Há cerca de dez anos a Internet se tornou um dos maiores meios de divulgação e fonte de pesquisas, saciando a necessidade do homem pela busca de informações. Por meio dela, realizam-se as trocas, as compras, transmitimos e recebemos informações e dados o tempo todo. E é justamente por meio de todo esse potencial que surgem, no dia-a-dia, programas com o intuito de sabotar, prejudicar e espionar informações sigilosas de pessoas físicas e jurídicas, se enquadrando na maioria das vezes em algum crime informático, afinal, o mundo virtual já conta com milhões de pessoas conectadas em toda parte do planeta, e o computador é usado por todas as classes sociais, pelos setores públicos e privados, sendo que quase tudo o que se faz hoje passa por um computador.

A informática já está presente em quase toda a nossa vida. Mas, mesmo com toda essa evolução e avanço tecnológico, não se conseguiu impedir os crescentes aumentos dos índices de crimes cibernéticos. Trata-se de crime informático qualquer conduta ilegal, não ética, ou não autorizada que envolva o processamento automático de dados e/ou transmissão de dados (GUIMARÃES; FURLAN NETO, 2003), podendo ser classificado em crime virtual puro, o qual atenta contra o hardware e/ou software de um computador, ou seja, tanto a parte física quanto a tecnológica do microcomputador; crime virtual misto, que é tipificado como as transações ilegais de valores de contas correntes, e o crime virtual comum, quando se utiliza a Internet apenas como forma de instrumento para realizar um delito que se enquadra no Código Penal.

O crime por computador pode acarretar danos tanto pessoais como empresariais. Os danos pessoais são obtidos no envio de mensagens com conteúdo pejorativo, falso ou pessoal em nome da pessoa, utilizando somente os dados dos e-mails; na movimentação de contas bancárias com o intuito de fazer transações, saques ou até mesmo pagamento de contas; na utilização de dados de cartão de crédito para fazer compras e na divulgação de fotos ou imagens com intenção de causar danos morais.

O criminoso informático é denominado vulgarmente de hacker, e este pode ser classificado em dois tipos: interno e externo.

Interno é aquele indivíduo que acessa indevidamente informações sigilosas de um nível superior. Normalmente é funcionário da empresa ou servidor público.

O externo é aquele que não tem acesso e utiliza um computador ou redes externas, ressaltando que não tem ligação à organização que ataca.

Outras condutas, de acordo com Guimarães e Furlan Neto (2003), são também consideradas crimes informáticos, tanto pessoais como empresariais: spamming: conduta de mensagens publicitárias por correio eletrônico para uma pequena parcela de usuários. Esta conduta não é ilícita, mas sim antiética; cookies: também chamados de “biscoitinhos da web”, são arquivos de textos que são gravados no computador de forma a identificá-lo com um número único; spywares: são programas espiões que enviam informações do computador do usuário para desconhecidos na rede; hoaxes: são e-mails, na maioria das vezes, com remetente de empresas importantes ou órgãos governamentais, contendo mensagens falsas, carregadas de vírus; sniffers: são programas espiões semelhantes ao spywares que são introduzidos no disco rígido para ter controle e leitura de e-mail; trojan horse ou cavalos de Tróia: quando instalado no computador permite o total controle do terminal.

O hacker pode obter informações de arquivos, descobrir senhas, introduzir novos programas, formatar o disco rígido, ver a tela e até ouvir a voz, caso o computador tenha um microfone instalado. Como a boa parte dos microcomputadores é dotada de microfones ou câmeras de áudio e vídeo, o trojan permite fazer escuta clandestina, o que é bastante utilizado entre os criminosos que visam à captura de segredos industriais; pornografia infantil: com a Internet ficou mais fácil a troca de vídeos e revistas, e aumentou o contato entre os pedófilos e pessoas que abusam sexualmente de crianças e adolescentes; jogos de azar: o jogo eletrônico surgiu na Internet à medida que ficou mais fácil a transferência de créditos e fundos; pirataria de programas: baixar músicas e filmes na Internet para depois copiar em CD ou DVD, com a

intenção de comercializá-los.

Na ausência de uma legislação específica, aquele que praticou algum crime informático deverá ser julgado por meio do próprio Código Penal, mantendo-se as devidas diferenças.

Atualmente, observamos que a segurança não é levada tão a sério quando se navega nesse universo por meio de um “click”, provavelmente por ser a informação ou dado “clicado” intangível. Porém, os recursos, que essa nova tecnologia nos oferece, nem sempre são empregados com o fim adequado e, nesse ambiente virtual, os “crimes informáticos” (termo utilizado pelo Centro de Estudos, Respostas e Tratamentos de Incidentes de Segurança no Brasil) podem ocorrer com alguns “clicks”, por meio de uma palavra digitada “inocentemente”, um “e-mail” ou um “arquivo” enviado erroneamente.

