OS "CRIMES DE INFORMÁTICA" NO DIREITO PENAL BRASILEIRO

Lóren Pinto Ferreira[1]

Resumo

O presente artigo apresenta um estudo sobre o tratamento dado pelo Direito Penal brasileiro aos crimes cometidos com o auxílio dos sistemas computadorizados. O uso da tecnologia da informação (TI) tem contribuído para o desenvolvimento sociocultural, porém, juntamente com o avanço, surgem usuários que se utilizam desses sistemas para cometer atos ilícitos. A imprensa tem noticiado diversos casos de crimes cometidos pela Internet ou por outros sistemas computadorizados. Porém, em alguns casos percebe-se que determinadas condutas, praticadas com a utilização da TI, que causam danos a bens jurídicos que deveriam ser tutelados pelo Direito, mas que não se enquadram em nenhum dos tipos penais previstos no sistema jurídico-penal do nosso país, ficam impunes. Os aplicadores do Direito tentam enquadrar, na medida do possível, esses atos lesivos aos tipos penais previstos no Código Penal e na legislação esparsa. Com o desenvolvimento do trabalho percebeu-se que várias condutas que trazem prejuízos consideráveis às vítimas não são tipificadas e, portanto, não podem ser consideradas como criminosas e sim como fatos atípicos. Assim, conclui-se ser necessária a criação de lei específica prevendo crimes dessa natureza ou a reformulação das leis existentes. Para o desenvolvimento do trabalho foi aplicado o método indutivo, efetuando-se uma pesquisa exploratória, com a aplicação da técnica de pesquisa bibliográfica.

Palavras-chave:
Crimes de Informática – Direito Penal – Tecnologia da Informação

1 INTRODUÇÃO

A informatização da sociedade se dá em alta velocidade. O impacto da tecnologia da informação (TI) sobre o Direito é um tema complexo, pois envolve vários dos seus ramos, dentre eles, o Civil, o Processual Civil, o Penal, o Processual Penal, o do Trabalho, o Comercial, o do Consumidor, o Tributário e o Internacional. Neste trabalho, a preocupação é somente com relação ao Direito Penal.

O uso da TI, principalmente da Internet, tem contribuído muito para o desenvolvimento sociocultural, mas, juntamente com o avanço, surgem usuários que se utilizam desses sistemas para cometer atos ilícitos e que praticam, com o auxílio do computador, condutas tipificadas como crime e outras novas, anti-sociais, porém não tipificadas, que fazem com que a ciência do Direito, sobretudo o Penal, tenha de assumir uma posição.

Escuta-se, diariamente, a imprensa noticiar a ocorrência dessas práticas via Internet ou por outros sistemas computadorizados. Porém, em muitos desses casos percebe-se que tais

[1] Professora dos cursos de Direito e Administração do INESC/CNEC. Mestre em Administração, Bacharel em Direito e em Informática. lorenpfg@gmail.com

condutas causam danos a bens jurídicos que deveriam ser tutelados, mas que ainda não possuem essa proteção estatal.

Os aplicadores do Direito tentam enquadrar, na medida do possível, esses atos lesivos aos tipos penais previstos no Código Penal e na legislação esparsa brasileiros, mas muitas, por não se enquadrarem em nenhum dos tipos penais previstos no sistema jurídico-penal do nosso país, ficam impunes, já que não são consideradas como condutas criminosas e sim como fatos atípicos.

Nesse contexto, conclui-se ser necessária a criação de lei específica prevendo crimes dessa natureza ou a reformulação das leis existentes. Além disso, é preciso, também, que sejam criados mecanismos de controle que garantam a identificação do autor dessas práticas, para que as pessoas possam utilizar as tecnologias da informação de forma segura, com a certeza de que o Direito possa garantir a paz social e a manutenção do Estado Democrático de Direito.

Para o desenvolvimento do trabalho foi aplicado o método indutivo, efetuando-se uma pesquisa exploratória, com a aplicação da técnica de pesquisa bibliográfica.

2 CRIMES PRATICADOS COM O COMPUTADOR E O DIREITO PENAL BRASILEIRO

Costa (1995), já na década de 90, afirmava que no Brasil ocorreriam várias dessas práticas e que, porém, as mesmas não eram noticiadas, devido à possibilidade dessa notícia abalar a credibilidade das empresas (vítimas), por se pensar que a conseqüência da divulgação poder ser mais grave do que o resultado da própria ação, já que pode acarretar desespero, comoção geral ou perda de inúmeros clientes que ficam receosos de negociar com uma empresa que não tenha segurança de dados, informações e sistemas.

