

O DIREITO FRENTE À ERA DA INFORMÁTICA

Rafaella REDIVO¹
Gabriela Loosli MONTEIRO²

RESUMO: Os avanços da tecnologia e o surgimento da Internet propiciaram o aparecimento de novos tipos penais, como também novas formas de praticar crimes já conhecidos, nasceu assim o crime de informática. Visa, portanto, este estudo, analisar à problemática acerca do ajustamento da norma penal em face dos crimes virtuais e sua repercussão em âmbito jurídico.

Palavras-chave: Computador. Internet. Crimes de Informática. Pedofilia. Impunidade

1 INTRODUÇÃO - EVOLUÇÃO HISTÓRICA

O primeiro computador eletrônico data de 1946 e foi criado pelas necessidades militares. Denominou-se ENIAC (*Electronic Integrator and Calculator*). Em 1951 apareceram os primeiros computadores em série.

A Internet surgiu em 1969 como uma experiência do governo dos Estados Unidos. A ARPA (*Advanced Research Projects Agency*), pesquisou uma forma segura e flexível de interconectar os computadores, permitindo que os pesquisadores acessassem centros de computação para compartilhar recursos de hardware e software. Algumas redes que utilizavam ondas de rádio e satélite foram conectadas a ARPANET através de uma tecnologia de interconexão. No início da década de 1980, a ARPANET foi dividida em duas redes: ARPANET e Milnet (rede militar). Essa interconexão de rede foi denominada DARPA e internet. Em 1986 foram interligados os supercomputadores do centro de pesquisa da entidade NSF – *National Science Foundation* com os da ARPANET.

¹ Discente do Curso de Direito das Faculdades Integradas “Antônio Eufrásio de Toledo” de Presidente Prudente. E-mail: rafa_redivo@hotmail.com

² Discente do Curso de Direito das Faculdades Integradas “Antônio Eufrásio de Toledo” de Presidente Prudente.

Os conjuntos de todos os computadores e redes ligados a esses dois supercomputadores formaram um *backbone* (espinha dorsal de rede) e, a partir daí essa estrutura foi denominada Internet.

A Internet é uma grande rede de comunicação mundial, pode ser conectada por linhas telefônicas, satélites, ligações por microondas ou por fibra ótica. Ela possui três serviços básicos: correio eletrônico, conexão remota por *login* e transferência de arquivos.

A internet teve sua origem embrionária em plena guerra fria como arma militar norte-americana de informação. A idéia consistia em interligar todos as centrais de computadores dos postos de comando estratégicos americanos, precavendo-se, pois, de uma suposta agressão russa. Sendo atacado um desses pontos estratégicos, os demais poderiam continuar funcionando autonomamente, auxiliando e fornecendo informações a outros centros bélicos.

Com o advento da WWW (ou *Web*), a Internet se transformou num instrumento de comunicação de massa.

A Internet chegou ao Brasil em 1988 por iniciativa das comunidades acadêmicas de São Paulo e do Rio de Janeiro, tendo sido criado em 1989, a Rede Nacional de Pesquisa, pelo Ministério de Ciência e Tecnologia, com a finalidade de disponibilizar os serviços de acesso a Internet. A exploração comercial da rede foi iniciado em dezembro de 1984.

Diante da propagação do microcomputador como um dos mais cobiçados e comuns objetos de consumo da era moderna, não é de se espantar que onde haja o uso, haja também o abuso.

O avanço da tecnologia na área da informática provocou uma grande revolução nas relações sociais. As facilidades alcançadas pelo uso do computador e, principalmente, a Internet, transformaram a vida moderna. É a era da Informática.

Tantas inovações na área tecnológica propiciaram o aparecimento de novos tipos de crime ou novas formas de praticar os já conhecidos tipos penais.

Dentre os delitos perpetrados pelos conhecidos como *hackers*, podemos citar as fraudes bancárias, o estelionato, violação de direito autoral, crimes

contra a honra, bem como divulgar material pornográfico ou de caráter discriminatório, entre outros.

