

CRIMES NA INTERNET

Felipe Augusto Basílio*

1. A RELAÇÃO ENTRE DIREITO PENAL E INFORMÁTICA

O estudo do direito em relação à informática apresenta-se como uma das tarefas mais árduas, já que ambos se baseiam em ramos do conhecimento completamente distintos, capazes cada qual, de ocupar vidas inteiras de dedicação: de um lado as letras, a interpretação, a função social a equidade e a justiça acima de tudo, do outro, a frieza da máquina, a exatidão e a velocidade. Não se discute mais a consolidação, importância e atuação da informática na sociedade. Com o advento da Internet, as pessoas mudaram seus costumes, fazendo surgir, por consequência um novo tipo de criminoso.

O direito brasileiro, somente agora, parece estar despertando para tal situação, porém escassa ainda é a legislação específica para punir o criminoso que se utiliza das máquinas, sendo que muitos atos danosos ainda ficam sem previsão legal. Isso se dá, principalmente, em função do princípio do *nullum crimen, nulla poena sine lege* que impossibilita a incriminação por analogia, na ausência de lei específica. A doutrina, por sua vez, também ignora o problema não se dispondo a superar as barreiras impostas pela falta de conhecimento técnico na área de informática. A jurisprudência ainda não tem posição consolidada na maioria dos aspectos, sendo assim não tem se manifestado de maneira eficiente e definitiva.

O grande desafio, ao se lidar com o tema, é compreender quais os bens protegidos, já que, tradicionalmente, o Direito Penal lida com a proteção de objetos tangíveis. O Direito Penal da Informática, ao contrário, lida com conceitos intangíveis visto que os bens ora estudados são “Sistemas de Informática”, “Integridade da Informação”, “Dado”, “Privacidade”, etc.

Pesquisas do Centro Nacional de Dados sobre Crimes por Computador, nos Estados Unidos, revelam que 75% dos crimes são cometidos por funcionários ou ex-funcionários contra seus empregadores. Outras vezes, são jovens amadores, na faixa etária de 13 a 18 anos, que agem simplesmente para se orgulhar de seus feitos. Hoje os crimes podem ser praticados por qualquer pessoa, devido a facilidade de operação e acesso à Internet o que ensejou uma disseminação dos crimes.¹

Do outro lado, estão as vítimas, que na maioria das vezes nem ficam sabendo que estão sendo atingidas, ou, ao saberem, preferem se calar e arcar com os prejuízos, sendo as instituições financeiras o alvo principal dos criminosos altamente especializados

* Bacharelado em Direito, pela Faculdade de Direito Padre Anchieta de Jundiá, Técnico em Processamento de Dados formado pelo Centro Paula Souza, Escola Técnica Vasco Venchiarutti.

¹ Sandra Gouvêa, *O direito na Era Digital*. Rio de Janeiro: Mauad, 1997, p. 59

Desde que seja usuário da Internet, qualquer pessoa ter seus dados destruídos ou danificados por vírus, ter seu número de cartão de crédito e informações bancárias descobertas ou ter sua honra ofendida criminosamente.

2. JURISDIÇÃO E TERRITORIALIDADE NA INTERNET

Sob quais leis estará subordinada uma pessoa que divulgue via Internet uma mensagem difamatória sobre um cidadão dinamarquês, escrita em Cingapura, lida por alguém no Brasil, através de um servidor localizado nos Estados Unidos ?

Segundo a doutrina tradicional, quatro princípios são apontados acerca da eficiência da lei penal no espaço: o da territorialidade, o da nacionalidade, o de defesa e o da justiça universal.²

No Brasil, a eficácia espacial da lei penal é determinada nos artigos 5º e 6º do Código Penal, onde se consagra o princípio da territorialidade. O artigo 6º, abrigou a teoria da ubiqüidade, que tem por lugar do delito aquele que for realizado qualquer um de seus elementos integrantes, seja o da execução ou o momento consumativo. Basta que tenha ocorrido qualquer parcela de atividade do agente ou qualquer efeito que integre o resultado do crime, para que se puna pela lei brasileira o delito como um todo. Também se refere a lei à tentativa de prática do crime ao inserir no artigo 6º a expressão “ou deveria produzir o resultado”.

O aspecto mais relevante da norma a ser analisado diante de crimes na Internet se refere à segunda parte do artigo, principalmente, em relação aos crimes contra a honra, que diferentemente de um ataque a um servidor ou uma apropriação de dados em que a consumação é imediata e tem destino certo, em geral, não possuem um local específico para surtir efeito, pois se consomem no momento em que a ofensa chega ao conhecimento de terceira pessoa no caso da calúnia e difamação e ao conhecimento do ofendido no caso da injúria. Caso contrário, configuram-se apenas na forma tentada. Sendo assim, pela regra da última parte do artigo 6º que diz: “*onde se produziu ou deveria produzir o resultado*” pode-se concluir que se a ofensa vier ou puder ser acessada pela Internet em território brasileiro, no caso dos crimes contra a honra, o crime estará se consumando aqui, podendo ser julgado pela justiça e lei nacionais.