O autor afirma que existem, há muitos anos, no Brasil, tímidas iniciativas no sentido de regulamentar essas condutas, através de projetos de lei que tramitam nas casas do Congresso Nacional. Porém até os dias atuais continua-se sem medidas efetivas.

O nosso Código Penal, quando defrontado com delitos dessa natureza, deixa claras as suas deficiências com relação ao tema, até porque a Parte Especial do referido Código data de 1940, época em que os sistemas computadorizados ainda não tinham aportado em nosso país (PIRAGIBE, 1985). Dessa forma verifica-se a “quase” impossibilidade de se aplicar esta parte do Código aos chamados “Crimes de Informática”. Porém, através dos princípios gerais do Direito Penal, é possível aplicar regras da Parte Geral do Código Penal a esse tipo de conduta.

Um dos temas mais polêmicos entre os doutrinadores de Direito Penal de Informática é a conceituação, pois essa vem, muitas vezes, em forma restritiva ou então abrangente demais, não refletindo as muitas situações em que se enquadram os crimes de informática (PINTO FERREIRA, 2007).

Muitas condutas delitivas de natureza informática são difíceis de ser tipificadas. Os crimes de informática, segundo Costa (1995), devem ser classificados adequadamente para que o legislador pátrio possa elaborar normas eficientes, e, se necessário, indicar as normas vigentes que podem ser aplicadas, porém é imprescindível o estudo crítico desses delitos. É necessário, também, que se busque individualizar as suas espécies, assim se instrumentalizaria o aprofundamento do objeto jurídico a ser protegido, bem como a aplicação da norma e da pena adequadas ao delito.

Antes de se falar em crimes praticados pelo computador é necessário que se tenha em mente a idéia do conceito de crime.

2.1 CRIME

Para Capez (2008) e Mirabete (2007), crime pode ser conceituado sob três aspectos diversos, quais sejam:

- material – sob esse enfoque crime é "todo fato humano que, propositada ou descuidadamente, lesa ou expõe a perigo bens jurídicos considerados fundamentais para a existência da coletividade e da paz social" (CAPEZ, 2008). Mirabete (2007) também chama esse aspecto de substancial e destaca que nele o que está sendo observado é o conteúdo do fato punível;
- formal – sob esse enfoque "o crime resulta da mera subsunção da conduta ao tipo legal e, portanto, considera-se infração penal tudo aquilo que o legislador descrever como tal, pouco importando o seu conteúdo" (CAPEZ, 2008). Aqui se está atendendo "ao aspecto externo, puramente nominal do fato" (MIRABETE, 2007) e, assim, se conceitua crime como "o fato humano contrário à lei" (CARMIGNANI apud MIRABETE, 2007). Capez (2008) salienta que a consideração da existência de um crime sem considerar a essência ou lesividade material afronta o princípio constitucional da dignidade humana, e Mirabete (2007) destaca que as definições sob essa ótica "alcançam apenas um dos aspectos do fenômeno criminal, o mais aparente, que é a contradição do fato à norma de direito, ou seja, sua ilegalidade como fato

contrário à lei penal. Então, essas definições não penetram em sua essência, em seu conteúdo, em sua matéria";

- analítico – nesse enfoque que busca, sob um prisma jurídico, estabelecer os elementos estruturais do crime, o conceito é: "todo fato típico ilícito" (CAPEZ, 2003). Aqui, em primeiro lugar, deve-se observar a tipicidade da conduta do agente. Mirabete (2007) afirma que, quanto a esse prisma, o que se analisa são as características ou os aspectos do crime.

2.2 CRIMES DE INFORMÁTICA

Com a expansão da utilização dos sistemas computadorizados e com a difusão da Internet, tornam-se cada vez mais freqüentes os casos em que as pessoas se utilizam dessas ferramentas para cometer atos que causam danos a bens jurídicos de terceiros. O desvalor cometido por intermédio desses meios não tem fronteiras, pois de um computador situado num país pode-se acessar um sistema e manipular seus dados, sendo que os resultados dessa ação podem ser produzidos em outro computador muito distante daquele em que ela foi originada, podendo, inclusive, estar localizado em um país diverso (ROSA, 2005).