2 CONCEITOS DE CRIME DE INFORMÁTICA

O conceito de crime de informática não é uniforme. Para Rodrigues Araújo de Castro (2003, p. 09):

Crime de informática é aquele praticado contra o sistema de informática ou através deste, compreendendo os crimes praticados contra o computador e seus acessórios e os perpetrados através de computador. Inclui-se nesse conceito os delitos praticados através da Internet, pois pressuposto para acessar a rede é a utilização de um computador.

Na visão de Senise Ferreira (1992, p. 141 e 142), “crime de informática é toda ação típica, anti-jurídica e culpável contra ou pela utilização de processamento automático e/ou eletrônico de dados ou sua transmissão”.

Para Bittencourt Brasil (2000, p.133 e 134), não há diferença entre crime comum e crime de informática; salienta, todavia que a fronteira que os separa é a utilização do computador para alcançar e manipular o seu sistema em proveito próprio ou para lesionar outrem.

3 CLASSIFICAÇÃO DOS CRIMES DE INFORMÁTICA

Os crimes de informática podem ser próprios ou impróprios. Os primeiros são aqueles que só podem ser praticados através da informática, sem ela é impossível a execução e consumação da infração. São tipos novos, que agridem a informática como bem juridicamente protegido. Daí porque, em face da escassa legislação existente, alguns fatos são atípicos e, portanto não podem ser punidos.

Exemplo violação do e-mail, pirataria de software, pichação de *homepages*, dano em arquivos provocado pelo envio de vírus e etc.

Os crimes de informática impróprios são os que podem ser praticados de qualquer forma, inclusive através da informática. Assim, o agente para cometer o delito, utiliza, eventualmente o sistema informático. O computador é um meio, um instrumento para a execução do crime. São delitos que violam bens já protegidos por nossa legislação, como patrimônio, honra. Exemplo ameaça, estelionato, calunia, pedofilia. Portanto utiliza-se a legislação vigente.

4 SUJEITOS DO CRIME DE INFORMÁTICA

A princípio qualquer pessoa pode ser sujeito ativo nos crimes de informática, ou seja, é um crime comum quanto ao agente. Muito embora verificamos que a grande maioria dos delitos são cometidos por funcionários ou ex-funcionários, contra suas empresas. Essas pessoas em razão da relação profissional, têm facilidades para a empreitada criminosa.

Em relação ao sujeito passivo, também pode ser qualquer pessoa. Porém, como vimos acima são as empresas as principais lesadas neste tipo de crime. E aqui, surge um dos maiores empecilhos para conhecimento e apuração dos crimes. Na maioria das vezes a empresa lesada prefere arcar com os prejuízos causados pela infração, do que tornar público o fato de ter sido vítima desse tipo de delito. A publicidade da vulnerabilidade do sistema de informática da empresa pode causar prejuízos maiores do que os efetivamente sofridos.

5 LUGAR DO CRIME

O grande problema, ao se trabalhar com o conceito de jurisdição e territorialidade na Internet, reside no caráter internacional da rede. Na Internet não existe fronteiras e, portanto, algo que nela esteja publicado estará em todo mundo.

A lei brasileira adota, entre os diversos princípios que determinam a aplicação da lei penal no espaço, como regra, o da territorialidade, segundo o qual são aplicados aos crimes as leis do país em que eles forem praticados, é o que determina o Art. 5º do nosso Código Penal.

Para determinar o lugar do crime e saber, portanto, se ele foi cometido em território nacional o Brasil adotou a teoria da ubiqüidade, que, nas palavras de Damásio Evangelista de Jesus (1995, p.112), “adota como local do crime aquele em que se realizou qualquer dos momentos do *iter*, seja da prática dos atos executórios, seja da consumação”.

Teoricamente, a maioria dos crimes praticados na Internet produz seus efeitos em todo lugar que ela puder atingir.

Como não há uma regulamentação acerca dessa matéria, pode-se fazer com que um delito possa ser julgado em todo e qualquer parte do mundo.

A melhor hipótese é a de que seja considerado como local do crime aquele em que está o autor das infrações. Este seria o país com melhores condições de aplicar uma eventual pena, bem como se evitaria a necessidade de extradição para o país em que ele fosse condenado.

