CRIMES INFORMÁTICOS

Maria José Crepaldi Ganancio LIBERATI[1]

RESUMO: O crescimento da tecnologia da Informação nas sociedades do mundo inteiro propiciou o aparecimento de novas formas de crimes – os crimes informáticos - e com eles o surgimento do criminoso informático, que realizam condutas censuráveis e condenáveis, movidos por todo tipo de interesse, por intermédio de computadores e redes de Internet. Diante desta nova realidade discute-se o conceito deste tipo de crime, suas classificações, os objetivos de seus agentes e suas condutas, sendo que a maioria delas não está prevista em lei e pela prevalência dos princípios da Reserva Legal e da legalidade esculpidos na Constituição Brasileira, não pode ser punida. Necessário se faz criar novos ordenamentos jurídicos para combater a cibercriminalidade e responder de forma eficaz a um crime que fica cada vez mais sofisticado.

Palavras-chave: Crime Informático. Criminoso Informático. Cibercriminoso. Direito Penal Informático.

1 INTRODUÇÃO

O desenvolvimento tecnológico modificou de forma irreversível o cotidiano das atividades das pessoas. A Tecnologia da Informação provocou alterações das sociedades em todo o mundo. A produtividade dos setores industriais tradicionais está melhor; os métodos de trabalho estão acelerados e os movimentos de capitais remodelados.

Ao mesmo tempo, à medida que os benefícios começam a espalhar-se, este rápido crescimento propiciou o aparecimento de novas formas de crimes - os crimes informáticos. Os recursos que as novas tecnologias oferecem, nem sempre são empregados com um fim adequado e neste ambiente virtual, os crimes informáticos podem ocorrer com alguns “clicks”, por meio de uma palavra digitada “inocentemente”, um “e-mail” ou um “arquivo” enviado erroneamente.

[1] Analista de Sistemas pela PUC Campinas/SP. Docente da Faculdade de Informática de Presidente Prudente/Unoeste. Discente do 1º termo do Curso de Direito das Faculdades Integradas “Antonio Eufrásio de Toledo” de Presidente Prudente - RA: 001.1.09.309.

Para Monteiro Neto (2003) os crimes informáticos são difíceis de captar e contextualizar e podem acarretar danos tanto pessoais como empresariais. Atualmente, novas questões surgem demandando respostas do operador do Direito, que devem ser imediatas, sob pena de o tradicional hiato existente entre o Direito e a realidade social vir a ser enorme.

A pedofilia é considerada um crime informático que está descrito no Estatuto da Criança e do Adolescente - ECA, conforme comenta Liberati (2008).

A maior parte das leis existentes, que pode ser usada para inibir os crimes informáticos, não foi elaborada especificamente para este fim.

O objetivo deste trabalho é apresentar as ocorrências legais do crime informático e indicar a lacuna legislativa existente para outros tantos crimes informáticos, para promover o combate a eles a partir de novos ordenamentos jurídicos.

2 DESENVOLVIMENTO

As tecnologias da informação, especialmente as redes informáticas além de propiciar facilidades e vantagens nunca antes cogitadas, também se revelam uma extrema facilitadora para o cometimento de ilícitos.

Os Crimes Informáticos ou “Computer Crimes” ou ainda Crimes Virtuais estão sendo cometidos por pessoas que muitas vezes ficam impunes pela dificuldade de investigação, produção de provas e ausência de leis.

Para que as leis sejam elaboradas e/ou aplicadas há a necessidade de esclarecer como os crimes informáticos são classificados, como podem ser cometidos e por quem.

Algumas leis para crimes informáticos já existem, outras necessitam de aprovação, outras ainda necessitam de estudos para a propositura de projetos de lei.

2.1 Crimes Informáticos

Trata-se de qualquer conduta ilegal, não ética, ou não autorizada que envolva o processamento automático de dados e/ou transmissão de dados, segundo a definição de (Reis, 1997), que seguiu a orientação da OECD (Organization for Economic Cooperation and Development - Organização para Cooperação Econômica e Desenvolvimento).

A conduta criminosa implica o uso de tecnologias digitais para cometer o delito, que é dirigida contra as próprias tecnologias da informação e comunicação; ou que envolve o uso acessório de equipamento informático na prática de outros crimes conforme documento da ONU de abril de 2005[2].