Em questão de segundos, um computador pode processar milhões de dados. No mesmo intervalo de tempo, ele também pode ser utilizado para furtar milhares de reais, porém, nesse caso, com a comodidade de poder cometer tal crime na privacidade do seu lar, desde que possua o conhecimento e o equipamento necessários, sem os riscos de, por exemplo, assaltar um banco ou um comércio portando uma arma de fogo.

Os crimes cometidos com o auxílio do computador, normalmente, são difíceis de ser detectados, costumam envolver grandes quantias e são crimes considerados 'limpos' (STAIR, 1998).

Percebe-se que não há um consenso quanto à denominação desse tipo de delito na bibliografia relacionada ao tema, sendo encontradas diversas expressões, tais como crimes de Informática, crimes informáticos, crimes com computador, *cybercrimes*, *e-crime*, crime *hi-tech*, crimes eletrônicos, entre outros.

Além do problema quanto à denominação, existe uma questão mais grave, que diz respeito à utilização da expressão crime.

2.2.1 A Expressão "Crime de Informática"

Durante o desenvolvimento do trabalho constatou-se que diversos autores utilizam o termo "crime" quando estão falando dessas condutas lesivas a dados, informações ou sistemas informáticos. Abaixo, é apresentado o conceito de "crimes de informática" encontrado por grande parte da doutrina e, dessa forma, pode-se comprovar tal utilização.

Costa (1995) afirma que grande parte dos doutrinadores define "crime de informática" como a conduta que atenta contra o estado natural dos dados e recursos oferecidos por um sistema de processamento de dados, seja pela transformação, armazenamento ou transmissão de dados, na sua forma, compreendida, pelos elementos do sistema de tratamento, transmissão ou armazenagem dos mesmos, ou ainda, na forma mais rudimentar.

Assim, depreende-se que "crime de informática" é todo aquele procedimento que atenta contra os dados, que o faz na forma em que estejam armazenados, compilados, transmissíveis ou em transmissão. Daí pressupõe-se a existência de dois elementos indissolúveis: dados (objeto material) e *hardware* (parte física do sistema) + *software* (parte lógica do sistema) para realizar alguma conduta com esses dados (meio executório).

Nesse sentido, "crime de informática" é, então, qualquer conduta ilegal não ética ou não autorizada que envolva processamento automático e/ou transmissão de dados (Organização para a Cooperação Econômica e Desenvolvimento *apud* Costa, 1995).

Costa (1995) definiu "crime de informática" como toda a ação típica, antijurídica culpável contra ou pela utilização de processamento automático de dados ou sua transmissão.

Vianna (2003, p.2-3) alerta sobre a utilização desse termo e explica que, partindo do conceito formal de crime, conclui-se que, para o Direito Penal brasileiro, algumas condutas ditas na bibliografia como crimes de Informática, como, por exemplo, o acesso não-autorizado a sistemas, não é crime, visto não haver previsão legal de tais condutas no Código Penal de nosso país. Quanto ao conceito analítico, segundo o qual crime é toda a conduta típica e antijurídica, tais ações são apenas condutas atípicas, pois não são contempladas em nenhum dos tipos penais do nosso sistema jurídico penal. Já com relação ao conceito material, é mister verificar se a conduta ofende ou não a um bem juridicamente tutelado. O autor afirma que "a inviolabilidade das informações é decorrência natural do direito à privacidade, devendo, portanto, ser reconhecida como bem jurídico essencial para a convivência numa sociedade". Assim, defende o autor, a inviolabilidade de dados e informações armazenados em sistemas computadorizados surge como um novo bem jurídico a ser tutelado pelo Direito Penal, de forma a garantir a privacidade e a integridade desses bens. Então, "existindo um

bem jurídico a ser tutelado, há crime sob o aspecto material. A simples omissão normativa não é suficiente para descaracterizá-lo como objeto de estudo do Direito Penal, já que este reconhece sua existência sob o aspecto material".