Além disso, ainda que o crime tenha sido praticado no estrangeiro, o artigo 7º de nosso Código Penal trata de diversos casos em que se constituem exceções ao princípio da territorialidade, alcançando então a lei brasileira o delinqüente. São esses os chamados “casos de extraterritorialidade” e valem-se do princípio *real* tendo em vista a relevância das objetividades jurídicas ou bens-interesses tutelados.

Na prática, o princípio da ubiqüidade, no caso da Internet, pode gerar controvérsias, pois os países que adotam esse princípio podem considerar delitos cometidos como tendo ocorrido também em seu país. Considerar como local do crime o

² Edgard Magalhães Noronha, Direito Penal, São Paulo: Saraiva, 1998, Volume I, p. 84

lugar onde está o autor, facilitaria aspectos processuais como a prova, bem como a aplicação da pena a ele cabível, sem necessidade de extradição.

Sobre a jurisdição no ciberespaço, o professor Henry H. Perritt, da Villanova Law School, na Pensilvânia, elaborou tese elencando a arbitragem, instituição de cortes internacionais e elaboração de leis específicas como opções para solucionar os problemas a ela atinentes.

Recentemente, no dia 23 de novembro de 2001, em Budapeste, foi assinado um tratado internacional para combater o cibercrime por representantes do Conselho da Europa (CoE). Essa convenção é o primeiro tratado internacional em crimes cometidos pela Internet e computadores ligados em rede, tratando especificamente de infrações de direitos autorais, fraudes, pornografia infantil e violações de segurança de rede. Seu objetivo principal é uma política criminal dirigida ao cibercrime, adotando legislação apropriada e cooperação internacional. A Convenção é o produto de quatro anos de trabalho de peritos do Conselho da Europa e também pelos Estados Unidos, Canadá, Japão e outros países que não são os sócios do Conselho.³

3. DOS CRIMES DE INFORMÁTICA IMPRÓPRIOS

Os crimes que estão dentro dessa classificação podem ser praticados independentemente de se utilizar os sistemas informatizados, porém, esses são usados como mera ferramenta ou meio para o cometimento. Tais delitos violam bens já protegidos pela legislação penal e dentre esse podem ser citados: crimes contra a honra, ameaça, interceptação de e-mail, divulgação de segredo, furto, envio de vírus, apropriação indébita, estelionato, violação de direito autoral, escárnio por motivo de religião, apologia de crime ou criminoso, jogos de azar, pedofilia, pirataria dentre outros. A seguir, uma breve análise daqueles que expressam maior relevância atualmente.

3.1 FURTO

Pacífico é o entendimento de que o furto pode se configurar através da internet pois conforme o § 3º do artigo 155 do Código Penal é necessário que a coisa subtraída tenha valor econômico, ou seja, configura o crime a transferência ilícita de dinheiro entre contas correntes, o furto de arquivos e dados confidenciais, senhas dentre outras coisas que expressem valor.

Porém, as instituições bancárias, por exemplo, ao serem vítimas de furto, através da rede e ataque de hackers, acabam, em sua maioria, arcando com os prejuízos com intuito de evitar que suas vulnerabilidades se tornem públicas.

3.2 ESTELIONATO

O crime de estelionato, previsto no artigo 171 do Código Penal, pressupõe a

³ CEBEJI – Centro Brasileiro de Estudos Jurídicos da Internet, www.cbeji.com.br/legislacao, acesso em 03/2002.

vantagem ilícita e o prejuízo alheio como resultados obtidos mediante artifício, ardil ou qualquer meio fraudulento, meios esses que podem utilizar a Internet como instrumento.

É neste tipo penal que os criminosos vêm mais desafiando a Polícia com ações arrojadas pela Internet. Recentemente, uma mensagem falsa, enviada em nome do UOL para cerca de 10 mil assinantes pedia o cadastramento dos mesmos, indicando o link para uma página falsificada do Universo Online. Nessa página, pedia-se o número do cartão de crédito do assinante. Conforme apurou a polícia paulista, os dados eram enviados para um provedor nos Estados Unidos, sendo que seriam utilizados para compras através da Internet. Uma assinante de Pernambuco, caiu no golpe e teve cerca de mil dólares debitados em seu cartão de crédito correspondentes a compras feitas naquele país.⁴

3.3 SEDUÇÃO

Uma menor brasileira, estudante, desapareceu em maio de 2001, no trajeto entre sua casa e a escola no Rio de Janeiro. Segundo sua mãe, a menina vinha freqüentando salas de bate-papo na Internet, onde conheceu um homem de 25 anos, com quem passou a se corresponder. A menina provavelmente o encontrou escondido da mãe e um dia antes de desaparecer chegou a comentar com um amigo do colégio que estava querendo romper um namoro com um homem mais velho que conhecera na Internet, mas que este estava se recusando e a seguindo por toda a parte.⁵