Nesta definição o crime informático pode implicar a manipulação de dados ou informações, a falsificação de programas, a sabotagem eletrônica, a espionagem virtual, a pirataria de programas, o acesso e/ou uso não autorizado de computadores e redes.

João Marcello Araújo Júnior (apud Monteiro Neto, 2003) conclui que crime informático consiste em "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".

A definição de crime informático deve estar intrinsecamente relacionada ao bem jurídico que se deseja proteger e deve ser aquele perpetrado contra bens jurídicos computacionais.

Monteiro Neto (2003) diz que para a caracterização do crime informático é necessária a existência de dois pressupostos:

---

[2] 11º Congresso das Nações unidas sobre Prevenção do Crime e Justiça Penal. www.unis.unvienna.org.

1. O crime deve ser perpetrado contra dados aptos ao processamento informático (o agente deve possuir a vontade subjetiva de lesar dados);

2. Sejam perpetrados através do computador (por meio da utilização de hardware e software).

Para este autor, o crime informático pode ser conceituado como toda ação típica, antijurídica e culpável cometida contra um sistema de informática ou contra dados e informações existentes no sistema computacional, não importando se o ato ocorre na introdução, no tratamento, no armazenamento ou na transmissão dos dados.

Com um olhar mais técnico, o crime informático pode ser definido, portanto, como qualquer ato ilícito cometido contra um sistema computacional ou por intermédio dele. Entende-se por sistema computacional (ou sistema de informação) um conjunto de componentes inter-relacionados que coletam, armazenam, processam, distribuem, recuperam as informações com o objetivo de facilitar o planejamento, o controle, a coordenação, a análise e o processo decisório em empresas e outras organizações, ou ainda para facilitar o trabalho e/ou estudo de pessoas físicas. Estes componentes são divididos em técnicos (hardware, software, banco de dados, telecomunicações), organizacionais (procedimentos para operar o sistema) e humanos (profissionais de sistemas e/ou usuários).

Com base no bem jurídico ofendido que pode ser um sistema de informática, um processamento automático de dados ou uma transmissão de dados é conveniente classificar a ação ilícita, surgindo assim novos problemas que desafiam os aplicadores do direito.

2.1.1 Classificação do crime informático

O Crime Informático pode ser classificado quanto à forma de autuação, quanto à finalidade, quanto aos efeitos e por se tratar de assunto novo no cenário jurídico, estas várias formas classificatórias são necessárias e interessantes.

Quanto à *forma de autuação do agente*, Monteiro Neto (2003) estabelece a seguinte classificação:

a) Fraude por manipulação de um computador contra um sistema de processamento de dados: consiste na modificação de dados dentro de um sistema informático com o intuito de obter vantagem ilícita. Pode ocorrer por meio da introdução de dados falsos ou também por meio da alteração de resultados;

b) Espionagem informática: consiste nos ilícitos que possuem como objetivo a obtenção de dados ou informações sigilosas por meio de sistema de informática;

c) Sabotagem informática: um dos mais danosos delitos praticados por meio de um sistema informático e tem como objeto o próprio sistema. Pode ser efetuado pela destruição do programa ou dos dados por meio de elementos criados pelos sabotadores como vírus ou mini programas que quando ativados inutilizam os programas principais destruindo-os ou distorcendo o seu funcionamento, tornando o sistema inapto a processar. E também pode ocorrer quando estes mecanismos desfiguram os dados já armazenados, o que acarreta inúmeros prejuízos aos programas principais;

d) Furto do tempo: é a modalidade ilícita mais comum e mais difundida dos crimes informáticos. Ocorre quando pessoas sem autorização utilizam-se de sistemas informáticos para fins particulares. Normalmente ocorre em empresas quando o funcionário sem possuir autorização para acessar a rede informática burla os sistemas de segurança e utiliza o computador e seus recursos para fins alheios aos interesses do empregador;

e) Acesso não autorizado: configura-se como o crime informático que mais se desenvolveu com o surgimento da Internet. Consiste em um acesso por pessoa não autorizada a um sistema de informática restrito no qual o invasor de maneira ilegal pode ter acesso a informações sigilosas, manipulando-as de forma a destruí-las, alterá-las ou praticar ações delituosas;

f) Ofensas tradicionais: podem ser praticada por meio de um sistema de informática ou que tenha a sua parte tangível como objeto. Consistem em utilizar o sistema informático para prática de ilícitos comuns como, por exemplo, a falsificação de documentos.

