo autor, insere-se em tipos penais já previstos, ou então, àqueles que não encontram previsão expressa ainda, os quais são conhecidos como crimes informáticos. Importante lembrar que há certa incoerência em falar nesse último caso, visto que se não existe tipicidade, não há que se falar em “crime”.

4 BEM JURÍDICO E SISTEMA INFORMÁTICO

4.1 Importância da informação

Uma das premissas a ser considerada é que para o Direito Penal não se pode levar em conta toda e qualquer lesão à vida em sociedade, pois é preciso que se respeite o princípio da intervenção mínima, o qual dá importância somente àquelas agressões insuportáveis no meio social. Assim, somente quando não for possível outro meio de solução, é que se busca uma intervenção da atividade jurisdicional. Vale lembrar que tal princípio decorre de outros previstos na Constituição, como por exemplo, o direito à vida, igualdade, propriedade, dentre outros.

Nos crimes de informática, o que se pode ver é uma violação a vários bens jurídicos, onde o indivíduo invade informações contidas nesse sistema, e prejudica a paz social.

Para se saber que bem jurídico foi afetado pela ação delituosa por meio do sistema informático, é preciso analisar sobre que objeto a conduta recaiu. Dessa forma, se há calúnia a alguém, a lesão foi contra honra objetiva. Se houver ameaça por correio eletrônico, é a liberdade individual que está em questão.

Porém, apesar de se detectar que bem jurídico foi atingido, para tipificação de tal lesão, pode ser que não sejam encontrados elementos constitutivos na conduta do agente, visto que o meio utilizado fora o sistema informático ou ainda não ter plena concordância com o bem já tutelado, pois pode tratar de termos desconhecidos pelo ordenamento jurídico.

Necessário se faz ainda, atentar para a relação entre a proteção de bens tangíveis e o Direito Penal, pois neste caso, o objeto pode ser o armazenamento ou transmissão e acessórios, e os próprios recursos que se encontram no sistema, tais como os dados armazenados, como também o *software*.

Assim, não se pode falar que são bens tangíveis, e há necessidade, portanto, de se tutelar bens intangíveis e imateriais também.

Pode-se afirmar então que o sistema informático como um todo é o bem jurídico que deve ser tutelado. No entanto, deve-se estar atento, pois pode se tornar excessiva essa consideração, onde furtos de equipamentos, como teclado, monitor, seriam abrangidos por essa forma de crime. Nesse caso, há que se lembrar que como se trata de elemento físico, tangível, este poderá se servir do próprio crime de furto para tipificação.

Conclui-se, portanto, que o que se busca não é o que está em torno da informática como um todo, mas sim os recursos que nela estão inseridos. Sandra Gouvêa (1997, p. 41) ressalta que "há que se atentar para a importância da informação e do dado, que devem ser compreendidos como bens jurídicos independentes do conteúdo que carregam". Complementa Débora Fisch Nigri (1992, p. 47) "uma legislação específica no campo penal deve levar em conta o aspecto autônomo das informações contidas em um sistema de computação e a importância da eletrônica no mundo de hoje".

Observa-se então que a informação, nos dias atuais, é de importância grandiosa, a qual merece tutela penal, pois pode servir tanto como um objeto de transmissão, como também ser um saldo bancário, podendo valer milhões, ou então ser quebra de sigilo completo de segredos do Estado.

Maria Hela Junqueira Reis (1996, p. 37) claramente descreve "a informação é um bem em si mesma, pode valer milhões e milhões de dólares, ou pode ser vital para a segurança dos Estados ou de certos organismos".

Como visto acima, nos crimes informáticos, a tutela recai em regra sobre o objeto "informação". Dependendo de que bem tutelado dirige-se a ofensa, tem-se uma tradução para a informação. Por exemplo, se for contra a honra, ela se traduzirá em honra; Se o dano for contra o patrimônio, sua tradução é em patrimônio, e assim por diante.

No entanto, pode acontecer de não ter essa especificidade esperada para todas as questões, necessitando-se, portanto, de novas soluções. É indiscutível que a informação possa se transformar em uma mercadoria, onde há uma junção de dados que são enviados por impulsos magnéticos. Nesse caso, pode-se dizer que o

objeto é um bem imaterial. Tratando-se dessa mesma mercadoria, nota-se que há possibilidade ainda de ser um objeto material também, onde a informação possa ser furtada, armazenada etc.

Garry Marshall (1984, p. 12) explica que:

> Considerar a informação como uma mercadoria que pode ser comprada ou vendida do mesmo modo que qualquer outra é uma atitude relativamente recente. Apesar disso, a informação é diferente das mercadorias convencionais de forma significativa.

Analisando-se o comentário acima, é fácil entender que nas compras de qualquer bem, o objeto passa ser do comprador somente. No caso da informação, isso não ocorre, já que tanto o vendedor, quanto o comprador têm conhecimento daquela.

Nota-se assim a tamanha dificuldade quando se trata desse objeto em questão, visto que não se sabe se deve considerá-lo como material, podendo ser regulado pelo Código Penal, tipificando a conduta como furto, por exemplo, ou se deve ser criadas novas normas, já que tipificação para esse tipo de crime imaterial não se encontra prevista.

Desta forma, não se pode considerar a informação como apenas objeto imaterial, devendo-se tratar e dar proteção à cada caso, analisando-se sua individualidade.

Nos dias atuais, verifica-se uma relevância cada vez maior da informação, a qual tem a finalidade de não somente levar ao saber, mas tem influência decisiva com sua utilização.

Diante do exposto, comprova-se que a informação pode se traduzir em diversos bens quando utilizada ilicitamente, como a honra, propriedade, liberdade, dentre muitos outros.

4.2 Dispositivos Legais acerca da Informação

Existem alguns dispositivos em nosso ordenamento acerca do tema exposto. Dentre eles, pode-se citar primeiramente aqueles definidos por nossa lei maior, Constituição Federal.

> **Art. 5.º** Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
>
> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;
>
> [...]
>
> LXXII - conceder-se-á "habeas-data":
>
> a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público;
>
> [...]
>
> **Art 220.** A manifestação do pensamento, a criação, a expressão e a informação, sob qualquer forma, processo ou veículo não sofrerão qualquer restrição, observado o disposto nesta Constituição.

Percebem-se nesses artigos as garantias constitucionais previstas, visando assegurar a intimidade, vida privada, honra, imagem das pessoas, liberdade de informação, dando-lhes o direito de conhecer informações relativas a elas que estejam contidas em banco de dados do governo ou de simples caráter público.

Outro importante código a se comentar é o de Defesa do Consumidor (Lei n. 8.078/90), onde merecem destaque especialmente dois artigos:

> **Art. 72.** Impedir ou dificultar o acesso do consumidor às informações que sobre ele constem em cadastros, banco de dados, fichas e registros: Pena – Detenção de seis meses a um ano ou multa.
>
> **Art. 73.** Deixar de corrigir imediatamente informação sobre consumidor constante de cadastro, banco de dados, fichas ou registros que sabe ou deveria saber se inexata: Pena – Detenção de um a seis meses ou multa.

Há uma preocupação clara em se proteger o direito do consumidor, permitindo-lhe a consulta das informações que constem sobre ele em qualquer tipo de cadastro ou mesmo poder corrigir alguma já existente, sendo sujeita sua recusa à pena de detenção e multa.

Apontam-se ainda regulamentações sobre os programas de computador, que tutelam tanto a propriedade intelectual de suas criações, quanto os direitos autorais sobre eles, quais sejam: Leis nº 9.609/98 e 9.610/98.

A Lei nº 9.296/96, a qual regulamentou a parte final do inciso XII do artigo 5º da Constituição Federal dispõe que:

> **Art. 1.º** A interceptação de comunicações telefônicas, de qualquer natureza, para prova em investigação criminal e em instrução processual penal, observará o disposto nesta Lei e dependerá de ordem do juiz competente da ação principal, sob segredo de justiça.
>
> **Parágrafo único.** O disposto nesta Lei aplica-se à interceptação de comunicações em sistemas de informática e telemática.
>
> **Art 5º, inciso XII, Constituição Federal** – é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal.

Há uma tutela nesses artigos para que se garanta o sigilo das comunicações, e, dentre elas, inclusa está a Informática. É, portanto, inviolável qualquer ato contra esse sigilo, salvo quando autorizado judicialmente.

No Código Penal, podemos encontrar os artigos 313-A e 313-B; 153, parágrafo 1º-A e 325, parágrafo 1º, inciso I, os quais foram acrescidos pela Lei n. 9.983/2000.

> **Art. 313-A.** Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano: Pena – reclusão, de 2 (dois) a 12 (doze) anos, e multa.
>
> **Art. 313-B.** Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente: Pena – detenção, de 3 (três) meses a 2 (dois) anos, e multa.
>
> **Art. 153, §1º A –** Divulgar, sem justa causa, informações sigilosas ou reservadas, assim definidas em lei, contidas ou não nos sistemas de

> informações ou banco de dados da Administração Pública: Pena – detenção, de 1 (um) a 4 (quatro) anos, e multa.
>
> **Art. 325, §1º, inciso I –** Nas mesmas penas deste artigo incorre quem permite ou facilita, mediante atribuição, fornecimento e empréstimo de senha ou qualquer outra forma, o acesso de pessoas não autorizadas a sistemas de informação ou banco de dados da Administração Pública.

Nestas disposições, é o funcionário público que se encontra sob observação da Justiça, onde se procura evitar qualquer ação ilegal daquele, nas condutas de modificar, inserir, excluir indevidamente qualquer informação constante no banco de dados de nossa Administração Pública, para obtenção de vantagem, seja para si ou para outrem; São reprovadas ainda as condutas de divulgar qualquer informação sigilosa relativa à profissão, e daquele que facilita ou permite o acesso de quem não é autorizado, fornecendo, emprestando, ou por qualquer outro meio possível, a senha para tal ato.