6 DIREITOS FUNDAMENTAIS VIOLADOS

Por direito fundamental, segundo a doutrina e a jurisprudência é o mínimo de direito que se concede a alguém para que possa viver com dignidade. Quando se fala em direito fundamental é no sentido de que o Estado proteja e garanta aquele direito fundamental, barrando nele próprio ou que um particular viole tais direitos.

Esses direitos existem, mas nos crimes de informática eles são violados, há um abuso desses direitos. Como por exemplo, o direito de inviolabilidade das comunicações, é um direito tão fundamental que a nossa Constituição o prevê no artigo 5º, inciso XI, dizendo que:

XI - é inviolável o sigilo de 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",

Ora, se o legislador penaliza a conduta de quem viola "correspondência", obviamente penaliza a conduta de quem viola "correspondência eletrônica", que é o "*e-mail*".

Um outro exemplo da violação dos direitos fundamentais, ocorre quando, um agente tem a intenção de "invadir" o sistema operacional de um Banco ou outra Instituição Financeira para desviar valores, mesmo sem subtrair fisicamente uma coisa móvel para si, houve no caso, como resultado final, uma alteração ilícita do domínio daqueles valores em favor dele próprio, o que constitui uma violação atentatória contra a propriedade do domínio. Portanto, como via de consequência, o objeto a ser tutelado é o direito à propriedade.

Em relação ao direito a vida, é o mais fundamental de todos os direitos, já que se constitui um pré-requisito a existência e exercício de todos os demais direitos.

Já o direito a intimidade e a própria imagem formam a proteção constitucional à vida privada, salvaguardando um espaço íntimo intransponível por intromissões ilícitas externas. A proteção constitucional consagrada no inciso X do art. 5º refere-se tanto a pessoas físicas como a pessoas jurídicas, abrangendo, inclusive, a necessária proteção à própria imagem frente aos meios de comunicação em massa, como por exemplo, a Internet.

7 PEDOFILIA

Dentre todos os crimes praticados na Internet, a pedofilia é o que provoca maior repúdio e revolta na sociedade. É inaceitável o constrangimento ao qual as crianças e adolescentes são submetidos para saciar o prazer doentio e repugnante de pessoas desequilibradas. A pedofilia tira da criança o que ela tem de mais valioso, sua inocência, sua infância.

A pedofilia consiste num distúrbio de conduta sexual no qual o indivíduo adulto sente desejo compulsivo por crianças ou pré-adolescentes, podendo ter carácter homossexual ou heterossexual.

A Lei 8.069/90 (Estatuto da Criança e do Adolescente) possui vários tipos penais, dentre eles encontramos o referente a pedofilia: “Art. 241. Fotografar ou publicar cena de sexo explícito ou pornográfica envolvendo criança ou adolescente: Pena – reclusão de um a quatro anos”.

Publicar é tornar público, acessível a qualquer pessoa, divulgar. Não importa o número de “internautas” que acessem a página, ainda que ninguém conheça seu conteúdo, as imagens estarão à disposição de todos configurando a infração, significa não se exigir que, em face da publicação haja dano real a imagem.

Trata-se de tipo de conteúdo alternativo, sendo suficiente a prática de uma das condutas (fotografar ou publicar) para a consumação.

O bem jurídico protegido pelo ECA é a criança e o adolescente.

É classificado como crime de informática impróprio.

A consumação se dá com a disponibilidade das fotos ao público, ou seja, com a inserção das fotos na rede.

Existem obstáculos para a punição desse crime. Duas situações podem dificultar a incriminação de quem publica as fotos na rede. Na primeira, o agente conhece a adolescente, trata-se de pessoa identificada e, quando é ouvida, esclarece que afirmou ser maior de idade, portanto ausente o conhecimento pelo agente da sua real idade, não há dolo, elemento subjetivo do tipo.

Outro problema para apuração do delito é o desconhecimento da identidade da vítima, o agente recebeu ou capturou as fotos na rede e as divulga.

Em relação à autoria do delito na pedofilia, como nos outros crimes praticados através da Internet, não é difícil identificar a máquina, posto que todo computador possui um número denominado IP, o problema é saber quem utilizou o computador para divulgar as fotos de criança e adolescente.