Uma classificação um pouco mais específica é estabelecida por Briat (apud Ferreira. In: Barra; Andreucci, 2000, p. 213) da seguinte forma:

a) Manipulação de dados e/ou programas a fim de cometer uma infração já prevista pelas incriminações tradicionais;

b) Falsificação de dados, de programas e entraves a sua utilização; divulgação, utilização ou reprodução ilícitas de dados e programas; uso não autorizado de sistemas de informação; acesso não autorizado a sistema de informação.

No 8º Congresso sobre Prevenção de Delito e Justiça Penal, em 1990 em Havana, Cuba, a ONU publicou uma relação de crimes informáticos, reconhecendo os seguintes delitos:

1. Fraudes cometidas mediante manipulação de computadores caracterizadas por: manipulação de dados de entrada (input); também conhecida como subtração de dados; manipulação de programas, modificando programas existentes em sistemas de computadores ou enxertando novos programas ou novas rotinas; manipulação de dados de saída (output), forjando um objetivo ao funcionamento do sistema informático, como por exemplo, a utilização de equipamentos e programas de computadores especializados em decodificar informações de tarjas magnéticas de cartões bancários ou de crédito; manipulação informática, técnica especializada que aproveita repetições automáticas dos processos do computador, apenas perceptível em transações financeiras, em que se saca um numerário rapidamente de uma conta e transfere para outra.

2. Falsificações informáticas: como objeto, quando se alteram dados de documentos armazenados em formato computadorizado; como instrumento, quando o computador é utilizado para efetuar falsificações de documentos de uso comercial, criando ou modificando-os, com o auxílio de impressoras coloridas a base de raio laser, cuja reprodução de alta qualidade, em regra, somente pode ser diferenciada da autêntica por perito.

3. Danos ou modificações de programas ou dados computadorizados, também conhecidos como sabotagem informática, ato de copiar, suprimir ou modificar, sem autorização, funções ou dados informáticos, com a intenção de obstaculizar o funcionamento normal do sistema, cujas técnicas são:

a) vírus, série de chaves programadas que podem aderir a programas legítimos e propagar-se a outros programas informáticos;

b) gusanos, análogo ao vírus, mas com o objetivo de infiltrar em programas legítimos de dados para modificá-lo ou destruí-lo, sem regenerar-se;

c) bomba lógica ou cronológica, requisitando autos conhecimentos especializados já que requer a programação para destruição ou modificação de dados em um certo momento do futuro;

d) acesso não autorizado a sistemas de serviços, desde uma simples curiosidade até sabotagem ou espionagem informática;

e) piratas informáticos que aproveitam as falhas nos sistemas de segurança para obter acesso a programas e órgãos de informações;

f) reprodução não autorizada de programas informáticos de proteção legal, causando uma perda econômica substancial aos legítimos proprietários intelectuais.

Posteriormente, no 10º Congresso sobre Prevenção de Delito e Tratamento do Delinqüente, em Viena, em abril de 2000, a ONU publicou outros tipos de delitos informáticos:

a) Espionagem industrial: espionagem avançada realizada por piratas para as empresas ou para seu próprio proveito, copiando segredos comerciais que abordam desde informação sobre técnicas ou produtos até informação sobre estratégias de comercialização;

b) Sabotagem de sistemas: ataques, como o bombardeio eletrônico, que consistem no envio de mensagens repetidas a um site, impedindo assim que os usuários legítimos tenham acesso a eles.

c) Sabotagem e vandalismo de dados: intrusos acessam sites eletrônicos ou base de dados, apagando-os ou alterando-os, de forma a corromper os dados.

d) Pesca ou averiguação de senhas secretas: delinqüentes enganam novos e incautos usuários da internet para que revelem suas senhas pessoais, fazendo-se passar por agentes da lei ou empregados de provedores de serviço. Utilizam programas para identificar senhas de usuários, para que, mais tarde, possam usá-las para esconder verdadeiras identidades e cometer outras maldades, como o uso

não autorizado de sistemas de computadores, delitos financeiros, vandalismo e até atos de terrorismo;

e) Estratagemas: astuciosos utilizam diversas técnicas para ocultar computadores que se parecem eletronicamente com outros para lograr acessar algum sistema geralmente restrito a cometer delitos.

f) Pornografia Infantil: a distribuição de pornografia infantil por todo o mundo por meio da Internet está aumentando. O problema se agrava ao aparecer novas tecnologias como criptografia, que serve para esconder pornografia e demais materiais ofensivos em arquivos ou durante a transmissão;

g) Jogos de Azar: o jogo eletrônico foi incrementado à medida que o comércio brindou com facilidades de crédito e transferência de fundos pela rede.

h) Fraude: já foram feitas ofertas fraudulentas ao consumidor tais como a cotização de ações, bônus e valores, ou venda de equipamentos de computadores pelo e-commerce;

i) Lavagem de dinheiro: pelo e-commerce é possível transferir mercadorias e dinheiro para lavar as ganâncias do crime, sobretudo, mediante a ocultação de transações.