Assim, expõem-se alguns dos dispositivos vigentes que mais se destacam sobre a Informação.

4.3 Possíveis atuações contra o bem jurídico tutelado

Na medida em que vemos avançar a tecnologia, podemos infelizmente acompanhar um crescimento juntamente dos meios possíveis para prática de ilícitos pelo uso do sistema informático. Porém, não há como definir precisamente todos os meios que o agente possa se utilizar para lesionar ou colocar em perigo o bem jurídico tutelado. Não se pode falar em uma tipificação comum, ou seja, é fácil se determinar que àquele que “subtrai para si ou para outrem coisa alheia” comete furto, ou então que um agente capaz e dentro dos requisitos legais retira a vida de alguém, cometerá um homicídio; o mesmo não ocorre nos delitos informáticos, visto que não se pode definir ao certo como foi que o agente atuou para a prática do delito.

Nota-se que em muitos casos o sistema informático era o único meio para se obter o resultado pretendido, enquanto poucos se utilizam desse instrumento apenas por ser um facilitador para o cometimento de certo delito.

Existem inúmeras formas de execução para esse tipo de crime. Podem ser citados alguns dos mais freqüentes, como Engenharia Social, Ataque de Força Bruta, Acesso Local (*offline*), Acesso Remoto (*online*), e o Cavalo-de-tróia.

Engenharia Social – é a técnica que o pirata se utiliza buscando uma fragilidade do usuário. É o único meio em que não é preciso conhecimento algum em Informática, pois é o comportamento do indivíduo que possibilitará o êxito do crime.

É fácil detectar este tipo de fragilidade quando se trata de usuários inexperientes, novatos, pois estes normalmente se utilizam de dados pessoais para criação de suas senhas, sejam nomes ou sobrenomes de pessoas próximas, data de nascimento, e estes certamente são as primeiras tentativas do invasor.

Uma outra técnica é induzir a pessoa a erro perguntando suas senhas. Isso se faz através de ligações, onde o invasor identifica-se como sendo um técnico especialista na área da Computação e a vítima, acreditando se tratar de um especialista, inocentemente passa suas senhas; ou ainda, atualmente mais comum, através de e-mails, onde o invasor utiliza-se de remetentes conhecidos, como suporte técnico, órgãos importantes como Receita Federal, ou de simples dúvidas, e pede-se que seja digitada a senha para que possa trocá-la por alguma falha no sistema.

Diante dessas técnicas, faz-se necessário definir o momento em que a execução do crime ocorre. Nestes casos, só se inicia quando o invasor tenta utilizar-se da senha adquirida pela Engenharia Social para adentrar em algum sistema. Não importa, portanto, se o agente só possui a senha e não tenta sequer acessar algo da vítima.

Essa técnica pode ocorrer tanto no acesso local quanto no remoto.

Ataque de força bruta – é uma outra técnica muito comum de invasão. O acesso aos sistemas atualmente, possui uma tela inicial onde o indivíduo precisa colocar seu nome de usuário e uma senha por este escolhida para que aquele seja iniciado. Ocorre que, ao digitar a senha para o acesso, confere-se esta com o nome

de usuário armazenado no banco de dados existente. Com a conferência destes, fica livre o acesso.

Neste tipo de técnica, o ofensor busca uma fragilidade não mais da pessoa, mas sim do sistema. Utilizando-se de tentativa e erro, o invasor encontra o conjunto certo de usuário e senha, passando ter o livre acesso ao sistema.

Por se tratar de tentativa e erro, se fosse feito manualmente, deveria haver plena disponibilidade de tempo do agente ofensor, já que são inúmeras as combinações possíveis. Posto isto, estes piratas criaram um programa em que essa tarefa de testar cada uma das possibilidades fica por conta dele, colocando-se possíveis pares ordenados para o acesso.

Assim, a execução terá início quando o sistema for liberado. No entanto, só haverá consumação se houver acesso aos dados que se encontram armazenados neste sistema, seja por simples leitura, execução ou escrita.

O ataque de força bruta também pode ser utilizado tanto no acesso local como no remoto.

Acesso Local – Neste, o invasor tem acesso ao computador fisicamente. Ele o acessa, e por meio de comandos emitidos pelo teclado ou mouse, fica conectado ao computador diretamente.

Esta técnica pode se dar tanto de forma secreta, quanto por violência ou ameaça à vítima.

Não há muito a ser feito para proteger o sistema desse tipo de invasão, já que com o contato físico direto do ofensor com o computador, o sistema é muito vulnerável.

As senhas que estão armazenadas no Sistema Básico de Entrada e Saída são apagadas quando se retira a bateria da placa-mãe. Neste tipo de delito, a execução se inicia quando a senha é apagada. Porém, sua consumação só se dará quando algum dado for lido, executado ou escrito.

Se por ventura o agente subtrair o disco rígido onde são armazenados os dados, o crime será de furto. No entanto, se houver acesso a esses dados posteriormente, será considerado como acesso indevido ou não autorizado, já que o

furto foi apenas um crime-meio para consumação daquele (Princípio da Consunção). É claro que é preciso analisar qual era o dolo do invasor naquele instante.

Acesso Remoto – é o mais comum. O pirata não tem qualquer contato físico com o computador da vítima. Os comandos emitidos são de um computador diverso daquele que contém as informações pretendidas. Na maioria das vezes, ele se dá por meio da rede Internet.

Existem inúmeras formas de se ter esse acesso proibido, mas resumidamente o agente procura falhas de programação ou nas configurações dos sistemas operacionais. A forma que será utilizada dependerá de qual sistema operacional a vítima está utilizando.

O início da execução se dá quando o agente emite os comandos, e a consumação quando acessa os dados pela leitura, execução ou escrita.

Cavalo de Tróia – São programas que se assemelham aos vírus, onde os sistemas computacionais são infectados, permitindo o acesso livre dos piratas, geralmente pela Internet.

O invasor envia um programa a ser executado pela vítima. Ao realizar tal conduta, ela fica em conexão direta com o computador do pirata e este passa ter todas as informações necessárias manter o controle remoto com computador invadido. Esse programa pode ser um jogo, uma música, uma foto, onde a vítima consegue acessar normalmente. No entanto, encontra-se inserido neles comandos que permitem o livre acesso pelo hacker. Ele poderá então ler, apagar, inserir ou modificar quaisquer dados no computador invadido, até mesmo descobrir todas as senhas, ter acesso aos arquivos, e acompanhar de perto tudo o que a vítima faz ou deixa de fazer em seu computador.

A execução se inicia quando o programa é enviado à vítima. Porém, a consumação só se dá quando o invasor acessar qualquer informação armazenada no computador da vítima.

5 SUJEITOS

5.1 Sujeito Ativo

Atualmente, o mundo tem visto inúmeros casos, das mais variadas formas para o cometimento deste tipo de delito. Há finalidades, resultados e o modo de realizar diversos. Basicamente, todos os atos lesivos ao Direito por esse meio se resumem em um ofensor: o *hacker.*

Deborah Fisch Nigri (1992, p. 40-48) explica que:

> A denominação hacker sofreu uma imensa transformação em seu significado original. No início dos anos 80, quando da evolução do uso de computadores pessoais, os hackers eram aqueles indivíduos que exploravam a fundo o sistema de computador com o intuito de descobrir todo o potencial do sistema e as nuances do computador. Hoje em dia o termo hacker é designado pejorativamente para referir-se aos invasores informáticos que, burlando esquemas de segurança, ou utilizando-se de senhas de outrem, penetrem indevidamente em um sistema de computador.

Acrescenta ainda em sua obra, fazendo uma citação de Guy Stelle, Deborah Fish Nigri (1992, p. 45) descreve em 7 conceitos sobre o termo:

> 1) pessoa que tem prazer em aprender detalhes do sistema de um computador e explorar sua capacidade;
> 2) pessoa que se entusiasma com o programar ou desenvolver programa de computador;
> 3) pessoa capaz de apreciar o valor de explorar o sistema;
> 4) pessoa capaz de programar rapidamente;
> 5) perito em um determinado programa de computador;
> 6) especialista em geral;
> 7) pessoa maliciosa que tenta descobrir informações através de meios fraudulentos ou ilegais, por exemplo, apropriar-se de senhas de outrem.

Este nome surgiu no Instituto de Tecnologia de Massachusetts (*Massachusetts Institute of Technology*). Era utilizado para definir àqueles estudiosos da computação, que passavam horas e horas pesquisando nos laboratórios do Instituto.

Há que se fazer uma diferenciação entre o *hacker* e o *cracker*. O hacker, ou também conhecido como hacker ético ou inocente é aquele que procura soluções para os problemas que o *cracker* criou. Eles podem entrar e sair do sistema sem sequer serem percebidos. Liliana Minardi Paesani (2000, p. 37) diz que eles "invadem sistemas, corrigem falhas de segurança e instalam uma porta única e controlada, com o propósito de garantir a exclusividade no acesso". Contudo, Deborah Fisch Nigri (1992, p. 45) esclarece que apesar do nome, o hacker inocente não é tão bonzinho como parece: "Eles possuem a habilidade de se apropriar de informações, valores e dados. Além disso, podem, inadvertidamente, causar danos aos sistemas, adulterar ou destruir um arquivo, ou parte dele, mover dados, transferir balanços etc".

Por outro lado, o *Cracker* é o *hacker* malicioso. Lílian Minardi Paesani (2000, p. 37) afirma que "é o invasor destrutivo que tenta invadir na surdina os portões de entrada dos servidores internet, que são a melhor forma de disseminar informações". Completa Alexandre Jean Daoun (2000, p. 209) que "é o hacker malicioso, ou seja, possui grande conhecimento técnico e utiliza tal conhecimento para praticar crimes".