Rosa (2005), por sua vez, destaca que existe um problema relacionado à dicotomização do delito comum e o de Informática, já que muitos doutrinadores garantem que não existem delitos dessa natureza, pois argumentam que os crimes cometidos com o computador encontram-se todos positivados na legislação brasileira. Porém, o autor destaca que existem crimes comuns – os previstos no Código Penal (CP) brasileiro, crimes comuns cometidos com o auxílio do computador - que encontram aplicação na legislação penal brasileira, visto que se enquadram nas condutas descritas nos tipos penais previstos no CP, e certas condutas que não estão tipificadas em tal legislação e que necessitam da utilização do computador para o resultado desejado. Esses são os "crimes de Informática" propriamente ditos e são essas situações que necessitam de legislação específica, já que não se encaixam na tipificação do sistema jurídico penal brasileiro.

Gouveia (2007) cita, dentre essas condutas não-tipificadas, as invasões, os vírus de computador e a destruição de dados e afirma que esses e outros delitos tradicionais ou clássicos, como pornografia infantil, racismo e violência moral, que vêm sendo praticados no ciberespaço, estão causando prejuízos reais à vida das pessoas.

Vianna (2003) classifica os crimes de Informática em:

1) impróprios – aqueles em que o computador é usado como instrumento para a execução do crime, porém não há ofensa ao bem jurídico inviolabilidade dos dados ou informações. Exemplo: crimes contra a honra cometidos por meio da Internet;
2) próprios – aqueles em que o bem jurídico protegido pela norma penal é a inviolabilidade dos dados ou informações. Exemplo: Art. 313-A, do CP, acrescentado pela Lei nº 9.983/2000, que determina:

> Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos ou excluir indevidamente dados corretos nos sistemas informatizados da Administração Pública com o fim de obter vantagem para si ou para outrem ou para causar dano: Pena – reclusão, de 2 (dois) a 12 (doze) anos e multa (VIANNA, 2003);

3) mistos – são crimes complexos em que a norma visa tutelar, além da proteção da inviolabilidade dos dados, bem jurídico de natureza diversa. São delitos derivados do acesso não-autorizado a sistemas computacionais. O autor destaca que, no ordenamento jurídico brasileiro, o delito informático fundamental ainda não foi tipificado, enquanto que um derivado já o foi, a saber: acesso não-autorizado a

sistemas computacionais do sistema eleitoral, com a Lei nº 9.100/95, em seu art. 69, VII, que prevê: "Obter ou tentar obter, indevidamente, acesso a sistema de tratamento automático de dados utilizado pelo serviço eleitoral, a fim de alterar a apuração ou contagem de votos" (apud VIANNA, 2003);

4) mediatos ou indiretos – delito-fim não-informático que herdou essa característica do delito-meio informático realizado para poder ser consumado. Exemplo: o acesso não-autorizado a um sistema computacional bancário para a realização de um furto. Pelo princípio da consumação[2], o agente só será punido pelo furto, e esse será classificado como informático mediato ou indireto, pois um crime-meio informático não será punido em razão da consumação desse outro crime.

Stair (1998) diz que os crimes praticados com o computador possuem natureza dupla: o computador tanto pode ser a ferramenta usada para cometer o crime como também pode ser o objeto do crime.

2.2.1.1 O Computador como Ferramenta para o Cometimento de Crimes

Assim como pode-se usar dinamite para abrir um cofre, o computador pode ser utilizado para se obter acesso a informações valiosas ou a um determinado sistema.

Conforme Stair (1998), para cometer esse tipo de crime, são necessárias duas habilidades:

1ª) saber como conseguir acesso ao sistema computadorizado. Normalmente, precisará conhecer a identificação e a(s) senha(s) de acesso ou deverá ter a capacidade de gerar códigos falsos ou autênticos;

2ª) saber como manipular o sistema para obter o resultado esperado.

[2] De acordo com Zaffaroni e Pierangeli (apud VIANNA, 2003, p. 26), "em função do princípio da consumação, um tipo descarta outro porque consome ou exaure seu conteúdo proibitivo, isto é, porque há um fechamento material".

2.2.1.2 O Computador como Objeto de Crimes

O computador se torna objeto de crime quando o acesso a um sistema computadorizado é obtido sem a autorização de seu proprietário e/ou quando dados ou equipamentos computacionais são furtados ou destruídos (STAIR, 1998).