Quanto á *finalidade do delito*, Pradel (apud Ferreira. In: Barra; Andreucci, 2000, p.214) exclui os delitos já abarcados pelo ordenamento jurídico classificando apenas os verdadeiros delitos informáticos:

a) Manipulações para obtenção de dinheiro;

b) Manipulações para obtenção de informações.

Hervé Croze e Yves Bismurth (apud Ferreira. In: Barra; Andreucci, 2000, p.215) propõem classificar os crimes informáticos em duas categorias:

a) Atos dirigidos contra um sistema de informática independentemente da motivação do autor; verdadeiro núcleo da criminalidade informática, por se tratarem de ações que atentem contra o próprio material informático (suportes lógicos ou dados dos computadores);

b) Atos que atentem contra outros valores sociais ou outros bens jurídicos cometidos através de um sistema de informática, que compreenderiam todas as espécies de infrações previstas em lei penal.

Maria de La Luz Lima (apud Furlaneto Neto, et al. Crimes na Internet. Brasília, CEJ, 2003) classifica os delitos eletrônicos em três categorias:

a) Os que utilizam a tecnologia eletrônica como *método*, ou seja, condutas criminais onde os indivíduos utilizam métodos eletrônicos para obter um resultado ilícito;

b) Os que utilizam a tecnologia eletrônica como *meio*, ou seja, condutas criminais em que para a realização de um delito utilizam o computador como meio;

c) Os que utilizam a tecnologia eletrônica como *fim*, ou seja, condutas dirigidas contra a entidade física do objeto ou máquina eletrônica ou seu material com o objetivo de danificá-lo.

Luís Flávio Gomes (Aras, 2009, on-line) divide os crimes informáticos em duas categorias:

a) Crimes praticados contra o computador, em sentido amplo;

b) Crimes praticados por meio de computador.

Nesta mesma linha de raciocínio, Damásio Evangelista de Jesus (Aras, 2009, on-line) classifica os crimes informáticos em duas categorias:

a) Crimes informáticos puros ou próprios: aqueles praticados por meio de um computador onde o resultado da conduta se opera em meio eletrônico, sendo a informática o bem jurídico protegido;

b) Crimes informáticos impuros ou impróprios: aqueles em que o sistema computacional funciona como ferramenta para a prática de condutas lesivas ao bem jurídico já protegido, não relacionado com a informática, produzindo resultado naturalístico que ofendem o mundo real.

Quanto aos *efeitos* os crimes informáticos podem ser classificados segundo Monteiro Neto (2003):

a) Crimes informáticos de efeitos tangíveis: condutas que além de perpetrarem-se em meio eletrônico produzem também efeitos diretos no mundo real;

b) Crimes informáticos de efeitos intangíveis: lesam somente os elementos imateriais formadores do sistema informático com os dados armazenados em processamento ou transmissão.

Todas estas classificações são importantes para facilitar o estudo e a divisão da matéria ressaltando os crimes comuns (tradicionais) e crimes informáticos.

2.2 Criminoso Informático ou Cibercriminoso

Nos anos 70 e 80 o criminoso informático era um exímio perito na operação de computadores e sistemas computacionais, isto é, agente ativo das condutas ilícitas.

Atualmente com as facilidades ocasionadas pelo desenvolvimento de software e hardware, qualquer indivíduo que possua as mínimas noções de como operar um computador pode ser considerado um criminoso informático em potencial.

A realidade social e cultural que permeia o ambiente digital torna extremamente complexa a confecção de um perfil do chamado criminoso virtual.