Antigamente a imagem de um *cracker* era somente aqueles que tinham um conhecimento exacerbado sobre o assunto informática é que poderia praticar essa conduta. Hoje não é essa a realidade. Um conhecimento básico sobre o assunto é claro que se mostra necessário, no entanto, qualquer pessoa que queira se aventurar nessa ilicitude consegue. Há até mesmo na rede online passos para como se atingir tal "façanha". Existem professores e muitos alunos e, dessa forma, mais e mais criminosos, uns mais habilidosos, outro menos. Existem aqueles que invadem grandes empresas, e outros que invadem um simples computador doméstico.

No Brasil, tal conduta passou a ser vista aproximadamente em 1988, onde se notaram invasões em sistemas de grandes bancos e do órgão público. Nos

dias atuais, há invasões dos mais variados sistemas, desde universidades, quanto acesso indevido a grandes cofres públicos.

O preocupante é saber que muitos desses delinqüentes buscam nem sempre uma vantagem material, mas sim a satisfação em saber que conseguiram burlar um sistema, ter contato com o proibido.

Portanto, um pequeno conhecimento em programações e sistemas operacionais permite chegar a enormes prejuízos à sociedade. A questão fundamental não é saber se houve uma invasão de um hacker ou não, mas sim saber ao certo como agiu o delinqüente, pois isto vai além das tipificações normais como visto alhures.

5.2 Sujeitos passivos

Para definição dos sujeitos passivos dos crimes informáticos não há muito que se analisar. Será de um modo geral, aqueles que tiverem lesão ou perigo de lesão de um bem jurídico tutelado por nosso Direito, podendo ser a própria pessoa, tanto física quanto jurídica, o Estado, ou qualquer outro que tiver sofrido a lesão, dependendo então da natureza da conduta ilícita em questão.

Um dos problemas que se pode citar é que para esse tipo de crime, a vítima pode preferir ao silêncio, o que impediria uma apuração real das possibilidades de atuação do ofensor, prejudicando a criação de normas eficientes para solução desses ilícitos.

Somente a título de observação, tem-se conhecimento de que muitos bancos estão ressarcindo aos seus clientes os danos decorrentes desse tipo de ação logo que têm conhecimento do ocorrido, ou quando possível, antes mesmo de seu cliente perceber qualquer alteração em sua conta, privando sua imagem frente à sociedade.

6 SISTEMA INFORMÁTICO E SEUS ILÍCITOS PENAIS

6.1 Fraude nos dados armazenados

Analisando-se as considerações anteriores, percebe-se que o sistema informática é utilizado tanto como um objeto material, como também como um meio para um determinado fim pretendido pelo autor.

Como já visto, a informação pode ter diversas traduções, dependendo-se para onde a ofensa é dirigida, ou seja, pode ser traduzida em patrimônio, honra etc. Quando essa afetação ocorre pelo sistema informático, o ilícito é nesse meio cometido.

Não é difícil perceber que quando o sistema informático é utilizado para enganar a vítima, seja por páginas da Internet ou conversas conectadas à rede ou por meio de outro computador, o estelionato está presente. Nestes casos, a utilização do sistema é apenas como um instrumento.

A discussão maior dessa fraude se dá na possibilidade ou não de haver furto e estelionato. A doutrinadora Deborah Fisch Nigri (1992, p. 40-48) defende que:

> O Código Penal de 1940 não é ferramenta ideal para tratar desse tipo de delito. Tornou-se difícil a punição dos infratores ainda que se tente aplicar o crime de estelionato ao acesso a extrato bancário de terceiros, ou a apropriação indébita, a invasão de domicílio, ou ao crime de furto.

Acrescenta ainda ser preciso primeiramente verificar que bem é tal informação no sistema informático, pois diz ser “um bem intangível especial que merece tratamento autônomo por tratar-se de um bem tão valioso quanto um bem corpóreo”.

Ao se falar nesse tipo de fraude, há que ser lembrado que foi somente pela ordem do infrator que o ato foi executado pelo computador. Isto levaria a uma idéia de ser furto. No entanto, o computador é mero empregado do homem, o que

faz com que seja facilmente enganado por uma pessoa que contenha a senha pessoal da vítima. Estaria caracterizado um estelionato quando o computador mostrasse as informações da vítima. Apesar de caracterizados danos à vítima, não se pode falar em estelionato, já que o enganado fora o computador, e, para caracterização daquele, seria necessária a indução ou manutenção da vítima em erro, e esta não teve participação pessoal na cena do crime.

No caso de transferência de dados de uma conta bancária para outra, o fim do agente é se apoderar das informações contidas naquela, independentemente de ser para si mesmo ou para outrem. O objeto material neste caso é a informação que foi transferida pelo sistema informático. No entanto, essa informação se representa materialmente em patrimônio.

Daí surge um motivo pelo qual não se reconheça o furto nos crimes cometidos por esse meio, já que se considera a informação como sendo um bem imaterial, e, desta forma, impossível de ser apreendida como objeto, não caracterizando a coisa (requisito do crime de furto).

Porém, no caso da conta bancária como citado anteriormente, a informação é representada em patrimônio. É então um bem material, representado em bits, podendo ser então objeto de furto. Conclui-se, portanto, que quando referentes a patrimônio, as fraudes de dados pertencerão aos crimes contra o patrimônio.

Luiz Regis Prado (2002, p. 368) diz que:

> A subtração pode ser executada mediante a apreensão direta da coisa, com o emprego de instrumentos – ou através de interposta pessoa (autoria mediata), sendo irrelevante que seja praticada na presença ou ausência da vítima (delito de forma livre).

Postas essas considerações, verifica-se que não há um meio específico para ser praticado o crime de furto. Assim, é possível considerar possível a prática desse delito no sistema informático, exigindo-se somente que o objeto (patrimônio) esteja representado em bits.

Seguindo o mesmo raciocínio, seria possível o crime de estelionato por esse meio, já que se as informações forem representadas em bits, poder-se-ia

induzir ou manter alguém em erro, por meio ardil, artificioso, ou qualquer outro meio fraudulento.

No entanto, é preciso analisar o modo que tal ação fora executada. Para que o agente obtenha acesso às informações traduzidas em patrimônio, deve também ter o acesso ao banco de dados que contém estas informações, através de comandos específicos para isso. O ponto que se deve verificar é a forma que ele conseguiu estes comandos. Ou seja, o agente pode ter se utilizado de meios fraudulentos, por ter adquirido a senha por qualquer outro meio, ou por falha operacional.

Quando por meio fraudulento, o agente utiliza-se de conhecimentos técnicos para burlar o sistema. Já nas outras hipóteses, ele consegue o acesso normal, e consegue transferir as informações como se fosse um usuário permitido. No primeiro caso, por meio de comandos não autorizados, ele consegue o acesso. Para caracterização do estelionato, seria necessária a obtenção de vantagem, induzindo ou mantendo a vítima em erro, mas nesta hipótese, há modificação dos dados sem que a pessoa esteja em erro.

Para que haja tipicidade objetiva do estelionato, se não houver o induzimento ou a manutenção da vítima em erro, não há que se falar em prática de estelionato. Luiz Regis Prado (2000, p. 502) esclarece que “A ação deve gerar na vítima um estado de ânimo propício à concreção da vantagem ilícita objetivada pelo agente”. O bem jurídico deve ser entregue ao agente pela vítima enganada.

Portanto, se não for por erro que a pessoa agiu, não se pode falar que houve o delito de estelionato.

Como Projetos de Leis existentes, podemos citar o n. 76/2000 e o 1.713/1996. No artigo 1º, parágrafo 2º do Projeto de Lei 76/2000 descreve-se o crime contra o patrimônio pelo uso irregular da informática, onde o agente altera ou transfere valores de contas bancárias. Há claramente uma falha nesta regulamentação, já que não se define ao certo qual conduta se deve punir. Outra irregularidade encontra-se no artigo 28, do Projeto de Lei n. 1.713/1996, o qual descreve a conduta de quem consegue acessar o sistema ou então à rede de instituição financeira com o intuito de transferir fundos, dinheiro, créditos ou aplicação de terceiros, seja para si ou para outrem. Nessa descrição, qualquer

pessoa que obtenha o acesso, ainda que regularmente, estará cometendo o ilícito mencionado.

Dessa forma, nota-se novamente a falta de definições precisas para a tipificação das condutas ilícitas por meio da informática.

6.2 Acesso não autorizado

O acesso não autorizado pode significar uma primeira etapa para grande parte dos crimes que utilizam a informática como meio. Pode-se citar como exemplo o crime de pirataria informática, onde há cópias de certos programas. Nesse caso, o agente pretende obter uma cópia de um programa do computador, porém, nota-se primeiro que ele obteve um acesso irregular ao sistema, para só depois se pensar em uma lesão ao direito do autor.

A preocupação inicial é quanto à inserção ou alteração de dados contidos no sistema informático. Depois, há que se falar na variedade de objetivos que o agente pode ter ao conseguir o acesso não autorizado, podendo até mesmo não buscar nenhum propósito específico, satisfazendo apenas sua curiosidade, ou um modo de se orgulhar pelo êxito de sua operação.

Existem programas, denominados *crackers*, que permitem ao invasor descobrir as senhas utilizadas pelo usuário, sendo possível acessar o sistema como se fosse ele.

Para isso, há uma espécie de programa, conhecida como *sniffers*, os quais são capazes de fazer um rastreamento no tráfego de toda a rede na busca de certas cadeias numéricas ou pacote de dados, os quais são disponibilizados ao infrator através da tela do computador ou de registros (*logs*) e consegue então conhecer as senhas que o usuário usa.