Casos como esses não são raros e aumentam a cada dia. O Código Penal pátrio tutela a prática de sedução em seu artigo 217. Cita Julio Fabbrini Mirabete, em sua obra que o tipo objetivo é seduzir a menor, levando-a à prática de conjunção carnal, sendo que seduzir é atrair, dominar, desviar, convencer e viciar a vontade da mulher. É exatamente nesta parte do tipo que a Internet pode ser usada pelo sujeito ativo, sendo este o primeiro passo para um posterior contato físico. Essa sedução pode ser simples, por utilização da palavra, juras de amor, ou a sedução qualificada, com promessa séria de casamento, namoro ou noivado.⁶

3.4 PEDOFILIA

Historicamente, todos os meios de comunicação já foram usados como forma de propagação da pornografia. Como é óbvio, a Internet também passou a servir como meio de veiculação da pornografia, principalmente após o desenvolvimento de seu potencial multimídia. A pornografia na Rede passou basicamente por três evoluções tendo seu auge com a pedofilia e materiais obscenos em geral. O material pedófilo é disseminado por uma comunidade fechada e altamente organizada, relacionando-se com empresas que cobram pelo serviço. Tais empreendimentos

⁴ Revista Consultor Jurídico, www.uol.com.br/consultor, acesso em 14/02/2001.

⁵ Wal Ribeiro, Quem Cai na Rede é Peixe, www.kids-denuncia.org.br, acesso em 04/2002.

⁶ Julio Fabbrini Mirabete, Código Penal Interpretado, São Paulo: Atlas, 2001, p. 1478.

têm se mostrado de grande sucesso, principalmente em vista do anonimato que a Internet proporciona, de modo que essas atividades são praticadas sem deixar “rastros”.⁷

Pedofilia é um distúrbio de conduta sexual, onde o indivíduo adulto sente desejo compulsivo, por crianças ou pré-adolescentes. As estatísticas têm mostrado que 80 a 90% dos contraventores sexuais não apresentam nenhum sinal de alienação mental, agindo pelo livre arbítrio, ou seja, são juridicamente imputáveis.

O abuso sexual contra crianças é uma das mais rentáveis indústrias globais estimando-se lucros em torno de US\$ 5 bilhões por ano.⁸ O ordenamento jurídico brasileiro condena tal prática desde a sua Lei Maior, a Constituição Federal, no seu artigo 227. Por sua vez, o Estatuto da Criança e do Adolescente estabelece no artigo 241 a proibição de fotografar ou publicar cena de sexo explícito ou pornográfica envolvendo criança ou adolescente, cominando pena de detenção de seis meses a dois anos, e multa.

Segundo o festejado Nelson Hungria, publicar significa tornar público, permitir o acesso ao público, o sentido de um conjunto de pessoas, pouco importando o processo de publicação⁹, ou seja, a Internet é meio em potencial para o cometimento desse crime. Importante observar que é indiferente o número de internautas que acessem a página e ainda que ninguém tome conhecimento de seu conteúdo, as imagens estarão à disposição, consumando a infração. O conteúdo do tipo é alternativo, bastando que se cometa apenas uma das condutas nele descritas: fotografar ou publicar, sendo que há a presunção legal de dano causado à vítima independente deste ter se caracterizado ou não.¹⁰

A jurisprudência pátria também já tem se manifestado sobre o tema sendo que recente julgado do Supremo Tribunal Federal considerou que a conduta de publicar cenas de sexo infanto-juvenil na Internet, fere o artigo 241 do Estatuto da Criança e do Adolescente, até porque, basta para a consumação do crime, a realização de seu núcleo, ou seja, publicar.¹¹

Vários projetos de lei têm sido criados a fim de regular mais especificamente o tema. Dentre eles, destaca-se o Projeto de Lei nº 5165 de 2001 que pretende dar nova redação ao Estatuto da Criança e Adolescente.

3.5 INTERCEPTAÇÃO DE COMUNICAÇÕES E E-MAIL

Incontáveis são as vantagens de se comunicar através dos recursos de informática e em especial pela Internet, através de conversas on line, transferência

⁷ Gustavo Testa Corrêa, Aspectos Jurídicos da Internet, São Paulo: Saraiva, 2000, p. 44.

⁸ Sandro D'Amato Nogueira, Polícia tem dificuldades para chegar aos pedófilos, www.direitonaweb.com.br, acesso em 28/03/2002.

⁹ Nelson Hungria, Comentários ao Código Penal, Rio de Janeiro: Forense, 1958, Volume VII, p. 340.

¹⁰ Carla Rodrigues Araújo de Castro, Crimes de Informática e Seus Aspectos Processuais, Rio de Janeiro: Editora Lumen Júris, 2001, p. 45.