Monteiro Neto (2003) explica que hoje tais delinquentes são normalmente pessoas que trabalham no ramo informático. Em geral são *insiders* vinculados a empresas que raramente se sensibilizam com punição penal. Possuem como motivos para delinqüência o ânimo de lucro, perspectiva de promoção, vingança, para chamar a atenção, entre outros. Escondem-se atrás do anonimato da Internet, que serve para bloquear a investigação da conduta ilegal.

Quando descobertos alegam sempre o desconhecimento do crime que praticaram e se escondem atrás do fato de praticarem o ato apenas por “brincadeira” acrescenta Monteiro Neto (2003).

Para este autor, o criminoso virtual pode ser classificado em dois tipos: interno (inside hacker): aquele indivíduo que acessa indevidamente informações sigilosas de um nível superior. Normalmente é funcionário da empresa ou servidor

público; externo (outsider hacker): aquele que não tem acesso e utiliza um computador ou redes externas, ressaltando que não tem ligação à organização que ataca.

O primeiro hacker mundialmente famoso foi Kevin Mitnick que teve sua história contada no livro “O pirata eletrônico e o samurai”: a verdadeira história de Kevin Mitnick e do homem que o caçou na estrada digital, de Jeff Goodell. O famoso pirata Kevin Mitnick se valeu de um estratagema em 1996, para invadir o computador da casa de Tsotonmo Shimamura, expert em segurança, e destruir pela internet valiosos segredos de segurança.

Os objetivos do criminoso virtual segundo Monteiro Neto (2003) podem ser divididos em três estágios de motivação: instinto aventureiro: movido pelo desafio de superação da máquina; ganhar dinheiro extra: superada a máquina e satisfeito o ego, percebem um jeito fácil e “seguro” para ganhar dinheiro extra; prática de infrações para sustentar seu alto custo de vida – prolongamento do 2º estágio. Para ilustrar esta questão, o autor exemplifica a conduta de um jovem brilhante estagiário de informática do Centro de Processamento de Dados de uma Universidade, que altera as notas e as freqüências dos alunos, ou um promissor programador de computador de uma multinacional ávido por reconhecimento que rompe os sistemas de segurança para depois apresentar-se como solução.

O *hacker* é a figura mais associada á prática de crimes informáticos. É um termo pejorativo, derivado de ‘mutilador’, em inglês e pode ser definido como aquele que burla os sistemas de segurança de redes de computador para obter acesso não autorizado ao sistema e aos recursos por ele disponibilizados.

Contudo a terminologia “hacker” no mundo virtual é relacionada somente a um indivíduo extremamente hábil no campo informático. No submundo virtual criou-se uma nova denominação, o “cracker”, tido como o hacker não ético que invade sistemas com interesses patrimoniais ou danosos.

Esta divisão entre hacker e cracker está sedimentada no seio da comunidade informática, mas independentemente dos objetivos ou motivações, ambos invadem sistemas informáticos e violam a privacidade e o sigilo dos dados contidos nesses sistemas, o que por si só já configura crime na maioria dos países de 1º mundo.

Vários estudos podem ser destacados sobre os diversos tipos de criminosos informáticos, especialmente a classificação desenvolvida pelo professor mineiro Vianna (2003):

a) Crackers de servidores: hackers que invadem computadores ligados em rede;

b) Crackers de programas: hackers que quebram proteções de softwares cedidos a título de demonstração para usá-los por tempo indeterminado;

c) Phreakers: hackers especialistas em telefonia móvel ou fixa;

d) Desenvolvedores de vírus, Worms e Trojans: programadores que criam pequenos softwares que causam algum dano ao usuário;

e) Piratas: indivíduos que clonam programas fraudando direitos autorais;

f) Distribuidores de Warez: Webmasters que disponibilizam em suas páginas, software sem autorização dos detentores dos direitos autorais.

Ainda segundo Vianna (2003) os crackers podem ser subdivididos em:

a) Curiosos: movidos por curiosidade, não causam danos aos dados armazenados ou em tráfego pelas redes, apenas violam a privacidade das vítimas e o sigilo dos dados em trânsito pelos sistemas computacionais;

b) Pichadores digitais: procuram auto-afirmação dentro da rede, agindo com o único objetivo de serem reconhecidos e famosos no universo virtual;

c) Revanchistas: formados por ex-funcionários ou empregados descontentes que se utilizam dos conhecimentos adquiridos na empresa para sabotá-la;

d) Vândalos: agem simplesmente pelo prazer de causar danos às vítimas;

e) Espiões: agem com a finalidade de adquirirem informações confidenciais armazenadas nos sistemas computacionais das vítimas. As informações podem ter caráter comercial ou não;

f) Ciberterroristas: possuem motivações políticas ou religiosas e utilizam-se do meio digital para realizarem atividades criminosas que possibilitem a divulgação de suas crenças.

g) Ladrões e estelionatários: tem objetivos de lesar o patrimônio das vítimas.