Ivette Senise Ferreira (2000, p. 221-222) defende que para esse tipo de conduta, não há uma tipificação específica, havendo a necessidade de enquadramento em normas já existentes, como violação de correspondência ou

ainda no crime de dano, lembrando-se de que a legislação atual não está adequada como deveria para solucionar tal questão.

Antes mesmo de se reconhecer um crime de dano ou de violação de correspondência, é preciso observar qual é o tipo de informação que consta no arquivo acessado indevidamente. Sabe-se que depende da natureza dessa informação a remissão para uma determinada norma. Assim, se houver um acesso indevido sem que tenha um prejuízo ao proprietário da informação, não há necessidade nem sequer de intervenção penal. No entanto, se houver prejuízo ao acessar indevidamente uma correspondência, tem-se um crime contra o sigilo de correspondência, havendo proteção tanto constitucional quanto penal.

Porém, se o acesso indevido fosse a dados pessoais que se encontram armazenado em um banco de dados, apesar de ser a mesma ação, o bem jurídico lesionado seria outro, mas que também possui proteção de nossa Constituição, a qual dispõe em seu artigo 5º, "caput" e inciso X que:

> **Artigo 5º, "caput" –** Todos são iguais perante a Lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos, seguintes:
>
> Inciso X – são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurando o direito à indenização pelo dano material ou moral decorrente de sua violação.

Preocupando-se com a violação ao Direito de Intimidade, existe o Projeto de Lei 3.943/1997, que pretende acrescer no Código Penal, em sua parte especial um novo capítulo denominado "Dos Crimes contra a Privacidade". Dois são os artigos por ele estipulados:

> **Artigo 145-A.** Violar mediante processo tecnológico ou qualquer outro meio, a intimidade alheia, sem o consentimento do titular do direito. Pena – detenção de seis meses a dois anos.
>
> **Parágrafo único.** Na mesma pena incorre aquele que indevidamente revela ou divulga imagem, escrito, palavra ou fato integrante da intimidade alheia, ainda que legitimamente conhecidos.

O que está em jogo neste dispositivo é a intimidade alheia que se encontra ameaçada. Àquele que violar, por qual meio que seja a intimidade alheia, estará incurso neste artigo.

> **Artigo 145-B.** Formar, indevidamente, com dados pessoais alheios, fichário automatizado ou banco de dados. Pena – detenção, de seis meses a dois anos.
>
> Inciso I – acrescenta, altera, suprime indevidamente dados pessoais alheios em fichário automatizado ou banco de dados;
>
> Inciso II – utiliza processo tecnológico ou qualquer outro meio que possibilite acesso indevido a fichário automatizado ou banco de dados;
>
> Inciso III – fornece, indevidamente, a terceiro, dados de fichário automatizado ou banco de dados;
>
> Inciso IV – divulga, indevidamente, dados pessoais de fichário automatizado ou banco de dados.

Sobre este último artigo, Rita de Cássia (2002, p. 91) comenta que "A informática tem suas peculiaridades de linguagem, assim, dever-se-ia usar o verbo armazenar que está em consonância com a matéria que se pretende regular".

Um outro Projeto de Lei a ser citado é o 1.713/96, o qual em seu artigo 18 estabelece que "Obter acesso, indevidamente, a um sistema de computador ou a uma rede integrada de computadores: Pena – detenção de 3 (três) meses a 6 (seis) meses ou multa".

Há ainda duas qualificadoras nos casos em que:

> **Parágrafo 2.º** Se, além disso, resulta prejuízo econômico para o titular: Pena – detenção de 1 (um) a 3 (três) anos, e multa.
>
> **Parágrafo 3.º** Se o acesso tem por escopo causar dano a outrem ou obter vantagem indevida: Pena – detenção de 2 (dois) a 4 (quatro) anos, e multa.

O que se nota nesses dispositivos, é um exagero nas várias colocações do elemento normativo, mostrando-se o legislador inexperiente ainda para tratar deste assunto, o qual se deve restringir tão somente a delitos que não haja disposição qualquer em nosso ordenamento, criando-se leis suficientes para conter os ilícitos, portanto, sem exageros.

Falando-se ainda no assunto de tutela à intimidade, tem-se outro projeto de Lei, n. 152/91,o qual dispõe no artigo 2º a punição ao agente que viola o sigilo de dados com o acesso indevido à informação constante no sistema ou então em outro suporte físico, sem permissão do proprietário. No parágrafo 1º há uma qualificadora ainda se caso o acesso for por utilização indevida de senha ou então de identificação magnética de um terceiro. Apesar de não constar no "caput" a descrição de uso não permitido de senha, não há como acontecer o delito sem que ocorra isto. Desta forma, não há necessidade desse parágrafo. Dispõe ainda o parágrafo segundo a possibilidade de haver um estelionato qualificado "Se o acesso resultar vantagem econômica indevida, em detrimento ao titular do sistema". No entanto, essa colocação não se faz verdadeira, uma vez que não há sequer uma pena pré-estabelecida para o tipo descrito.

6.3 Dano a programa de computador ou a dados nele contidos

Neste tipo de crime, o agente quer destruir, inutilizar ou alterar um programa de computador com a invasão por vírus, vermes, dentre outros métodos, que, por não serem conhecidos pelo sistema, acabam por atrapalhar o funcionamento normal daquele. São sabotagens informáticas, que permitem até o contato com o banco de dados. Neste caso, o invasor pode ter diversas finalidades, seja uma curiosidade, espionagem de grandes empresas industriais, ou comerciais, as quais só são possíveis através do uso do sistema informático.

O tipo mais conhecido é o cavalo de tróia, já citado anteriormente. Ocorre a inclusão em algum programa que já existe de outros comandos, podendo-se então alterá-lo sem destruição alguma.

Quando o agente contamina o sistema levando à alteração, exclusão ou à inutilidade, pode-se considerar como sendo um dano, tipificado no artigo 163, do Código Penal, onde a tipicidade objetiva será exatamente estas: alteração, deterioração, destruição de coisa alheia.

Quanto às modalidades em que essa conduta é aplicada existem alguns posicionamentos doutrinários. Para Julio Fabbrini Mirabete (1999, p. 270)

destruir significa “eliminar, desfazer, desmanchar, demolir”. Luiz Regis Prado (2000, p. 448) acrescenta que “é quando a coisa deixa de subsistir na sua individualidade, ainda que subsista materialmente”. Inutilização já seria a perda, ainda que temporária, da funcionalidade a que se destina a coisa. E, por fim deteriorar é desvalorizar, estragar, diminuir a utilidade da coisa.

É claro que independente de qual modalidade é aplicada, o bem jurídico lesado será o patrimônio, já que tanto o software, quanto o hardware podem ser objeto material desse tipo de delito (dano), já que podem ser destruídos (queimado, sofrer um curto circuito etc), ou então inutilizados, seja por vírus ou por outras formas de contaminação do sistema, que impeçam um bom funcionamento de seus atributos.

Ivette Senise Ferreira (2000, p. 219) não se conforma com a tutela provida a esse tipo de contaminação por programas ilícitos, já que não considera suficiente para atender todas as necessidades desse tipo de problema. Exemplifica uma das possibilidades, como sendo a ausência de tutela aos projetos intelectuais, como uma tese, monografia, pesquisas importantíssimas, que podem ser perdidas em questão de segundos.

O fato é que não depende de estarem ou não armazenados em um sistema informático, diferente do papel que devem ser protegidos. O tratamento caso fosse queimada toda a dissertação de uma pessoa, ainda que no papel, deveria ter a mesma proteção. Não há que se falar então em uma ausência de tutela quanto ao modo em que está armazenada a produção intelectual, já que deve ser inserido nessa modalidade.

Importante se faz lembrar que não é só a destruição ou então a inutilidade do equipamento que deve ser destacado. Poderá haver conseqüências maiores e mais graves do que isto, ocorrendo, por exemplo, transferências, alterações, que lesionam um bem jurídico diferente de um simples suporte eletrônico.

Visando-se a contenção de atos que venham destruir ou alterar um programa de computador, foi criado o Projeto de Lei 597/91, onde é estabelecido que:

> **Artigo 1.º** Pratica crime quem, objetivando prejuízo de alguém, a um sistema, a computador, a equipamento que acompanha o sistema ou a computador:
>
> a) destrua ou altere, dolosamente, ou utilize de modo indevido, programa de computador a que tem acesso;

Neste dispositivo já se observa uma impropriedade nos termos utilizados, visto que cria a possibilidade de haver prejuízo a seres inanimados, como um sistema, computador, equipamentos, quando na verdade, estes só devem ser atribuídos a seres humanos, a pessoas. O programa, sistema, computador podem sofrer alterações, danos, destruição, porém, quem sofre o prejuízo é a pessoa que se serve deles.

Postas essas considerações, nota-se mais uma vez, que existem projetos de regulamentação, mas que seus criadores não se atentaram para certas peculiaridades desse meio, ora utilizando-se de termos inadequados, ora esquecendo-se de utilizar qualquer expressão ideal para os crimes informáticos.

6.4 Quebra do sigilo das correspondências

Como já dito alhures, o artigo 5º, inciso X da Constituição Federal garante "a intimidade, a vida privada, a honra e a imagem das pessoas, assegurando o direito à indenização pelo dano material ou moral decorrente de sua violação". Assim, o indivíduo tem o direito de se manter reservado no plano do direito à intimidade.

René Ariel Dotti (1980, p. 69) afirma que a intimidade é "a esfera secreta da vida do indivíduo na qual este tem o poder legal de evitar os demais". No mesmo sentido Paulo José da Costa Junior (1995, p. 49) diz que "Enquadra-se entre os direitos que constituem um atributo da personalidade, caracterizando-se por ser absoluto, indisponível e por não se revestir de natureza patrimonial".