Colares (apud GOUVEIA, 2007) também faz uma classificação dos crimes cometidos com o uso do computador, a saber:

1. crimes eletrônicos - crimes tradicionais nos quais a Internet é utilizada como meio para a sua prática, dentre eles: pornografia infantil, racismo, ofensas morais, plágio e incitação à violência;
2. crimes informáticos - práticas ofensivas que têm como fim a lesão de dados ou sistemas computacionais, especialidade dos *hackers*[3], que não têm previsão legal no Brasil e, portanto, não poderiam ser chamados de "crimes" no sentido jurídico da palavra.

Essa discussão quanto à utilização do termo crime se dá devido ao fato de o Direito Penal brasileiro ter como dois de seus princípios fundamentais o da legalidade e o da anterioridade, previstos no art. 1º, do CP e no art. 5º, XXXIX, CF, que determinam que não há crime sem lei anterior que o defina e não há pena sem prévia cominação legal. Pelo princípio da legalidade (MIRABETE, 2007), uma pessoa só pode ser punida se, anteriormente ao fato por ela praticado, existir uma lei que o considere como crime; mesmo que a conduta seja imoral, anti-social ou danosa, não poderá ser punida, sendo irrelevante se entrar em vigor lei posterior que o preveja como crime, devido ao princípio da anterioridade (JESUS, 2002).

Também há muita discussão a respeito da necessidade ou não da criação de legislação específica para o tratamento dos ditos "crimes de Informática". Rosa (2005) é um dos defensores da corrente que entende ser mister a sua criação. Ele destaca que "é preciso proteger a sociedade e o cidadão contra tais comportamentos, de modo que a tipificação desses delitos específicos, os chamados crimes de Informática, acaba sendo uma das medidas consideradas urgentes e que não pode esperar mais".

Já Silva (2003) defende que a interação entre a Informática e o Direito, chamada por ela de Direito de Informática, trata-se de um novo ramo do conhecimento jurídico. A autora

[3] *Hacker* é uma pessoa que possui uma grande facilidade de análise, assimilação, compreensão e capacidades surpreendentes para lidar com um computador. Ele sabe que nenhum sistema é completamente livre de falhas e sabe onde procurar por elas, utilizando-se de técnicas das mais variadas. Popularmente o *hacker* é visto como um 'criminoso', porém, tecnicamente, quem utiliza as habilidades de *hacker* 'para o mal' é chamado de *cracker* (ULBRICH et al, 1999).

afirma haver sustentação doutrinária para o reconhecimento desse novo ramo do Direito e que sua origem está na necessidade social perante a invasão da informática na vida das pessoas; porém, ela destaca não haver unanimidade quanto ao surgimento desse ramo, mesmo reconhecendo tratar-se de matéria que exige cuidado devido a suas peculiaridades.

> O aparecimento da Informática no meio social ocorreu de forma tão rápida e passou a exigir, com a mesma rapidez, soluções que o Direito não estava preparado para resolver. Com isso, a necessidade social aparenta estar desprovida da tutela do Direito e a busca ansiosa por regular a matéria pode provocar a criação de leis excessivas e desnecessárias (SILVA, 2003).

2.2.2 Condutas Classificadas como "Crimes Próprios de Informática"

A seguir são apresentadas algumas condutas danosas a bens jurídicos de terceiros e que só podem ser realizadas com a utilização da TI.

2.2.2.1 Acesso e Uso Não-Autorizados

O acesso não-autorizado a um sistema computadorizado ou rede de computadores pela violação de regras de segurança "concerne especificamente à conduta daquele que ilegalmente penetra em um sistema informático ou telemático protegido por medidas de segurança, ou, ainda, ali se mantenha contra a vontade expressa ou tácita de quem tem o direito de excluí-lo" (ROSA, 2005). Já o uso não-autorizado pode ser realizado aceitando o risco de causar prejuízo ou dano ao sistema, ao seu proprietário ou a quem tenha autorização para acessá-lo, no intuito de causar tal prejuízo ou efetivamente o causando.

2.2.2.2 Alteração e Destruição de Dados

Dados e informações são bens pessoais ou corporativos. O uso intencional de programas ilegais e destrutivos para alterar ou destruir dados é um ato tão criminoso quanto a destruição de bens tangíveis.

Os exemplos mais comuns desse tipo de programas são os vírus que, quando carregados em um computador, podem destruir dados, interromper ou provocar erros no processamento.