As práticas mais corriqueiras do cracker são:

a) Spamming: envio de mensagens publicitárias por correio eletrônico para uma massa finita de usuários da rede, que não requisitaram a informação;

b) Cookies: também chamados de “biscoitinhos da WEB”, são arquivos de textos que são gravados no computador do usuário pelo browser quando ele visita determinados sites de comércio eletrônico de forma a identificar o computador com um número único e obter informações para reconhecer quem está acessando o site, de onde vem, com que periodicidade costuma voltar, etc.

c) Spyware: são programas espiões que enviam informações do computador do usuário para desconhecidos na rede de maneira que até o que é teclado é monitorado com informação;

d) Hoaxes: são e-mails, na maioria das vezes com remetente de empresas importantes ou órgãos governamentais contendo mensagens falsas, carregadas de vírus;

e) Sniffers: são programas espiões (farejadores) semelhantes aos spywares que são introduzidas no disco rígido para ter controle de leitura de e-mail;

Outra atitude criminosa é aquela cometida por meio do computador pelos “bullies”, isto é por pessoas que cometem “Bullying”.

O termo Bullying compreende todas as formas agressivas, intencionais e repetidas que ocorrem sem motivação evidente, adotadas por um ou mais estudantes contra outro(s) causando dor e angústia, e executadas dentro de uma relação de desigual poder que tornam possível a intimidação da vítima.

Nogueira (2008) descreve algumas ações de bullying como sendo aquelas que podem colocar apelidos, ofender, zoar, perseguir, intimidar, aterrorizar, humilhar e atormentar a vítima.

O criminoso digital é, portanto, aquela pessoa que usa computadores de maneira ilegal, ilícita, não ética, para prejudicar pessoas ou empresas, executando diversos tipos de práticas informáticas.

2.3. Crimes Informáticos e as Leis.

A necessidade de uma legislação penal para a proteção de bens jurídicos informáticos e de outros, igualmente relevantes, que possam ser ofendidos por meio de computadores é um dos problemas que vem sendo apresentado aos operadores do Direito.

É importante considerar que há alguns dispositivos constitucionais que já são utilizados pelos operadores do Direito, para os delitos cometidos pelo computador e pela Internet, a saber:

a) o art. 5º, inciso II, segundo o qual "ninguém será obrigado a fazer ou deixar de fazer alguma coisa senão em virtude de lei";

b) o art. 5º, inciso X, que considera "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";

c) o art. 5º, inciso XII, que tem por "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".

Existem também alguns tipos penais que descrevem crimes de informática:

a) O art. 10 da lei Federal nº 9296/96, que considera crime, punível com reclusão de 2 a 4 anos e multa, "realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo de Justiça, sem autorização judicial ou com objetivos não autorizados em lei". Este artigo regulamenta o art. 5º, inciso XII da CF/88;

b) O art. 153, § 1º-A do Código Penal, com a redação dada pela Lei Federal nº 9983/2000, que tipifica o crime de divulgação de segredo: "Divulgar, sem justa

causa, informações sigilosas ou reservadas, assim definidas em lei, contidas ou não nos sistemas de informação ou banco de dados da Administração Pública", punindo-o com detenção de 1 a 4 anos e multa;

c) A art. 313-A, do Código Penal, introduzido pela Lei nº 9983/2000, que tipificou o crime de inserção de dados falsos em sistemas de informação, com a seguinte redação: "Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou banco de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano", punindo-o com pena de reclusão, de 2 a 12 anos e multa;

d) O art. 313-B, do Código Penal, introduzido pela Lei nº 9983/2000, que tipificou o crime de sistema de informação, com a seguinte redação: "Modificar ou alterar, o funcionário, sistema de informação ou programa de informática sem autorização ou solicitação de autoridade competente", com pena de detenção de 3 meses a 2 anos e multa;

e) O art. 325, § 1º, incisos I e II, introduzido pela Lei nº 9983/2000, tipificando novas formas de violação de sigilo funcional, nas condutas de quem "I – 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" e de quem "II – se utiliza indevidamente, do acesso restrito", ambos sancionados com penas de detenção de 6 meses a 2 anos, ou multa;