Na miríade de opções, que o mundo virtual nos proporciona, temos o “Orkut” (Comunidade Virtual de Relacionamentos), um ambiente originalmente criado para integração e que gradativamente cede o lugar do seu objetivo inicial de integrar as pessoas, pois vem criando um espaço de diversas apologias e a prática de crimes informáticos que afrontam o direito de personalidade preconizado no Código Civil Brasileiro.

Em se tratando da utilização dessa ferramenta tecnológica (Orkut) por meio dos/das professores/as, os/as quais “adicionam” alunos/as “crianças e adolescentes” (menores de 18 anos) como seus/suas amigos/as e membros de comunidade, sabendo que esses/essas não

poderiam estar cadastrados em tais ferramentas, pois “aumentam” suas idades para terem seus cadastros aceitos, não estariam como “educadores” agindo de forma errada? Como ficaria a questão moral e ética desses profissionais de ensino? E ainda, como ficaria, se um/a aluno/a, ao visitar o endereço de seu/sua professor/a, verifica uma imagem de seu professor/a “em trajes íntimos”? E se o perfil desse/dessa professor/a for “clonado/a” por um/uma aluna/o, o/a qual deseja prejudicar tal profissional por ter recebido/a uma nota baixa, criando então uma comunidade que injurie, calunie e difame esse/essa professor/a? O que a escola poderia fazer? Afinal, esse mundo virtual, parecer “não ter fronteiras”, tido como “terra de ninguém”, pois não existe controle sobre o que se publica nessa ferramenta virtual, afinal casa usuário tem liberdade total de escrever o que quiser, seja de uma maneira positiva ou negativa. E até que se prove o contrário, o profissional que tem a sua imagem profissional afetada, poderá perder muitas oportunidades em seu campo de trabalho, pois como educadores, temos que ter ciência dos perigos que o mundo virtual nos apresenta e ainda temos a “obrigação” de orientar nossos alunos para esses perigos para que não insiram nos sites de relacionamento: fotos (que podem ser copiadas e utilizadas em perfis falsos), dados pessoais (endereço, telefone, local de trabalho ou estudo), dados reais dos locais que freqüenta ou estuda (exposição de seu cotidiano) e principalmente tomar cuidado com o que se escreve nesses sites (scraps), pois poderá ser utilizado contra o próprio criador do scrap.

Ainda com relação ao enquadramento dos crimes informáticos, poderíamos complementar, afirmando que eles enquadrar-se também em uma categoria especial de delitos, tutelados pela ordem jurídica brasileira por meio do Código Penal Brasileiro, em seu Capítulo V — Dos Crimes Contra a Honra, entendendo 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.

Cabe-nos mencionar ainda que tais delitos não estão imunes a possíveis sanções por crimes que são praticados com o auxílio da Internet. Atualmente temos um canal de comunicação entre o cidadão e a Polícia, denominada de Delegacia Virtual, criada para apresentações de queixas, informes, denúncias e registro de crimes cometidos por meio de computadores ligados à Internet. Tal Delegacia possui como “clientela interna” a própria Polícia, pois a partir de uma

queixa crime, demandada em uma Delegacia Comum, esta irá auxiliar investigando e rastreando suspeitos para que sejam processados, atuando como uma facilitadora de todas as delegacias. Na cidade de Curitiba, temos o NUCCIBER, Núcleo de Crimes Informáticos, o qual é responsável por “fiscalizar” uma denúncia anônima, ou seja quando não sabemos o autor de um delito virtual, esse Núcleo rastreia o “IP” da máquina e mesmo vindo de uma “lan house” o autor poderá ser descoberto.

De acordo com o Delegado Demetrius do NUCCIBER/PR, quando nos depararmos com um “crime informático” contra nossa pessoa, devemos nos dirigir a um Cartório e fazermos uma “Ata Notarial”, ou seja “iremos acessar a página que está sendo veiculada no site de relacionamento, e o cartorário irá copiar tais páginas e arquivá-las, dando-lhes “fé pública”. Munidos com esse documento de comprobatórios nos dirigirmos até a Delegacia Comum (caso não tenha em sua cidade uma Delegacia Especializada), apresentando uma queixa-crime, tendo ainda como opção, após a identificação do autor, de ingresso com uma ação na esfera civil, por danos morais comprovando a autoria e a materialidade do fato.