¹¹ STF, Julgamento em 22/09/1998, Primeira Turma. Publicado no DJ em 06/11/1998, p. 3, ement. Vol. 1930-01, p.70. Origem HC nº 76.689/PB.

de arquivos e principalmente e-mail. Com o correio eletrônico, pode-se enviar uma mensagem para qualquer usuário da rede e em questão de minutos, chegará ao destino. O sigilo de correspondências e comunicações constituem garantia constitucional no direito brasileiro que consagra a condenação à sua violação no artigo 5º, XII. Correspondência nada mais é do que uma troca de informações entre pessoas ausentes que pode ser feita por cartas, bilhetes telegramas e, atualmente, por computador.¹²

Nota-se que o legislador estava atento às novas tendências referentes aos modernos meios de comunicação, incluindo no texto constitucional a inviolabilidade de dados, o que por óbvio abrange os e-mails, que nada mais são que meios de transmissão de dados.

Apesar da presente omissão do Código Penal, que só tutela a violação de correspondência comum, a violação de e-mails e dados não estão fora da esfera penal, visto que a Lei 9.296 de 24 de julho de 1996, veio a regulamentar o artigo 5º, XII da Constituição Federal, em seu artigo 10 que dizendo que *“constitui crime realizar a interceptação de comunicações telefônicas, de informática e telemática, ou quebrar segredo de Justiça, sem autorização judicial ou com objetivos não autorizados em lei”*.

A conduta típica é a interceptação da comunicação por qualquer meio, caracterizando-se o ilícito penal ainda que não haja divulgação ou transmissão a terceiro. Interceptar é captar ou conhecer o conteúdo da comunicação feita pelos meios da informática. Para tais condutas, prevê a lei a pesada pena de dois a quatro anos de reclusão e multa, sendo que para sua caracterização, é necessário o dolo do agente.

Ainda a esse respeito, a violação de dados de informática e e-mail poderiam ser enquadrados nas disposições do Código Brasileiro de Telecomunicações, Lei 4.117/62, em seu artigo 56 que estabelece que *“pratica o crime de violação de telecomunicações quem, transgredindo lei ou regulamento, exiba autógrafa ou qualquer documento ou arquivo, divulgue ou comunique, informe ou copie, transmita a outrem ou utilize o conteúdo, resumo, significado, interpretação, indicação ou efeito de qualquer comunicação dirigida a terceiro.”*

3.6 DANOS CAUSADOS POR VÍRUS

Vírus são programas desenvolvidos para alterar o funcionamento de um computador de forma nociva. Propagam-se automaticamente, por meio de disquetes, arquivos compartilhados, pelas redes corporativas e pela Internet, sendo esta última a maior via de propagação atual. Segundo dados atuais do Computer Economics, o balanço final sobre o prejuízo causado pelas pragas virtuais em 2001 aponta perdas avaliadas em US\$ 13,2 bilhões. A pesquisa aponta o vírus CodeRed como a

¹² Aurélio Buarque de Holanda Ferreira *Novo Dicionário Aurélio da Língua Portuguesa*, Rio de Janeiro: Nova Fronteira, 1986, p. 484.

maior ameaça, gerando prejuízos de US\$ 2,62 bilhões.¹³ Diante de tais números representando prejuízos, é evidente que o envio de vírus e similares é conduta criminosa. Porém, na ausência de tipo penal específico e mais rigoroso, aplica-se o artigo 163 do Código Penal, que estabelece o crime de dano.

A conduta típica de tal crime é “inutilizar coisa alheia”, que significa tornar inútil, imprestável e inservível. Como se sabe, a maioria dos vírus tem essa finalidade, destruindo dados e por consequência inutilizando planilhas, arquivos de texto e o próprio computador infectado, sobrevivendo em consequência, os prejuízos econômicos. Como se observa, a pena de detenção de 1 (um) a 6 (seis) meses é muito pequena em vista dos prejuízos e do potencial ofensivo que tem um vírus de computador.

3.7 CRIMES CONTRA A HONRA COMETIDOS PELA INTERNET

Diariamente, a polícia é procurada por alguém que foi alvo de alguma maldade ou brincadeira ofensiva pela Internet. Para a polícia especializada, a investigação é mais fácil do que se pensa pois se baseia no número IP que o computador recebe e que fica devidamente registrado no provedor a cada acesso à rede.

Os crimes contra a honra podem ser cometidos por **e-mail**. Atualmente, inúmeras empresas como Starmedia e BOL, fornecem serviço de e-mail gratuito, bastando para sua utilização que o usuário faça um simples cadastro, que pode ser preenchido com dados verdadeiros ou não. Para usuários mal intencionados, os serviços de correio eletrônico gratuito podem servir, mais uma vez, como meios para a prática de crimes pois propiciam a sensação de anonimato.