f) O art. 12, caput, § 1º e § 2º, da Lei Federal nº 9609/98, que tipifica o crime de violação de direitos de autor de programa de computador, punindo-o com detenção de 6 meses a 2 anos, ou multa; ou com pena de reclusão de 1 a 4 anos e multa, se o agente visa ao lucro;

g) O art. 2º, inciso V, da Lei Federal nº 8137/90, que considera crime "utilizar ou divulgar programa de processamento de dados que permita ao sujeito passivo da obrigação tributária possuir informação contábil diversa daquela que é, por lei, fornecida à Fazenda Pública";

h) O art. 72 da Lei nº 9504/97, que cuida de 3 tipos penais eletrônicos de natureza eleitoral: "Constituem crimes, puníveis com reclusão de 5 a 10 anos: I –

obter acesso a sistema de tratamento automático de dados usado pelo serviço eleitoral, a fim de alterar a apuração ou a contagem de votos; II – desenvolver ou introduzir comando, instrução, ou programa de computador capaz de destruir, apagar, eliminar, alterar, gravar ou transmitir dado, instrução ou programa ou provocar qualquer outro resultado diverso do esperado em sistema de tratamento automático de dados usados pelo serviço eleitoral; III – causar, propositadamente, dano físico ao equipamento usado na votação ou na totalização de votos ou a suas partes".

Os crimes informáticos poderão ser enquadrados também em uma categoria especial de delitos, tutelados pela ordem jurídica brasileira por meio do Código Penal Brasileiro e seu capítulo V – Dos Crimes contra a honra, entendendo-se aqui como honra o conjunto de atributos morais e intelectuais de uma pessoa.

As três formas de crimes capitulados no referido ordenamento jurídico são: calúnia (art. 138), quando se atribui falsamente a alguém a prática de um fato definido como crime; injúria (art.140) quando se ofende a dignidade e o decoro da pessoa; e a difamação (art. 139), atribuição de fato não definido como crime, mas que ofende a reputação da vítima.

Segundo Liberati (2008), a lei 8069/90 que estabeleceu o Estatuto da Criança e do Adolescente (ECA) revolucionou o Direito Infanto-Juvenil. Esta lei descreve em seu artigo 241 o crime de informática, a saber: "Apresentar, produzir, vender, fornecer, divulgar ou publicar, por qualquer meio de comunicação, inclusive rede mundial de computadores ou internet, fotografias ou imagens com pornografia ou cenas de sexo explícito envolvendo criança ou adolescente" - pena de 2 a 6 anos de reclusão e multa. Nos incisos I, II, III, incluídos pela Lei 10.764/03 (pedofilia) os agentes incorrem na mesma pena (§ 1º) quando:

I – Agencia, autoriza, facilita ou, de qualquer modo, intermedeia a participação de criança ou adolescente em produção referida neste artigo;

II – assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens produzidas na forma do caput deste artigo;

III – assegura, por qualquer meio, o acesso, na rede mundial de computadores ou internet, das fotografias, cenas ou imagens produzidas na forma do caput deste artigo.

No § 2º - pena de reclusão de 3 a 8 anos se:

I - o agente comete o crime prevalecendo-se do exercício de cargo ou função;

II – o agente comete o crime com o fim de obter para si ou para outrem vantagem patrimonial.

Liberati (2008) explica que o crime previsto no art. 241 do ECA preocupa-se com a garantia “do direito à dignidade, ao respeito, à imagem, à liberdade sexual e ao domínio do corpo de criança e adolescente”. O citado autor ainda inclui como objeto jurídico da norma incriminadora “o pudor e a moralidade públicos, considerados enquanto analisados o comportamento indivíduo do grupo social”.

Os provedores de acesso à Internet começaram a se preocupar com a responsabilidade penal, depois da promulgação da Lei Federal 10.764/03 que alterou o art. 241 do ECA.

Mas a grande maioria de crimes informáticos ainda não está previsto em lei. E de acordo com o Princípio da Reserva Legal não podem ser punidos.

3 CONCLUSÃO

Muitas das novas tecnologias da atualidade tem criado novas oportunidades para crimes. As tecnologias de informática, especialmente a Internet, criaram novos itens valiosos para roubar, novas maneiras de roubá-los e de prejudicar pessoas, especialmente a Internet.