8 IMPUNIDADE

Nosso legislador não é tão rápido e eficiente como os cientistas que se dedicam no avanço da tecnologia. Enquanto os funcionários da Microsoft, IBM e outras empresas se empenham em descobrir novos equipamentos que facilitem a vida do usuário, nosso Congresso não consegue discutir e aprovar as leis com a necessária celeridade.

Em se tratando dos tipos novos surge um problema. Considerando que nosso Código Penal data de 1940, por razões óbvias não prevê tipos penais relacionados à informática. O ideal seria aplicar as normas existentes, adequando-as aos fatos que forem acontecendo. Mas não é tão simples assim. O princípio da reserva legal, elevado pelo legislador constituinte à garantia fundamental, exige que lei tipifique um fato como criminoso. Sem lei, não há crime. Este é o maior obstáculo para a apuração e repressão dos atos praticados através da Internet. Por outro lado constitui uma garantia do cidadão, não ser punido senão após uma lei que defina a conduta como criminosa e ao mesmo tempo imponha uma sanção penal.

Devido à especialidade destas figuras, as quais atingem bens jurídicos novos, como: dados, informações, *sites*, *home pages*, *e-mails*, etc; bem como a ausência de lei, muitos fatos não podem ser reprimidos pelo Estado. Não há que se cogitar em interpretação extensiva ou analogia, ambas vedadas no Direito Penal se tem por fim prejudicar o réu.

A atipicidade impede, deste modo, a punição do agente, não obstante tenha ele praticado atos lesivos ou até mesmo imorais. É claro que eventuais danos poderão ser discutidos no cível, mas no campo penal nada poderá ser feito.

Assevera Norberto Bobbio no entendimento que:

É impossível que o Poder Legislativo formule todas as normas necessárias para regular a vida social; limita-se então a formular normas genéricas, que contêm somente diretrizes, e confia aos órgãos executivos, que são muito mais numerosos, o encargo de torná-las exequíveis (1995).

9 CONCLUSÃO

Muitos países já possuem leis sobre esta matéria. Em Portugal lei de 1991 dispõe sobre a criminalidade na informática, já na Itália houve uma alteração do Código Penal acrescentando quinze preceitos sobre este tema. Estados Unidos, Inglaterra e Alemanha também possuem leis específicas. No Brasil temos apenas a Lei 9.609/98 que protege o direito autoral de programa de computador. Muitos projetos de lei foram apresentados, alguns estão em tramitação, outros foram engavetados.

A carência existe e aguardamos com ansiedade ver disciplinados novos tipos penais, bem como as outras áreas do Direito que sofreram impacto com a evolução digital.

REFERÊNCIAS BIBLIOGRÁFICAS

ARAÚJO DE CASTRO, Carla Rodrigues – **Crimes de Informática e seus Aspectos Processuais**, 2ª edição;

_____. **Impunidade na Internet**. In: Jus Navegandi. Disponível em <<http://www.jusnavegandi.com.br>>. Acesso em 08/ago/2007.

BOBBIO, Norberto. - **O Positivismo Jurídico**, Lições de Filosofia do Direito. Tradução de Márcio Pugliesi, Edson Bini e Carlos E. Rodrigues. São Paulo: Ed. Ícone, 1995.

BRASIL, Ângela Bittencourt. **Informática Jurídica – o ciber direito**. Rio de Janeiro. 2000.

FERREIRA, Ivette Senise. **Os Crimes da Informática**. São Paulo : RT, 1992.

MORAES, Alexandre. **Direitos fundamentais**. 1ª ed., São Paulo, 1998.

OLIVEIRA JÚNIOR, João B. C. **A Internet e os novos crimes virtuais**. A fronteira cibernética. In: Jus Navegandi. Disponível em <<http://www.jusnavegandi.com.br> >. Acesso em 08/ago/2007.

RAMALHO TERCEIRO, Cecílio da Fonseca Vieira. **O problema na tipificação penal dos crimes virtuais**. In: Jus Navegandi. Disponível em <<http://www.jusnavegandi.com.br> >. Acesso em 08/ago/2007.

ROVER, Aires José. **Direito, Sociedade e Informática: limites e perspectivas da vida digital**, Florianópolis: Fundação Boiteux, 2000.