Porém, dentre todos os recursos oferecidos pela Internet, o e-mail é o meio menos eficaz para os crimes contra a honra, visto ter o propósito inicial de estabelecer comunicação entre duas pessoas. Na prática, se uma pessoa envia um e-mail para outra acusando-a injustamente de prática de homicídio, e se só esta ler a mensagem, não há de se falar em crime pois a prática dos crimes de calúnia e difamação, indispensável é que terceiro tome conhecimento das ofensas. Por outro lado, se o mesmo e-mail for enviado propositalmente para terceiro, estariam preenchidos os requisitos para se reconhecer a prática do crime.

Conforme a doutrina de Mirabete, diferente análise deve se fazer a respeito da injúria: *“Consuma-se a injúria quando o sujeito passivo toma conhecimento do **insulto, quando ouve ou lê a ofensa, não sendo necessário que terceiro a perceba. Trata-se de crime formal, em que prescinde o resultado danoso para sua configuração**”* (grifo nosso).¹⁴ Sendo assim, basta que o próprio ofendido tome conhecimento da mensagem ofendendo sua honra, para que o crime se configure, não sendo necessário que terceiro leia o e-mail.

Outro meio idôneo para o cometimento de crimes contra honra são os **chats**.

¹³ www.uol.com.br/mundodigital, acesso em 05/2002

A internet propicia as salas de bate-papo, que nada mais são do que sites criados para possibilitar conversas online entre visitantes, além de programas como o ICQ e MSN, que permitem a várias pessoas trocar mensagens ao mesmo tempo em grupo ou individualmente.

Assim, pode ocorrer de a mensagem trocada ser realmente ofensiva, caracterizando o crime. Quando a ofensa puder ser conhecida por outrem, além do próprio ofendido, consumir-se-á a infração. Mais uma vez, a exigência de publicidade não se dá no caso de injúria.

Grupos de discussão também são verdadeiras “armas” para se ofender a honra de outrem na internet. Estes são espaços públicos na Internet que objetivam o estímulo ao debate de idéias. Seja qual for o método usado pelas listas de discussões, a sua principal característica é a publicidade, alcançando um grande número de destinatários. Atualmente, a maioria dos processos gerados por crimes contra a honra na Internet, se deve a mensagens expostas em listas de discussão.

Bastante controverso ainda é a responsabilidade do provedor que armazena as mensagens do grupo de discussão. Algumas listas possuem o chamado “moderador”, que é a pessoa responsável pela leitura prévia das mensagens julgando se estas são oportunas ou não e se devem ir para o ar, ganhando publicidade.¹⁵ Caso alguma mensagem de conteúdo ofensivo seja publicada após análise do moderador, este poderia ser responsabilizado criminalmente por omissão, tendo em vista sua incumbência de atentar para o conteúdo ofensivo das mensagens que publica. A esse respeito, observe-se o disposto no artigo 13 do Código Penal em seu parágrafo 2º que estabelece que a *omissão é penalmente relevante quando “(...) de outra forma, assumiu a responsabilidade de impedir o resultado.”*

Assim, uma vez tendo o moderador da lista ou os responsáveis pelo serviço avisado que exercerão fiscalização sobre as mensagens a serem publicadas, estão trazendo para si a responsabilidade, e caso não o façam, sua conduta estará perfeitamente enquadrada naquela descrita na alínea “b” do § 2º do artigo 13 do Código Penal, ou seja, sua omissão será penalmente relevante.

Por último, os sites, ou **páginas gráficas**, também fornecem meios para os crimes contra a honra pois dispõem de recursos que podem ser usados dolosamente, quais sejam textos publicados, desenhos, caricaturas, fotos, montagens fotográficas, sons, dentre outros.

Na calúnia em especial, vale dizer que, se a foto publicada for comprovadamente verdadeira e imputar ao sujeito pratica de crime, configura-se a exceção da verdade descaracterizando o crime.

3.8 VIOLAÇÃO DE DIREITOS AUTORAIS

Atualmente, as discussões sobre direitos autorais não mais se enfocam nos

¹⁴ Julio Fabbrini Mirabete, ob. cit, p. 907.

¹⁵ Celso Henrique de Castro Baptista Vallim, Crimes Contra a Honra na Internet, Florianópolis, junho/2000, p.10, monografia, Universidade Federal de Santa Catarina.

velhos, toca-fitas e CDs, mas sim na Internet com sua velocidade de propagação de arquivos e informações e pela sua crescente popularização, principalmente em razão da criação dos arquivos MP3 responsáveis atualmente por um rastro de prejuízo à indústria fonográfica em torno de US\$ 90 milhões.¹⁶

Ao se tratar de obras colocadas na Internet, tem-se a falsa idéia de que as mesmas são de domínio público ou que por ali estarem publicadas, podem ser usadas livremente, presumindo-se que o autor autorizou sua livre utilização. Portanto, cabe aqui a distinção entre “obras em domínio público” e “obras liberadas ao público”.