Segundo O´Brien (2001), vírus é o termo mais conhecido, mas, tecnicamente, é um programa que se oculta dentro de outro programa, ou seja, não pode funcionar sem a

existência de outro no qual será inserido. Existe também um programa destrutivo que pode rodar de forma independente e é chamado de verme. Os dois copiam rotinas destrutivas nos computadores, isolados ou em redes, de qualquer pessoa que acessar computadores infectados pelo vírus ou que utilizar cópias de discos magnéticos tiradas a partir de computadores infectados. Assim, um vírus ou verme de computador pode disseminar a destruição entre muitos usuários. Um programa desse tipo pode apenas exibir mensagens humorísticas, mas, muitas vezes alteram completamente o funcionamento de um computador ou de uma rede de computadores, podendo destruir dados e programas, os quais correm o risco de não voltar a ser funcionais (LAUDON e LAUDON, 1999). Normalmente, o vírus ou o verme entra em um sistema computadorizado por intermédio de cópias ilegais de *software* ou de *e-mails* e *links* da Internet.

Para diagnosticar, remover e prevenir os computadores e as redes contra os vírus e os vermes, os usuários devem ter programas antivírus instalados e atualizados em seus computadores.

2.2.3 Condutas Classificadas como "Crimes Impróprios de Informática"

A seguir são apresentadas condutas que trazem danos a bens jurídicos de terceiros e que podem ser realizadas com ou sem a utilização dos sistemas computadorizados.

2.2.3.1 Furto ou Roubo de Equipamentos

A redução do tamanho dos computadores e de seus componentes facilitou a prática de furto ou roubo desse tipo de equipamento. Os computadores portáteis (*notebooks, palmtops,* etc.), juntamente com os dados e informações contidos neles, são alvos fáceis para ladrões.

Destaca-se que esse furto ou roubo não acarreta somente na subtração do *hardware*, visto que, na maioria das vezes, junto com ele são subtraídos os *softwares,* dados e informações existentes em tal equipamento.

Hodiernamente, esse crime é tão comum que existem quadrilhas especializadas em furto ou roubo de *notebooks* nos aeroportos brasileiros.

2.2.2.2 Furto ou Roubo de Dados e Informações

Assim como qualquer bem, dados e informações podem ser objetos de furto ou de roubo. As pessoas que acessam sistemas sem a autorização de seus proprietários, muitas vezes, o fazem para furtar esses bens intangíveis.

Furto e roubo são crimes previstos no CP, nos artigos 155 e 157, respectivamente. Assim, não há porque se considerar essas condutas como crimes de Informática. Simplesmente o objeto desses crimes pode ser um ou alguns dos elementos que compõem os sistemas computadorizados.

Destaca-se que a prática de roubo de dados e informações não é muito freqüente, porém é possível sua configuração, já que, por exemplo, pode-se invadir uma empresa e sob ameaça física obter seus dados.

2.2.3.3 Privacidade

A questão da privacidade, segundo Stair (1998), trata, basicamente, da coleta e mau uso de dados. Dados sobre as pessoas são constantemente coletados, armazenados e distribuídos por redes facilmente acessíveis, sem o conhecimento ou o consentimento da pessoa a quem eles se referem ou a quem eles pertençam.

De acordo com Moraes (2005), a garantia constitucional do sigilo de dados foi trazida com a Constituição Federal de 1988.

A inviolabilidade do sigilo de dados está prevista no art. 5º, XII, CF e complementa a previsão ao direito à intimidade, determinando ser "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" (NERY JUNIOR e NERY, 2006) e à vida privada, previsto no art. 5º, X, CF que determina: "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação".

Pinho (2003) afirma que o direito à privacidade, dentro da sistemática estabelecida pela CF, trata de uma denominação genérica que compreende a tutela da intimidade, da vida privada, da honra e da imagem das pessoas e destaca que "em razão dos avanços tecnológicos, com a possibilidade crescente de intromissão na vida íntima das pessoas, é indispensável assegurar-se, entre os direitos individuais, o respeito à privacidade de cada ser humano".

A intimidade e a vida privada são círculos concêntricos da esfera de reserva da vida pessoal, sendo a intimidade mais restrita, por se referir ao próprio indivíduo, bem como ao que possui de mais próximo como seus segredos, seus desejos e seus relacionamentos sexuais. Já a vida privada abrange o relacionamento do indivíduo com outras pessoas, tais como seus familiares, seus amigos e seus sócios (PINHO, 2003).