Ninguém conhece a magnitude do problema do crime informático – quantos sistemas são invadidos, quantas pessoas são adeptas dessa prática ou qual é o total dos danos econômicos – mas estima-se que custem muitos milhões de reais apenas no Brasil.

O imperativo moral Kantiano é útil, mas não suficiente para regular a vida em sociedade. O direito precisa ser provisionado com um poder coercitivo.

O Direito, por estar a serviço da sociedade, não é, e nem poderia ser estático, mas sim, dinâmico. O poder legislativo deve reagir às ameaças do crime informático aprovando leis que regulamentem este tipo de crime.

É inevitável a atuação do Direito Penal para inibir todas as formas de criminalidade informática, entre elas a criminalidade pela Internet, para proteger bens jurídicos tradicionais, ou para assegurar a proteção de novos bens jurídicos decorrentes das novas tecnologias como a cibercultura, a liberdade cibernética, o comércio eletrônico, a vida privada, a intimidade e o direito de autor na Internet.

Se já existe uma instrumentalização legal para caçar e punir pedófilos que tentam assassinar moralmente crianças e adolescentes, agora urge que se crie uma equivalente para casos como de empresas vendedoras que enviam e-mails não solicitados, em massa, a destinatários que não requisitaram a informação, como de hackers que exploram os pontos fracos da segurança da Internet para obter acesso a senhas e informações sigilosas ou como de vândalos cibernéticos ou de bisbilhoteiros eletrônicos, pois, causam dor a quem não merece e nem pode se explicar.

O mau caráter que comete o crime informático precisa ser punido e a lei deve ser eficaz, para que pessoas indefesas não tenham suas intimidades próprias exibidas por desaviso ou inexperiência.

As ações praticadas com a nova tecnologia da informação ainda se encontram sem a devida repressão jurídico-penal.

A necessidade de uma reflexão ética por parte dos profissionais da informação sobre a dimensão ética contida nos novos espaços e suportes informacionais exige também a discussão dos entraves de ordem jurídica a que o uso inadequado e inadvertido destes espaços pode levar. Os crimes informáticos, praticados ‘com’ e ‘contra’ o computador são uma preocupação social e carecem de tipificação no ordenamento jurídico brasileiro.

Se a sociedade migrou virtualmente para a Internet, para lá também deve caminhar o Direito - “Ubi societas ibi jus”.

REFERÊNCIAS BIBLIOGRÁFICAS

VIANA. Túlio Lima. **Hackers: um estudo criminológico da subcultura cyberpunk.** Disponível em HTTP://www.infojur.ccj.ufsc.br.

ANDREUCCI. Ricardo Antunes; BARRA. Rubens Preste (coord.). **Estudos Jurídicos.** São Paulo: RT, 2000.

REIS. Maria Helena Junqueira. **Computer Crimes: a criminalidade na era dos computadores.** Belo horizonte: Del Rey, 1997.

FERREIRA. Ivette Senise. **A criminalidade informática.** In: Lucca. Newton de; SIMÃO FILHO, Adalberto (coord). Direito e Internet: aspectos jurídicos relevantes. Bauru: Edipro, 2000.

ARAS. Vladimir. **Crimes de Informática – Uma nova criminalidade**.< http://www.informatica-juridica.com/trabajos/artigo_crimesinformaticos.asp>. Acesso em 26/04/2009.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **10º Congresso sobre Prevenção de Delito e Tratamento do Delinquente.** Disponível em: http://www.on.org/. Acesso em 01/04/2009.

LEVENE. Ricardo: CHIARAVALLOTI. Alicia. **Delitos informáticos.** VI Congresso Iberoamericano de Derecho e Informática, Montevidéu. Maio, 1998.

FURLANETO NETO. Mário. GUIMARÃES. José Augusto Chaves. **Crimes na Internet: elementos para uma reflexão sobre a ética informacional.** Brasília, CEJ, 2003.

MONTEIRO NETO. João Araújo. **Crimes informáticos uma abordagem dinâmica ao direito penal informático.** Fortaleza, Pensar. 2003.

LIBERATI. Wilson Donizeti. **Comentários ao Estatuto da Criança e do Adolescente.** São Paulo: Malheiros Editora. 2008.

NOGUEIRA. Sandro D´Amato. **Crimes de Informática.** São Paulo: BH Editora, 2008.

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