Uma obra cai em *domínio público* (arts. 41 a 45 da Lei de Direitos Autorais - 9.610/98), quando decorrido o prazo de proteção aos direitos patrimoniais, embora persistam alguns aspectos dos direitos morais, pois estes direitos são perpétuos, não se extinguindo jamais. *Obras liberadas ao público* são, em síntese, aquelas ao qual o público tem acesso por qualquer meio, inclusive a Internet, mas que não têm seu uso liberado. O artigo 29, inciso IX, da Lei de Direitos Autorais disciplina tal matéria estabelecendo que “*depende de autorização prévia e expressa do autor a utilização da obra por quaisquer modalidades*”, o que cria grandes problemas ao se tentar controlar a autorização referente a sua obra no espaço virtual. Assim, permite-se somente que da obra sejam explorados os elementos de utilização livre, estabelecidos no artigo 46 da lei.¹⁷ O artigo 184 da referida lei prevê as sanções penais para os infratores de direitos autorais.

Portanto, independente de estar a obra exposta na Internet, um grande meio de comunicação que atinge enormes índices de popularidade, há de se obter autorização prévia do autor para sua utilização, salvo se estas forem obras em domínio público ou pelas exceções de uso livre, previstas no art. 46 da Lei de Direitos Autorais.

Impossível se falar em violação de direito autorais de obras musicais pela Internet sem se falar do programa Napster que nada mais é do que um canal entre dois internautas que funciona como intermediário para a troca de músicas em formato MP3..

Não há como negar a participação dos criadores do **Napster** nos prejuízos causados a todos os envolvidos no processo fonográfico e detentores dos direitos. Pela análise jurídica, podemos constatar que os criadores são partícipes ou co-autores, pois atuam diretamente no resultado material do delito, não sendo necessária a ação pessoal para que a conduta seja tipificada como tal pois exprimem a vontade livre e consciente dirigida ao fim de violar os direitos autorais dos criadores das obras musicais, facilitando os meios de acesso, ao máximo, para que isto aconteça. A causalidade psíquica, ou seja, a consciência da participação no even-

¹⁶ Nehemias Gueiros Júnior, O som ameaçador da Grande Rede, Revista Consultor Jurídico, www.uol.com.br/consultor, acesso em 22/05/2000.

¹⁷ Obras protegidas - Alberto da Silva Dantas, Revista Consultor Jurídico, www.uol.com.br/consultor, acesso em 23/12/2001.

to, acompanha o nexa causal fazendo uma ponte entre a ação concreta e o resultado pretendido.

A justiça americana julgou procedente o pedido das gravadoras de se restringir o uso do Napster que passou a ser obrigado a “filtrar” os arquivos musicais proibidos e a bloquear o download dos mesmos. Atualmente inúmeros programas similares e até mais poderosos estão surgindo e sendo disponibilizados como é o caso do Kazaa¹⁸, que permite o download não só de música, mas de vários outros tipos de arquivos, como vídeos, por exemplo.¹⁹

4. DOS CRIMES DE INFORMÁTICA PRÓPRIOS

Essa classificação engloba os crimes que só podem ser praticados por meio da informática, sendo impossível a sua existência e consumação fora do âmbito dos computadores. Tais crimes acabam por gerar tipos penais novos que surgiram e estão surgindo diante da necessidade de se tutelar a informática de maneira mais precisa. Dentre esses podemos citar a pirataria de software, o spam a inserção de dados falsos e a modificação de dados em sistema de informação. A seguir, a análise dos mais relevantes dentre esses.

4.1 VIOLAÇÃO DE DIREITOS AUTORAIS SOBRE O SOFTWARE E PIRATARIA

Com o desenvolvimento e popularização dos microcomputadores, junto à indústria e aos usuários domésticos, a partir da década de 70, o software tornou-se um dos bens de maior importância econômica no contexto internacional e brasileiro. Por essa razão, o ordenamento jurídico brasileiro vem tentando desenvolver o sistema mais adequado fundamentando-se em lei específica que qual seja, Lei nº 9.609, de 19 de fevereiro de 1998 (“Lei de Software”).

Tal lei confere prazo de duração da proteção, à propriedade intelectual de programas de computador, é de 50 (cinquenta) anos, sendo seu registro facultativo.

Porém, é cada vez maior o número de casos de pirataria de softwares, principalmente através do uso da Internet resultando atualmente num rombo de 1,1 bilhão de dólares, sendo que a taxa de programas piratas é de 80% em relação aos programas vendidos.

Pirataria é a reprodução de software sem autorização do detentor dos direitos sobre o mesmo, com ou sem finalidade de lucro. A Internet permite que o processo de cópia dos programas violados se simplifique e se torne mais barato, sem que haja a necessidade de quaisquer meios físicos para sua distribuição.²⁰

O capítulo V da referida lei, trata das infrações e das penalidades, sendo que a violação de programa de computador vem disciplinada no artigo 12. A conduta típica punível descrita é “violar”, que significa ofender o direito do autor do software.

¹⁸ www.kazaa.com, acesso em 13/07/2002.