A defesa da privacidade deve proteger a pessoa contra (NERY JUNIOR e NERY, 2006): a) a interferência em sua vida privada, familiar e doméstica; b) a ingerência em sua integridade física ou mental, ou em sua liberdade intelectual e moral; c) os ataques à sua honra e reputação; d) a sua colocação em perspectiva falsa; e) a comunicação de fatos relevantes e embaraçosos relativos à sua intimidade, f) o uso de seu nome, identidade e foto; g) a espionagem e a espreita; h) a intervenção na correspondência; i) a má utilização de informações escritas e orais; j) a transmissão de informes dados ou recebidos em razão de segredo profissional.

Honra, em termos jurídicos, é o "conjunto de atributos morais, físicos e intelectuais que tornam uma pessoa merecedora de apreço no convívio social e que promovem em sua auto-estima" (NERY, apud MENDES, 2005).

A honra, segundo Pinho (2003), é um atributo pessoal que compreende a consideração que ela tem de si mesma, a sua auto-estima, o seu amor-próprio, que é a chamada "honra subjetiva", e a consideração de que ela goza no meio social, ou seja, a imagem que a pessoa tem perante a sociedade, a sua reputação, também conhecida como "honra objetiva". A legislação penal tutela a honra, estabelecendo os crimes de calúnia, difamação e injúria em diversos estatutos legais, dentre eles: CP, arts. 138 a 140; Código Eleitoral - Lei nº 4.737/65, arts. 324 a 326 e Lei de Imprensa – Lei nº 5.250/67.

Nery Junior e Nery (2006) destacam que a ofensa à honra, liberdade ou intimidade das pessoas enseja indenização por dano moral e patrimonial.

Conforme Araújo Nunes (apud PINHO, 2003), o direito à imagem tem dupla acepção: 1) retrato físico ou imagem-retrato - é a representação gráfica, fotográfica, televisionada ou cinematográfica de uma pessoa, ou seja, é o direito de não ter sua representação reproduzida por qualquer meio de comunicação sem a devida autorização; 2) retrato social ou imagem-atributo – forma pela qual uma pessoa é vista no meio social em que vive. A imagem de bom profissional, de pessoa de boa índole, leal e honesta, é construída ao longo dos anos, não podendo ser atingida por notícia difamatória veiculada de forma precipitada. A Súmula 227 do STJ determina que a pessoa jurídica também pode sofrer danos morais (NERY JUNIOR e NERY, 2006).

2.2.3.4 Pirataria de *software*

No Brasil, a pirataria de *software* é tratada como propriedade intelectual e, como tal, é considerada um bem jurídico tutelado pelo Direito.

Assim como os livros e filmes, os programas de computador (*software*) são protegidos por leis de direitos autorais. Normalmente, pessoas que jamais pensariam em plagiar uma obra escrita por outro autor não hesitam em usar e copiar programas pelos quais nada pagaram. As pessoas que fazem essas cópias ilegais são chamadas de "piratas", e o ato de realizar tais cópias chama-se "pirataria de *software*".

Quem adquire um *software* recebe, somente, o direito de utilizá-lo sob certas condições, ou seja, não o possui de fato. Geralmente, essas condições permitem que seja feita uma cópia de segurança (*backup*) para uso no caso da ocorrência de problemas ou de destruição do programa original. Qualquer cópia além dessa é passível de sanção.

A legislação especial que trata sobre a pirataria de *software* é a Lei nº 9.609/98, chamada de Lei do *Software.*

3 CONSIDERAÇÕES FINAIS

O Código Penal brasileiro foi elaborado em 1940, quando o legislador daquela época visou o bem a ser protegido, na definição de cada crime. Desse período para os dias atuais inúmeras mudanças ocorreram na sociedade, principalmente quanto ao desenvolvimento tecnológico e, mais especificamente, quanto à Informática, e percebe-se que esta mudança não foi acompanhada pela legislação pátria.

A tecnologia da informação passou a ser utilizada não somente com os fins para os quais ela foi desenvolvida, tornando-se poderosa "arma" para a prática de crimes e de condutas lesivas a diversos bens jurídicos se utilizada por pessoa mal intencionada.

Com o desenvolvimento deste trabalho verificou-se que a evolução da informática proporcionou uma nova dimensão à criminalidade, pois a TI trouxe um *modus operandi* distinto daquele amplamente conhecido pelos operadores do Direito. Nos crimes cometidos por meio de computador, não há contato direto entre autor e vítima, o contato é apenas virtual, e os meios de execução foram simplificados a um aparato eletrônico.