A pretensão de querer a intimidade é, portanto, não desejar a participação de outras pessoas em sua vida privada. Há que se destacar que a vida privada se difere ao direito à intimidade, visto que este se mostra como uma espécie

daquela. Diz Luciana Fregadolli (1998, p. 42) que “a intimidade seria um círculo concêntrico e de menor raio que a vida privada”.

No direito à intimidade, dois interesses são tutelados: interesse de que ela não seja agredida, e outro de que não seja divulgada. Luciana Fregadolli (1998, p. 63) lembra que a Constituição Federal: “Garante o direito ao indivíduo de obstar a intromissão de estranhos na sua vida privada e familiar, assim como o de impedir-lhes o acesso a informações sobre esta área da manifestação existencial do ser humano”.

Vários são os desdobramentos desse direito, seja a inviolabilidade da correspondência, sigilo bancário, segredo profissional, dentre outros, englobando-se ainda documentos, cartas confidenciais etc. O objeto então a ser protegido é o segredo, que foi violado ou divulgado por quem não era permitido.

Com relação à Informática, no que tange ao direito à intimidade, o primeiro assunto a ser discutido, refere-se aos e-mails. Quanto à violação desse tipo de comunicação, Carla Rodrigues Araújo de Castro (2001, p 22) defende que deveria ser aplicada a regra da especialidade nesse caso, alegando que o artigo 10 da Lei 9.296/96 deve prevalecer sobre o artigo 151, do Código Penal, uma vez que aquele descreve as condutas realizadas por meio informático e, o e-mail seria uma correspondência eletrônica feita por este.

Porém, esse raciocínio não parece mais coerente, já que o artigo 10 da Lei citada utiliza a expressão “interceptar” para tipificar objetivamente o delito. Grande parte da doutrina tem entendido que tal verbo envolve o acesso sem autorização, visto que no artigo mencionado, o verbo teria o significado de captar, conhecer o conteúdo, ou então, como Sérgio Marcos Roque (2000, p. 321) diz “importa em escuta direta e secreta das mensagens, captando-se a conversa no momento mesmo em que se desenvolve, sem o conhecimento de pelo menos um dos interlocutores”.

Para se chegar o destinatário exato, essa mensagem eletrônica passa por vários caminhos, sendo longos e inseguros, seja nos servidores responsáveis pelo acesso à internet, ou pelos provedores. É possível então que se modifique totalmente a informação antes que ela chegue ao seu destinatário final.

Luiz Regis Prado (2000, p. 324) afirma que “correspondência é toda comunicação interpessoal realizada por meio capaz de transmitir o pensamento”. Dessa forma, não é somente através de carta que ela se faz presente; poderá ser por qualquer outro meio que se possa comunicar, seja por rádio, telefone, televisão etc. No caso do sistema informático, ela está grafada em bits, mas não deixa de ser um veículo de comunicação.

Uma outra questão importante é analisar o conteúdo que o artigo 151, do Código Penal expressa: “Devassar indevidamente o conteúdo de correspondência fechada, dirigida a outrem: Pena – detenção, de 1 (um) a 6 (seis) meses, ou multa”.

A expressão “fechada” neste artigo pode tanto se referir às correspondências escritas, como às realizadas por meio eletrônico, pois não é necessário que seja aquela lacrada em envelope, visto que uma mensagem eletrônica pode também estar “fechada”.

Como bem explica Luiz Regis Prado (2000, p. 325):

> O devassamento pode se dar através da abertura da correspondência ou de outro processo que possibilite a leitura do conteúdo sem que para isto se tenha que romper o envelope ou envoltório da comunicação, por exemplo, efetuar a leitura colocando a correspondência contra a luz.

Para o sistema informático, a abertura dessa mensagem eletrônica se dará por meio de software específico que realizará essa tarefa mediante senha do usuário.

Diante do exposto, pode-se considerar que o sigilo das mensagens eletrônicas (e-mails) encontra proteção no artigo 151 do Código Penal, onde a conduta deverá se restringir ao ato de devassar somente, visto que acrescentar, modificar, suprimir informações não encontra disposições expressas neste artigo, faltando tipicidade objetiva para punição daquelas.

A título de observação, ainda com relação ao sigilo, pode-se citar o segredo profissional. Tal conduta encontra tipificação no artigo 152 do Código Penal, onde:

> **Art. 152.** Abusar da condição de sócio ou empregado de estabelecimento comercial ou industrial para, no todo ou em parte, desviar, sonegar, subtrair ou suprimir correspondência, ou revelar a estranho seu conteúdo: Pena – detenção de 3 (três) meses a 2 (dois) anos.

Portanto, àquele que, aproveitando-se da condição de sócio ou empregado, realizar alguma dessas condutas previstas através do meio informático também estará incurso neste artigo, onde a correspondência deverá estar grafada em bits, ou estar armazenada neste suporte eletrônico.

7 CONCLUSÃO

Ao longo desses anos, a evolução tecnológica é surpreendente. Novas tecnologias são criadas todos os dias. Uma das mais visíveis é a evolução da informática.

A informação antes passada através da fala, gestos, sinais, hoje é transmitida por veículos mais rápidos, como a televisão, o rádio, e nos dias atuais, a internet. Pode-se dizer que poucos segundos após certos acontecimentos, já se encontrarão estampados na rede mundial de informática.

Na medida em que cresce a informática, aumenta-se a preocupação com o conteúdo nela armazenado. Pode-se dizer que juntamente com ela, criou-se um mundo virtual, onde todas as informações são gravadas por meio de bits, ou seja, por uma linguagem de máquina.

Toda informação digitalizada, ou seja, por meio de números binários é chamada de virtual. Porém, não é por isso que deve se considerar a informação somente como bem imaterial, dependendo, portanto, da natureza do bem jurídico tutelado em que ela se transforma.

Com esse crescimento acelerado do meio informático, os operadores do Direito começaram a se preocupar, já que pode ocorrer tanto o bom quanto o mau uso daquele, interferindo então em vários ramos do Direito, como no Direito do Consumidor, Direito do Trabalho, Comercial etc.

Desta forma, é preciso que se analise cada peculiaridade desse novo instrumento de prática ilícita, para que se possa coibir a utilização inadequada desse meio, seja criando-se novos dispositivos, ou se utilizando daqueles já existentes por meio de uma adequação típica.

Para o Direito Penal, o que se pretende estudar são as práticas delinqüentes no uso da informática. Vários doutrinadores tentaram nomear essa nova prática ilícita, porém, deve-se ter cautela ao considerar as condutas como delito ou crime, já que para isso, é necessário que haja definição legal. Portanto, o termo mais adequado para tal prática seria crime informático, que pode ser

considerado a conduta típica, antijurídica e culpável, realizada através de dispositivos pertencentes ao sistema informático, não importando para esse conceito, o fim que o delinqüente almeja.

A utilização do sistema de forma irregular pode ser tanto como objeto material da prática ilícita, como um instrumento único para realização de um determinado delito, ou ainda mais um meio para o cometimento de diversos crimes.

É preciso que se verifique a natureza da informação armazenada no computador, já que esta pode ser objeto material de condutas delinqüentes. Dependendo do conteúdo dela, a lesão será a um determinado bem jurídico. As informações, portanto, podem ser traduzidas em bens jurídicos diferentes, dependendo do que contém a mensagem.

Existe uma diversidade de técnicas para invasão de um sistema informático, podendo ser por acesso local, acesso remoto, engenharia social, vírus, cavalo-de-tróia, dentre outros.

Antigamente acreditava-se que para ser um hacker, ou seja, sujeito ativo dessa prática delituosa necessitava ter conhecimentos profundos de linguagem e técnicas dessa área. Porém, atualmente já se percebe que não há nenhuma qualidade especial para isso. Páginas da internet até mesmo ensinam passo a passo para essa prática. O sujeito passivo, igualmente, não tem nenhuma característica especial; será aquele que teve um bem jurídico atingido por meio de invasão de um delinqüente.

Na prática desse tipo desse delito, necessariamente deve haver um sistema informático, seja o hardware ou o software. É preciso diferenciá-los, na medida em que o Hardware pode tanto ser tutelado pelo Direito de Propriedade Industrial, como também o equipamento onde se consegue realizar diversas atividades, podendo então ser objeto material dos crimes de furto, dano etc.

Já o Software é tutelado pelo Direito de autor, o dono da criação intelectual. Tendo em vista às possíveis condutas ilícitas contra ele, surgiram as Leis n. 9.609 e 9.610 de 1998, as quais asseguram o direito de autor pela criação dos programas de computador, bem como sua comercialização, e pune algumas condutas.

Há divergência doutrinária com relação às condutas ilícitas contra o sistema informático e a própria informação. Deve-se analisar o conteúdo dela, e qual a execução contra ela ou contra um programa de computador fora cometido.

Na fraude por manipulação de dados armazenados, a questão principal é a discussão sobre a possibilidade da prática de haver estelionato e furto. O furto mediante fraude caracteriza-se pela invasão do agente ao banco de dados por meios não permitidos, ou descobre a senha por uma falha do sistema operacional ou então por qualquer outro meio ilícito. Já o estelionato poderá ocorrer quando através da informática, o agente consegue fazer com que o operador do sistema altere, suprima ou transferira dados sem perceber que há fraude, entregando o seu patrimônio ao delinqüente.

O acesso não autorizado ao sistema pode ser apenas um início para o cometimento de outros delitos, ou se encerrar nele mesmo. Não há tipificação legal acerca do assunto, a não ser o artigo 335, do Código Penal que tipifica somente ação contra o sistema da Administração Pública.