¹⁹ Angela Bittencourt Brasil, A Questão Napster, Revista Consultor Jurídico, www.uol.com.br/consultor, acesso em 27/07/2000.

²⁰ Gustavo Testa Corrêa, ob. cit., p. 47.

A esta conduta cabe detenção de seis meses a dois anos ou multa. Por outro lado, se a violação tiver a finalidade de comércio, conseqüentemente a pena a ser aplicada será maior, ou seja, reclusão de um a quatro anos e multa, conforme disposto nos §§ 1º e 2º.

Ainda, os softwares *shareware*²¹ também podem ser objetos de pirataria, através do uso de programas que rompem seu sistema de segurança (cracks). Uma vez executado o crack no programa shareware, este passa a funcionar normalmente, podendo o usuário utilizá-lo como se tivesse regularmente adquirido e registrado. Na Internet é possível encontrar muitos sites especializados na distribuição de cracks como, por exemplo, o “Astalavista”²², um dos mais famosos sites do ramo.

4.2 SPAM

Spam nada mais é que o envio não solicitado e não autorizado de mensagens pelo correio eletrônico, visando à divulgação de propagandas de produtos ou de serviços, assim como de quaisquer informações, com ou sem natureza comercial, de interesse da pessoa divulgadora, assemelhando-se a uma mala-direta eletrônica, via Internet.

Tal prática ilícita, segundo a Associação Brasileira dos Provedores de Acesso, Serviços e Informações da Rede Internet, onera os recursos da rede, pelo excessivo trânsito de e-mails gerados, causando um prejuízo mensal da ordem de R\$ 90.000.000,00.

Diante da gravidade de tal ato, as normas vigentes, de forma muito limitada, acabam por proteger o indivíduo do recebimento de spams. O artigo 5º, X e XII, da Constituição Federal, que trata dos direitos fundamentais e das garantias individuais, estabelece que a intimidade, a vida privada e o sigilo de dados são invioláveis. Assim, tanto aquele que, conhecendo os dados do consumidor, forneceu os mesmos para o remetente do e-mail, como os próprios fornecedores do produto ou serviço anunciado no e-mail são considerados infratores das normas constitucionais citadas.

Por sua vez, o artigo 65 da Lei das Contravenções Penais estabelece pena de prisão simples, de 15 (quinze) dias a 2 (dois) meses, ou multa para a conduta de molestar alguém ou perturbar-lhe a tranqüilidade, por acinte ou por motivo reprovável.

O bem jurídico tutelado pelo tipo é a tranqüilidade, direito inerente a qualquer pessoa, sendo que ao ser ameaçada, pode-se invocar a proteção do Estado. A conduta típica de tal fato constitui em o agente praticar intencionalmente um ato visivelmente perturbador ou molestandor da paz de espírito ou do sossego da vítima, promovendo-lhe injustos dissabores ou atribuições injustas ou lhe induzindo a so-

²¹ Softwares de teste com utilização limitada.

²² www.astalavista.com, acesso em 10/2001.

bressaltos e preocupações. A ameaça à tranqüilidade se caracteriza quando o ato praticado causa aborrecimentos, ira ou execução de trabalho desnecessário, inoportuno ou indevido. O tipo também exige que o sujeito ativo aja com acinte ou por motivo reprovável, ou seja, que faça algo de propósito, intencionalmente, deliberadamente, não sendo necessário que o ato seja grosseiro e sim, reprovável.²³ O spam, viola a tranqüilidade e causa perturbações na rotina pessoal do sujeito passivo por ocupar espaço e tempo quando se necessita fazer uso do e-mail para fins profissionais e pessoais, por causar extrema lentidão e congestionamento nos sistemas e redes de informática e ainda por obrigar o usuário a ficar alerta para que não seja infectado com algum vírus que tenha se atrelado às mensagens indesejadas.

Dentre os projetos de Lei que abordam o tema, destaca-se o de número 6.210 de 2002, que estabelece limites ao envio de mensagens não solicitadas e critérios para que o destinatário possa identificar a sua origem e bloquear o seu recebimento, além de fixar multa de até oitocentos reais por mensagem enviada.

5. DA RESPONSABILIDADE DOS PROVEDORES

Provedor é o nome dado às empresas que oferecem o serviço de acesso à Internet para usuários residenciais ou empresas.

Atualmente, grande é a discussão a respeito da responsabilidade dos provedores por atos cometidos pelos seus usuários. Porém o concurso de pessoas no artigo 29 do Código Penal não é cabível neste caso, pois os provedores não desejam o resultado nem mesmo sabem de sua existência.

Conforme sustenta Carla Rodrigues Araújo de Castro²⁴, *“o usuário utiliza o provedor como um meio de acesso à Internet, como um instrumento para a prática do crime. Além do que, a quantidade de informações veiculadas através do provedor dificulta a fiscalização”*. Além disso, não existe legislação específica exigindo que o provedor fiscalize os atos de seus usuários.