Com a utilização dos sistemas computadorizados, os agentes podem cometer, além de crimes impróprios de informática - aqueles podem ser realizados com ou sem a utilização do computador, tais como os contra a honra e a prática de pornografia infantil, os específicos ou

próprios - os que só podem ser realizados através desse tipo de sistema, tais como o acesso ao sistema alheio para furtar, alterar, danificar, excluir ou transferir dados sem a autorização do proprietário.

O crescimento desenfreado da utilização da Informática obriga os aplicadores do Direito a uma adaptação forçada, ou seja, se tenta, na medida do possível, enquadrar as práticas cometidas por meio dos sistemas computadorizados nos tipos penais existentes, descritos na legislação penal brasileira, já que, em âmbito legislativo, as adaptações não acontecem no mesmo ritmo.

Assim, verifica-se que a falta de um enquadramento da conduta lesiva aos tipos penais existentes no ordenamento jurídico brasileiro pode levar à impunidade de seus agentes. Por isso, torna-se imperioso o desenvolvimento de uma legislação específica ou a adequação da existente com relação aos chamados crimes de informática.

REFERÊNCIAS

CAPEZ, Fernando. **Curso de direito penal:** parte geral. 12. ed. São Paulo: Saraiva, 2008. v.1.

COSTA, Marco Aurélio Rodrigues da. Crimes de Informática . **Jus Navigandi**, Teresina, ano 1, n. 12, maio 1997. Disponível em: <http://jus2.uol.com.br/doutrina/texto.asp?id=1826>. Acesso em: 11 mar. 2009.

GOUVEIA, Flávia. Tecnologia a serviço do crime. **BR – Notícias do Brasil.** Disponível em: <http://www.cienciaecultura.bvs.br/pdf/cic/v59n1/aobv59n1.pdf>. Acesso em: 07 abr. 2007.

JESUS, Damásio . **Código penal anotado.** 13. ed. São Paulo: 2002.

LAUDON, Kenneth C.; LAUDON, Jane P. **Sistemas de informação com Internet**. 4. ed. Rio de Janeiro: LTC, 1999.

MENDES, Carolina de Aguiar Teixeira. Perfil: *Orkut*. **Jus Navigandi.** Teresina, ano 10, n. 883, 3 dez. 2005. Disponível em: <http://jus2.uol.com.br/doutrina/texto.asp?id=7631>. Acesso em: 09 abr. 2007.

MIRABETE, Julio Fabbrini. **Manual de direito penal**. 25. ed. São Paulo: Atlas, 2007. v.1.

MORAES, Alexandre. **Direito constitucional.** 18.ed. São Paulo: Atlas, 2005.

NERY JUNIOR, Nelson; NERY, Rosa Maria de Andrade. **Constituição federal comentada e legislação constitucional.** São Paulo: Revista dos Tribunais, 2006.

O'BRIEN, James A. **Sistemas de informação e as decisões gerenciais na era da Internet.** São Paulo: Saraiva, 2001.

PINHO, Rodrigo César Rebello. **Teoria geral da Constituição e direitos fundamentais.** 4.ed. São Paulo: Saraiva, 2003.

PINTO FERREIRA, Lóren Formiga. **A Eficácia da Lei Penal Brasileira Frente aos Crimes Praticados Por Intermédio dos *Sites* de Relacionamento.** Bagé: URCAMP, 2007. Monografia, Faculdade de Direito, Universidade da Região da Campanha, 2007.

PIRAGIBE, Clélia. **Indústria da Informática:** Desenvolvimento Brasileiro e Mundial. Rio de Janeiro: Campus, 1985.

ROSA, Fabrízio. **Crimes de informática.** 2.ed. Campinas: Bookseller, 2005.

SILVA, Rita de Cássia Lopes. **Direito penal e sistema informático.** São Paulo: Revista dos Tribunais, 2003.

STAIR, Ralph M. **Princípios de sistemas de informação: uma aborgagem gerencial**. 2ª ed. Rio de Janeiro: LTC, 1998.

VIANNA, Túlio Lima. **Fundamentos de Direito Penal Informático.** Rio de Janeiro: Forense, 2003.