Quanto à violação de correspondência, deve ser citado o e-mail, o qual pode ser considerado como uma, já que também guarda informação e pode ser aberto e fechado da mesma maneira que uma carta, diferenciando-se somente na forma de representação da informação, que, no caso deste, será por meio de bits. Há tipificação legal tão somente à questão de devassar o conteúdo, ficando fora as condutas de suprimir, alterar, acrescentar algo na mensagem eletrônica.

Como se pôde ver, a evolução tecnológica provocou uma mudança na sociedade rapidamente, o que obrigou o Direito a acompanhar, ou pelo menos tentar acompanhar o ritmo dessas evoluções, adequando-se quando possível, às normas já vigentes. Para criação de novas leis, portanto, deve-se ter o máximo de cuidado para não ter excessiva regulamentação.

O que se verifica nas últimas tentativas de legislação é uma inexperiência por parte dos legisladores. Para a informática, principalmente, poderia haver uma restrição àquelas normas já existentes, onde o uso desse sistema fosse para majorar a pena, ou qualificação desta. Porém, há que se lembrar que existem certas condutas que não encontram nenhuma ressonância típica, justificando-se então a criação de alguns dispositivos para rechaçá-las.

Portanto, nota-se claramente nesses casos, a necessidade de criação de normas flexíveis, adequável a cada momento cultural, para que não seja preciso novos tipos todos os dias. Seria mais sensato que o legislador inserisse esses tipos dentro do nosso Código Penal já existente, como já se verifica em outros países.

Por fim, mostra-se necessário então uma conscientização dos operadores do Direito, em especial dos legisladores que, na velocidade em que a tecnologia se evolui, deve haver juntamente um acompanhamento por nossos dispositivos legais, sendo criados novos quando precisos, ou adequados quando possíveis para que continue havendo a paz social em nosso país que pela lei maior nos é garantido.

BIBLIOGRAFIA

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

BRASIL. Lei n. 9.609, de 19 de fevereiro de 1998. Dispõe sobre a Propriedade Intelectual de Programa de Computador, sua Comercialização no País e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/L9609.htm>. Acesso em 15 out. 2008.

BRASIL. Lei n. 9.610, de 19 de fevereiro de 1998. Altera, Atualiza e Consolida Legislação sobre Direitos Autorais e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/L9610.htm>. Acesso em 15 out. 2008.

BRASIL. Lei n. 9.296, de 24 de julho de 1996. Regulamenta o inciso XII, parte final, do artigo 5º, parte final da Constituição Federal. Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/L9296.htm>. Acesso em 17 out. 2008.

BRASIL. Lei n. 9.983, de 14 de julho de 2000. Altera o Decreto-Lei nº 2.848, de 7 de Dezembro de 1940 – Código Penal e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/L9983.htm>. Acesso em 17 out. 2008.

BRASIL. **Código Penal**. Decreto-lei nº 2.848, de 7 de Dezembro de 1940. <http://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del2848.htm>. Acesso em 20 out. 2008.

CASTRO, Luiz Fernando Martins. **O Direito da Informática**. Dissertação de Mestrado em Direito (USP). São Paulo, 1992.

CHAVES, Antônio**. Aspectos jurídicos da juscibernética. Direito de autor do programador.** Brasília: Revista de Informação Legislativa do Senado Federal, ano 19, n. 73, jan – mar 1982.

CORRÊA, Gustavo Testa. **Aspectos jurídicos da internet.** São Paulo: Saraiva, 2000.

COSTA JUNIOR, Paulo José da. O **direito de estar só: Tutela Penal da Intimidade**. São Paulo: Revista dos Tribunais, 2ª edição, 1995.

DAOUN, Alexandre Jean. **Crimes informáticos. Direito eletrônico: a internet e os tribunais.** Bauru: Editora Edipro, p. 203-221, 2001

FERNANDES, Antonio Scarance. **Crimes praticados pelo computador. Dificuldades na apuração dos fatos.** Maringá: Revista de Ciências Jurídicas, ano 3, n 1, 1999.

FERRREIRA, Aurélio Buarque de Holanda. Minidicionário da língua portuguesa. 3ª ed. Rio de Janeiro: Nova Fronteira, 1993.

FERREIRA, Ivette Senise. **A criminalidade informática. Direito & Internet: aspectos jurídicos relevantes**. Bauru: Edipro, p. 207-237, 2000.

FREGADOOLI, Luciana. **O Direito à intimidade e a prova ilícita.** Belo Horizonte. Editora Del Rey, 1998.

GOUVÊA, Sandra**. O Direito na era digital: crimes praticados por meio da informática.** Rio de Janeiro. Editora Mauad,1997.

JUNIOR, João Marcelo de Araújo**. Computer-crime. Conferência Internacional de Direito Penal.** Rio de Janeiro: Editora Anais, p. 460, 1988.

MARSHALL, Garry. **Iniciação à tecnologia da informação.** Lisboa: Editora Presença, 1984.

MARTINHO, Antonio Anselmo. **Informática Jurídica Hoje.** Revista Oficial do Tribunal de Alçada Criminal do Estado de São Paulo, vol 91, ano 21, jan – mar, p. 7 a 22, 1987.

NIGRI, Deborah Fisch. **Crime e informática: um novo fenômeno jurídico**. Revisto Trimestral de Jurisprudência dos Estados, n 100, ano 16, p. 40-48, 1992.

PAESANI, Lilian Minardi. **Direito e internet: liberdade de informação, privacidade e responsabilidade civil**. São Paulo: Atlas, 2000.

PAIVA, Mario Antonio Lobato de. **Os Institutos do Direito Informático.** Disponível em: < http://www.alfa-redi.org/rdi-articulo.shtml?x=1550>. Acesso em: 20 set. 2008.

PÉREZ LUÑO, Antonio Enrique. **Ensayos de informática jurídica.** México: Distribuciones Fontamara, 1994.

PRADO, Luiz Regis. **Curso de Direito Penal brasileiro v.1**: Parte Geral. 3ª ed. São Paulo: Revista dos Tribunais, 2002.

_____. **Curso de Direito Penal brasileiro v. II**: Parte Especial. São Paulo: Revista dos Tribunais, 2000.

_____. **Curso de Direito Penal brasileiro v. III**: Parte Especial 2ª ed. São Paulo: Revista dos Tribunais, 2001.

REIS, Maria Helena Junqueira. **Computer crimes: a criminalidade na era dos computadores.** Belo Horizonte: Del Rey, 1996.

ROQUE, Sérgio Marcos. **Crimes de informática e investigação policial**. São Paulo: Revista dos Tribunais, n. 718, p. 309-333, 2000.

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

ROSSINI, **Augusto Eduardo de Souza.** Informática, Telemática e Direito Penal. São Paulo: Memória Jurídica, 2004.

SILVA, Rita de Cássia Lopes da. **Direito Penal e Sistema Informático.** Série Ciência do Direito Penal Contemporânea - vol 4 - ed RT, 2003

VIANNA, Túlio Lima. **Fundamentos de Direito Penal Informático**: do acesso não autorizado a sistemas computacionais. Rio de Janeiro: Forense, 2003.

ANEXOS

ANEXO 1
PROJETO DE LEI 597/1991

Artigo 1º - Pratica crime quem, objetivando prejuízo de alguém, a um sistema, a computador, a equipamento que acompanha o sistema ou a computador:

a) destrua ou altere, dolosamente, ou utilize de modo indevido, programa de computador a que tem acesso;

b) abuse, por qualquer outra forma, de seu direito de acesso a computador, a sistema de computação, de transmissão de dados, ou de processamento de dados de qualquer espécie:

Pena – detenção de um a quatro anos e multa de igual valor ao proveito visado ou do risco de prejuízo da vítima;

c) utilize senha de outrem para obter acesso indevido a um sistema ou a um computador:

Pena – detenção de um ano a três anos e multa igual ao valor do proveito visado ou do risco de prejuízo da vítima.

Artigo 2º - A interferência não intencional, por negligência, imprudência ou imperícia, constitui crime culposo:

Pena – multa igual ao prejuízo causado. Mínimo de CR$ 170.000,00 (Cento e Setenta Mil Cruzeiros). Na reincidência, detenção de um a três meses e multa.

ANEXO 2

PROJETO DE LEI 152/91

Artigo 1º - Consideram-se crimes contra a inviolabilidade dos dados a sua comunicação a prática das condutas descritas nos arts. 2º e 3º desta lei.

Artigo 2º - Violar o sigilo de dados, acessando informação contida em sistema ou suporte físico de terceiro, sem autorização deste:

Pena – detenção de um a seis meses e multa.

§1º Se o acesso se faz com uso indevido de senha ou de processo de identificação magnética de terceiro:

Pena – detenção de três meses a um ano e multa.

§ 2º Se o acesso resultar vantagem econômica indevida, em detrimento ao titular do sistema, pune-se o fato como estelionato qualificado nos termos do art. 4º desta lei.

Artigo 3º - Inserir em suporte físico de dados, ou em comunicação de dados, programa destinado a funcionar clandestinamente no sistema de terceiro, causando nele efeito indesejado por seu titular:

Pena – detenção de um a seis meses e multa.

§1º Se resulta perda definitiva de informação contida no sistema:

Pena – detenção de um a seis meses e multa.

§ 2º Se, além da perda de informação, resulta prejuízo econômico para o titular do sistema:

Pena – detenção de um a três anos e multa.

Artigo 4º - A realização de conduta descrita nesta lei como meio para a prática de qualquer crime qualifica-o, agravando a pena de um sexto até a metade.

Artigo 5º - A informação ou dado constante de sistema eletrônico que, por qualquer razão, tenha relevância nas relações entre pessoas, considera-se “documento”, punindo-se sua adulteração material e ideológica nos termos do Código Penal, como qualificadora do art. 4º, desta lei.