Porém, os provedores que fornecem serviço de hospedagem de páginas, terão eventual responsabilidade por omissão, no caso de anunciarem previamente a possibilidade de se retirar sites com conteúdo criminoso, chamando para si tal responsabilidade,²⁵ ou se o provedor tenha sido notificado a respeito do conteúdo ilícito de sites nele hospedados e não tome providências no sentido de tirá-lo do ar.

6. CONCLUSÃO

Por mais eficientes e entusiasmantes que possam ser os sistemas de segurança criados pelos técnicos em informática, estes sempre serão superados pelos criminosos. É exatamente neste ponto que o direito deverá ser cada vez mais

²³ Amaro Moraes e Silva Neto, Mensagens inúteis, Revista Consultor Jurídico, www.uol.com.br/consultor, acesso em 17/12/2001.

²⁴ Carla Rodrigues Araújo de Castro, ob. cit., p. 70.

²⁵ Código Penal, art. 13 § 2º.

atuante, punindo os responsáveis e oferecendo a devida segurança para a sociedade.

Porém grandes e prematuras discussões cercam o tema. É certo e incontroverso que os crimes cometidos na Internet ou os crimes de informática em geral necessitam de legislação específica, estabelecendo-se princípios para que seja possível uma punição justa e proporcional aos danos. A legislação e a atuação do direito no campo da Internet só será eficaz através da união e parceria dos operadores do direito em geral e de especialistas em informática. Através dos mecanismos legais existentes e dos que estão por vir, deve surgir uma eficaz resistência às condutas criminosas, minimizando, assim, o descaso com que parte da sociedade prefere tratar a informática, presente de maneira irreversível em nosso meio.

BIBLIOGRAFIA

ARRUDA JÚNIOR, Itamar, *Injúria e Difamação em Meio Virtual*. {on line} <http://www.cbeji.com.br>, 04/2002.

BRASIL, Angela Bittencourt, *A Questão Napster*. {on line} <http://www.uol.com.br/consultor>, 27/07/2000.

CASTRO, Carla Rodrigues Araújo de, *Crimes de Informática e Seus Aspectos Processuais*. Rio de Janeiro: Editora Lumen Júris, 2001.

CEBEJI – Centro Brasileiro de Estudos Jurídicos da Internet. {on line} <http://www.cbeji.com.br/legislacao>, 03/2002.

CORRÊA, Gustavo Testa, *Aspectos Jurídicos da Internet*, São Paulo: Saraiva, 2000.

DANTAS, Alberto da Silva, *Obras Protegidas*. {on line} <http://www.uol.com.br/consultor> 23/12/2001.

FERREIRA, Aurélio Buarque de Holanda, *Novo Dicionário Aurélio da Língua Portuguesa*, Rio de Janeiro: Nova Fronteira, 1986.

GOUVÊA, Sandra, *O direito na Era Digital*. Rio de Janeiro: Mauad, 1997.

GUEIROS JÚNIOR, Nehemias, *O Som Ameaçador da Grande Rede*. {on line} <http://www.uol.com.br/consultor>, 22/05/2000.

HUNGRIA, Néelson, *Comentários ao Código Penal*. Rio de Janeiro: Forense, 1958, Volume VII.

MAUDONNET, Maria Clara, *Invasão De Privacidade - Spammers Podem Ser Acionados Por Perdas e Danos*. {on line} [http:// www.uol.com.br/consultor](http://www.uol.com.br/consultor), 23/04/2002.

MIRABETE, Julio Fabbrini, *Código Penal Interpretado*. São Paulo: Atlas, 2001.

NOGUEIRA, Sandro D Amato, *Polícia tem dificuldades para chegar aos pedófilos*. {on line} [http:// www.direitonaweb.com.br](http://www.direitonaweb.com.br), 28/03/2002.

NORONHA, Edgard Magalhães, *Direito Penal*. São Paulo: Saraiva, 1998, Volume I.

REVISTA CONSULTOR JURÍDICO. {on line} <http://www.uol.com.br/consultor>, 06/2002.

REVISTA INFO ONLINE. {on line} <http://www2.uol.com.br/info/aberto/infofaq>, 05/2002.

RIBEIRO Wal, *Quem Cai na Rede é Peixe*. {on line} www.kids-denuncia.org.br, 04/2002.

SILVA NETO, Amaro Moraes e, *Mensagens linúteis*. {on line} <http://www.uol.com.br/consultor>, 17/12/2001.

STUBER, Bentivegna e Armani, *Lei do Software - Proteção Legal dos Programas de Computador*. {on line} [http:// www.uol.com.br/consultor](http://www.uol.com.br/consultor), 14/04/99.

VALLIM, Celso Henrique de Castro Baptista, *Crimes Contra a Honra na Internet*. Florianópolis: 06/2000, monografia. Universidade Federal de Santa Catarina.

VIANNA, Túlio Lima, *Dos Crimes Por Computador*. Belo Horizonte: 2000, monografia, Faculdade de Direito da UFMG