Parágrafo único: Para fins deste artigo considera-se “documento público” a informação constante de sistema:

a) pertencente ou a serviço de órgão público da administração direta ou indireta, instituição financeira, Bolsa de Valores ou estabelecimento de ensino oficial ou reconhecido;

b) em condições de autorizar pagamento, quitação, movimentação de conta corrente ou qualquer transferência de valores;

c) destinado ao acesso público, pago ou gratuito, as informações comerciais, econômicas ou financeiras.

ANEXO 3

PROJETO DE LEI 1.713/96

Capítulo I

DOS PRINCÍPIOS QUE REGULAM A PRESTAÇÃO DE SERVIÇOS POR REDES INTEGRADAS DE COMPUTADORES

Artigo 1º - O acesso, o tratamento e a disseminação de informações através das redes integradas de computadores devem estar a serviço do cidadão e da sociedade, respeitados os critérios de garantia dos direitos individuais e coletivos, da privacidade das informações pessoais e da garantia de acesso às informações disseminadas pelos serviços da rede.

Artigo 2º - Considera-se, para efeitos desta lei:

a) Rede integrada de computadores – qualquer sistema ou conjunto de sistemas, destinados à interligação de computadores ou demais equipamentos de tratamento eletrônico, optoeletrônico ou ótico de dados com o fim de oferecer em caráter público ou privado informações e serviços a usuários que conectem seus equipamentos ao sistema.

b) Administrador de rede integrada de computadores – entidade responsável pelo funcionamento de rede de computadores, ou de parte de uma rede de computadores e pela continuidade dos respectivos serviços de rede.

c) Infra-estrutura de rede – conjunto de recursos ou serviços de telecomunicações ou de conexão de outra natureza que viabilizem o funcionamento de rede de computadores.

d) Serviços de rede – serviços essenciais ao funcionamento de rede integrada de computadores, providos pelo administrador de rede, inclusive serviços de controle de acesso, segurança das informações, controle do tráfego de informações e catalogação de usuários e provedores de serviços de valor adicionado.

e) Serviços de valor adicionado – serviços oferecidos aos usuários da rede integrada de computadores que criam novas utilidades específicas, ou novas atividades, relacionadas com o uso da rede.

f) Serviço de informação – serviço de valor adicionado caracterizado pela disseminação de informação, limitada ou não através de rede integrada de computadores.

g) Serviço de acesso a bases de dados – serviço de valor adicionado caracterizado pela coleta, armazenamento e disponibilidade para consulta de informações em base de dados.

h) Transferência eletrônica de fundos (TEF) – serviço de valor adicionado caracterizado pelo intercâmbio de ordens de crédito ou débito entre usuários de uma rede integrada de computadores, ou por operações cuja finalidade e efeito sejam a transferência de fundos de um patrimônio a outro sem movimentação efetiva de moeda, através de instruções eletrônicas.

i) Bases de dados – coleção de informações, armazenada em meio eletrônico, optoeletrônico ou ótico, que permita a busca das mesmas por procedimentos manuais ou automatizados de qualquer natureza.

j) Provedor de serviços – entidade responsável pela oferta de serviços de valor adicionado.

k) Provedor de informações – entidade responsável pela oferta de serviços de valor adicionado.

l) Usuário de rede – pessoa física ou jurídica que utiliza os serviços oferecidos pela rede integrada de computadores ou pelos provedores de serviços ou de informações através dessa rede, ou que possa, legitimamente, receber ou ter acesso a informações transportadas pela rede de computadores.

m) Controle de acesso à rede – conjunto de procedimentos de segurança estabelecidos pelo administrador da rede, a serem executados pelo usuário para ter acesso aos serviços da rede.

Artigo 3º - É livre a estruturação e o funcionamento de redes integradas de computadores e seus serviços, nos termos desta leu, ressalvadas as disposições específicas aplicáveis à sua infra-estrutura.

Capítulo II

DO CONTROLE DE ACESSO ÀS REDES DE COMPUTADORES

Artigo 4º - Toda rede de computadores cujo acesso é oferecido ao público, ou a uma comunidade restrita, gratuitamente ou mediante remuneração de qualquer natureza deverá ter um administrador de rede legalmente constituído.

Artigo 5º - O administrador de rede é responsável pelos serviços de rede e pela segurança do controle de acesso, nos termos contratuais estabelecidos com o usuário, respeitadas as disposições da Lei 8.078, de 11 de setembro de 1991, que “dispõe sobre a proteção do consumidor e dá outras providências”.

Artigo 6º - O usuário deverá empenhar-se em preservar a segurança e o segredo de suas senhas, cartões, chaves ou outras formas de acesso à rede de computadores.

Artigo 7º - Os provedores de serviços de valor adicionado poderão estabelecer procedimentos adicionais de controle de acesso a seus serviços, bases de dados ou informações.

Capítulo III

DA SEGURANÇA DOS SERVIÇOS E DAS INFORMAÇÕES NAS REDES DE COMPUTADORES

Artigo 8º - O administrador da rede e o provedor de cada serviço são solidariamente responsáveis, nos termos de suas atribuições específicas, pela segurança, integridade e sigilo das informações armazenadas em bases de dados ou disponíveis à consulta ou manuseio por usuários da rede.

Artigo 9º - O provedor de informações está sujeito às determinações e limitações estabelecidas na legislação vigente para a atividade da agência de notícias.

Artigo 10 – As disposições relativas aos serviços de transferência eletrônica de fundos são regulamentadas por disposição específica, atendidos os direitos e obrigações estabelecidos nesta lei.

Capítulo IV

DO USO DE INFORMAÇÕES DISPONÍVEIS EM REDES DE COMPUTADORES OU BASES DE DADOS

Artigo 11 – São consideradas pessoais as informações que permitam, sob qualquer forma, direta ou indiretamente, a identificação de pessoas físicas às quais elas se refiram ou se apliquem.

Artigo 12 – Ninguém será obrigado a fornecer informações e dados sobre sua pessoa ou a de terceiros, salvo nos casos previstos em lei.

Artigo 13 – A coleta, o processamento e a distribuição, com finalidades comerciais, de informações pessoais ficam sujeitas à prévia aquiescência da pessoa a que se referem.

§1º A toda pessoa cadastrada dar-se-á conhecimento das informações armazenadas e das respectivas fontes.

§2º É assegurado ao indivíduo o direito de retificar qualquer informação pessoal que julgar incorreta.

§3º Salvo por disposição legal ou determinação judicial em contrário, nenhuma informação pessoal será conservada à revelia da pessoa a que se refere ou além do tempo previsto para a sua validade.

§4º Qualquer pessoa, identificando-se, tem o direito de interpelar o prestador de serviço de informação ou de acesso a bases de dados para saber se estes dispõem de informações pessoais a seu respeito.

Artigo 14 – É proibida a coleta de dados por meios fraudulentos, desleais ou ilícitos.

Artigo 15 – Os serviços de informação ou de acesso a bases de dados não distribuirão informações pessoais que revelem, direta ou indiretamente, as origens raciais, as opiniões políticas, filosóficas, religiosas ou sexuais e a filiação a qualquer entidade, salvo autorização expressa do interessado.

Artigo 16 – Nenhuma decisão administrativa ou judicial poderá basear-se, para a definição do perfil do acusado ou da parte, apenas em dados obtidos mediante o cruzamento de informações automatizadas.

Artigo 17 – Somente por ordem judicial e observados os procedimentos e a legislação cabíveis poderá haver cruzamento de informações automatizadas com vistas à obtenção de dados sigilosos.

Capítulo V

DOS CRIMES DE INFORMÁTICA COMETIDOS EM DECORRÊNCIA DA UTILIZAÇÃO DE COMPUTADOR OU EQUIPAMENTO DE INFORMÁTICA EM REDES INTEGRADAS

Artigo 18 – Obter acesso, indevidamente, a um sistema de computador ou a uma rede integrada de computadores:

Pena – detenção de 3 (três) meses a 6 (seis) meses ou multa.

§1º Se o acesso se faz por uso indevido de senha ou de processo de identificação magnética de terceiro:

Pena – detenção de 1 (um) a 2 (dois) anos, e multa.

§2º Se, além disso, resulta prejuízo econômico para o titular:

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

§3º Se o acesso tem por escopo causar dano a outrem ou obter vantagem indevida:

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

§4º Se o sistema ou rede integrada de computadores pertence a pessoa jurídica de direito público interno, autarquias, empresas públicas, sociedades de economia mista, fundações instituídas ou mantidas pelo Poder Público e serviços sociais autônomos, a pena é agravada em um terço.

Artigo 19 – Apropriar-se indevidamente de informações, de que tem a posse ou a detenção em rede integrada de computadores:

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

Parágrafo único: Aumentam-se em um terço as penas se as informações são copiadas ou transferidas a outrem.

Artigo 20 – Obter segredos empresariais ou informações de caráter confidencial em sistema ou em rede integrada de computadores, com o intuito de causar danos financeiros ou obter vantagem econômica para si ou para outrem:

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

Parágrafo único: Aumentam-se em um terço as penas se as informações são copiadas ou transferias a outrem.

Artigo 21 – Apropriar-se indevidamente de valores, de quem tem a posse ou a determinação, através da manipulação de qualquer sistema de processamente de dados obtendo assim vantagem econômica para si ou para outrem:

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

Parágrafo único: Se resulta obstrução permanente ou distúrbio grave:

Pena – reclusão, de 4 (quatro) a 6 (seis) anos e multa.

Artigo 22 – Obstruir o funcionamento de rede integrada de computadores ou provocar-lhe distúrbios:

Pena – detenção, de 1 (um) a 2 (dois) anos, e multa.

Parágrafo único: Se resulta obstrução permanente ou distúrbio grave:

Pena – reclusão, de 4 (quatro) a 6 (seis) anos, e multa.

Artigo 23 – Obter acesso a sistema ou a rede integrada de computadores, com o intuito de disseminar informações fraudulentas:

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

Artigo 24 – Falsificar, alterar ou apagar documentos através de sistema ou rede integrada de computadores e seus periféricos:

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

§1º Nas mesmas penas incorre quem, sabendo ser falso, utiliza-se de documento obtido através de sistema ou rede integrada de computadores.

§2º Considera-se documento o dado constante no sistema de computador e suporte físico como disquete, disco compacto cd-rom ou qualquer outro aparelho usado para o armazenamento de informação, por meios mecânico, ótico ou eletrônico.

Artigo 25 – Interceptar indevidamente a comunicação entre computadores durante a transmissão de dados:

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

Parágrafo único: A pena é agravada em um terço se a interceptação invade a privacidade do usuário.

Artigo 26 – Obter, de forma não autorizada, informações confidenciais ou pessoais do indivíduo em sistema ou rede integrada de computadores:

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

Parágrafo único: Se resulta prejuízo econômico, a pena é aumentada até a metade.

Artigo 27 – Deixar de informar ou de retificar dados pessoais contidos em rede integrada de computadores, quando requerido pelo interessado:

Pena – detenção de 3 (três) e 9 (nove) meses, e multa.

Parágrafo único: Na mesma pena incorre quem:

I - transfere dados pessoais contidos em um sistema de computador, sem a permissão do interessado, a pessoa não autorizada com finalidade diversa daquela À qual a informação foi obtida.

II – transfere, sem permissão do interessado, dados pessoais para fora do País.

Artigo 28 – Obter acesso a sistemas de dados ou rede integrada de computadores de instituições financeiras com o objetivo de transferir, para si ou para outrem, dinheiro, fundos, créditos e aplicações de terceiro:

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

Artigo 29 – Obter acesso ilícito a sistema de computador ou a rede integrada de computadores, com o intuito de apropriar-se de informações confidenciais ligadas à segurança nacional:

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

Parágrafo único: Se além do acesso, as informações são copiadas, vendidas ou transferidas para outrem, a pena é aumentada de um sexto até metade.

Capítulo VI

DAS DISPOSIÇÕES FINAIS

Artigo 30 – Se os crimes cometidos nesta lei são praticas como meio para a realização de outros, a pena é aumentada de um sexto até a metade.

Artigo 31 – Os administradores de redes integradas de computadores, os provedores de serviços e de informações que, no exercício da função, provocam desvio nas finalidades estabelecidas para o funcionamento da rede, incorrem na pena de reclusão de 1 (um) a 2 (dois) anos, e multa.

Artigo 32 – Nos crimes definidos nesta lei somente se procede mediante representação do ofendido, salvo nos casos do §4º, do art. 18 e do art. 29, em que a ação é pública incondicionada.

Artigo 33 – Aplica-se subsidiariamente a legislação penal em vigor.

Artigo 34 – Esta lei entra em vigor 30 (trinta) dias a contar da data de sua publicação.

Artigo 35 – Revogam-se as disposições em contrário.

ANEXO 4

Projeto de Lei 3.943/97

O Congresso Nacional decreta:

Artigo 1º - O Título I da Parte Especial do Decreto-lei 2.848, de 7 de setembro de 1940 – Código Penal - , passa a vigorar acrescido do seguinte Capítulo VI, adequando-se a numeração dos capítulos subseqüentes:

“Capítulo VI – Dos crimes contra a privacidade

Violação da intimidade

Artigo 145 – A – Violar mediante processo tecnológico ou qualquer outro meio, a intimidade alheia, sem o consentimento do titular do direito:

Pena – detenção de seis meses a dois anos.

Parágrafo único: Na mesma pena incorre aquele que indevidamente revela que divulga imagem, escrito, palavra ou fato integrantes da intimidade alheia, ainda que legitimamente conhecidos.

Abuso da informática

Artigo 145 – B – Formar, indevidamente, com dados pessoais alheios, fichário automatizado ou banco de dados:

Pena – detenção, de seis meses a dois anos.

Parágrafo único: Na mesma pena incorre quem:

I – acrescenta, altera, suprime indevidamente dados pessoais alheios em fichário automatizado ou banco de dados;

II – utiliza processo tecnológico ou qualquer outro meio que possibilite acesso indevido a fichário automatizado ou banco de dados;

III – fornece, indevidamente, a terceiro, dados de fichário automatizado ou banco de dados;

IV – divulga, indevidamente, dados pessoais de fichário automatizado ou banco de dados.

ANEXO 5

Projeto de Lei do Senado 76/2000

O Congresso Nacional decreta:

Artigo 1º - Constitui crime de uso indevido da informática:

§1º contra a inviolabilidade de dados e sua comunicação:

I – a destruição de dados ou sistemas de computação, inclusive sua inutilização;

II – a apropriação de dados alheios ou de um sistema de computação devidamente patenteado;

III – o uso indevido de dados ou registros sem consentimento de seus titulares;

IV – a modificação, a supressão de dados ou adulteração de seu conteúdo;

V – a programação de instruções que produzam bloqueio geral no sistema ou que comprometam a sua confiabilidade:

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

§2º contra a propriedade e o patrimônio:

I – a retirada de informação privada contida em base de dados;

II – a alteração ou transferência de contas representativas de valores:

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

§3º contra a honra e a vida privada:

I – difusão de material injurioso por meio de mecanismos virtuais;

II – divulgação de informações sobre a intimidade das pessoas sem prévio consentimento:

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

§4º contra a vida e integridade física das pessoas:

I – o uso de mecanismos da informática para ativação de artefatos explosivos, causando danos, lesões ou homicídios;

II – a elaboração de sistema de computador vinculado a equipamento mecânico, constituindo-se em artefato explosivo:

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

§5º contra o patrimônio fiscal:

I – alteração de base de dados habilitados para registro de operações tributárias;

II – evasão de tributos ou taxas derivadas de transações “virtuais”:

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

§6º contra a moral pública e opção sexual:

I – a corrupção de menores de idade;

II – divulgação de material pornográfico;

III – divulgação pública de sons, imagens ou informação contrária aos bons costumes:

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

§7º contra a segurança nacional:

I – a adulteração ou revelação de dados declarados como reservados por questões de segurança nacional;

II – a intervenção nos sistemas de computadores que controlam o uso ou ativação de armamentos;

III – a indução a atos de subversão;

IV – a difusão de informação atentatória à soberania nacional:

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

Artigo 2º - Os crimes tipificados nos §§1º a 3º são ações penais públicas condicionadas à representação e as demais ações penais incondicionadas.

Artigo 3º - Qualquer um desses crimes que venha a ser praticado contra empresa concessionária de serviços públicos, sociedades de economia mista ou sobre qualquer órgão integrante de administração pública terão suas penas aumentadas para dois a seis meses e multa, nos casos dos §§1º e 3º e de um ano e seis meses a dois anos e eis meses e multa nos demais casos.

Artigo 4º - Caso seja praticado qualquer um dos crimes tipificados nesta lei como meio de realização ou facilitação de outro crime, fica caracterizada a circunstância agravante qualificadora, aumentando-se a pena de um terço até a metade.

Artigo 5º - Todos os crimes por uso indevido de computador estão sujeitos a multa igual ao valor do proveito pretendido ou do risco de prejuízo da vítima.

Artigo 6º - Esta lei entra em vigor na data de sua publicação.

ANEXO 6

Projeto de Lei 6.210/02

Artigo 1º - Esta lei dispõe sobre as limitações ao envio de mensagens eletrônicas não solicitadas (Spam), por meio da Internet, originadas ou destinadas a computadores instalados no País.

Artigo 2º - Considera-se mensagem eletrônica não solicitada (Spam), para os efeitos desta lei, a mensagem eletrônica recebida por meio de rede de computadores, sem consentimento prévio do destinatário, e que objetive a divulgação de produtos, marcas, empresas ou endereços eletrônicos, ou a oferta de mercadorias ou serviços, gratuitamente ou mediante remuneração.

Artigo 3º - Toda mensagem eletrônica não solicitada deverá atender aos seguintes princípios:

I – a mensagem poderá ser enviada uma única vez, vedada a repetição a qualquer título sem o prévio consentimento do destinatário;

II – a mensagem deverá conter, no cabeçalho e no primeiro parágrafo, uma identificação clara de que se trata de mensagem não solicitada;

III – o texto da mensagem conterá a identificação do remetente e um endereço eletrônico válido;

IV – será oferecido um procedimento simples para que o destinatário opte pelo não recebimento de outras mensagens do mesmo remetente.

Parágrafo único: É vedado o envio de mensagem eletrônica não solicitada a quem tiver se manifestado ao remetente contra seu recebimento.

Artigo 4º - Todo usuário de rede de computadores que utilizar serviço de correio eletrônico tem o direito de identificar, bloquear e optar por não receber mensagens eletrônicas não solicitadas.

§1º O destinatário pode exigir do seu provedor de acesso ou de correio eletrônico, ou do provedor do remetente, o bloqueio de mensagens não solicitadas, desde que informado o endereço eletrônico do remetente.

§2º É obrigação do provedor atender às solicitações de que trata o parágrafo anterior em prazo não superior a vinte e quatro horas, vedada a cobrança de taxas de qualquer natureza.

§3º Não será responsabilizado pelo recebimento indevido de mensagem eletrônica não solicitada o provedor de acesso ou de serviço de correio eletrônico que tenha se utilizado, de boa-fé, de todos os meios a seu alcance para bloquear a transmissão ou recepção da mensagem.

Artigo 5º - As infrações aos preceitos desta lei sujeitarão o infrator à pena de multa de até oitocentos reais por mensagem enviada, acrescida de um terço na reincidência.

Artigo 6º - Esta lei entra em vigor em sessenta dias, contados da sua publicação.