DOS DELITOS PRATICADOS NO ÂMBITO DA INTERNET EM FACE DA LEGISLAÇÃO PENAL BRASILEIRA

Reginaldo César Pinheiro*

RESUMO:
O presente estudo se propõe a investigar os principais aspectos jurídicos dos crimes praticados por meio da Internet e conseqüentemente a apuração da responsabilidade proporcionada pela conduta delituosa dos usuários. A inexistência de leis específicas que tipifiquem os crimes na Internet e a impossibilidade, em muitos casos, de adequar as condutas às leis existentes no ordenamento jurídico pátrio, constitui um óbice inegável ao intérprete e aos aplicadores do Direito. A metodologia empregada na elaboração do presente trabalho será o método dedutivo, partindo-se de princípios considerados verdadeiros e indiscutíveis para chegar-se a conclusões de maneira puramente formal, com o auxílio da investigação bibliográfica. Com isso, pretende-se contribuir para difusão dos conhecimentos do Direito Penal de Informática, notadamente, os *cybercrimes*, apontando os melhores mecanismos para a sua repressão e a respectiva tutela do bem jurídico do cidadão no âmbito da Rede Mundial de Computadores, com observância no ordenamento jurídico brasileiro.

PALAVRAS-CHAVE:
Internet – Delito – Responsabilidade Penal – Propostas Legislativas – Prevenção.

1. Introdução

Com o aperfeiçoamento das tecnologias digitais, a informática passou a fazer parte do cotidiano do homem moderno. Com isso, as mais variadas atividades passaram a ser realizadas também eletronicamente. Concomitantemente a esse processo, as redes de comunicação também se difundiram expressivamente, sobretudo, a Internet, que agrega hoje, quantia superior a 250 milhões de usuários em todo o mundo, conforme dados aferidos em dezembro de 1999 pela *Computer Industry Almanac*.

* Discente do 5. º ano do Curso de Ciências Jurídicas da Universidade Paranaense – UNIPAR, em Umuarama/PR e bolsista do Instituto de Pesquisa, Estudos e Ambiência Científica (IPEAC) na área de Direito de Informática e Internet, sob orientação da Prof.ª Dr.ª Tereza Rodrigues Vieira. Email: <pinheiro@unipar.br>.

Por outro lado, esse desenvolvimento vem proporcionando diversos problemas ligados ao uso da Rede Mundial de Computadores. A possibilidade da interconexão global fez com que a Internet assumisse uma característica própria entre os povos: a inexistência de uma sede geográfica definida. Logo, a possibilidade do anonimato e a eventual inaplicabilidade da lei estrangeira em território pátrio,[1] fizeram com que se constituísse uma *pseudo*liberdade na Internet.

Conseqüentemente, por não existir limites materiais, políticos e jurídicos claros, alguns usuários (mal intencionados ou não), acabam por conduzir-se de maneira criminosa no ambiente virtual. Essas condutas, embora em alguns casos sejam atípicas, criaram para o *Direito Informático*[2] novas modalidades delituosas, que se convencionou chamar de "Crimes Virtuais".

Sendo assim, o presente estudo buscou, de forma singela, apontar os principais meios para a solução dos conflitos gerados pelos *cybercrimes*, abordando os aspectos jurídicos dos delitos praticados pela Internet à luz do ordenamento jurídico brasileiro.

2. Os crimes virtuais e as suas espécies

Os crimes virtuais já começam a ser objeto de preocupação e de debates pela comunidade jurídica, embora ainda não sejam pacíficas as suas interpretações. Até mesmo na definição de crime virtual não existe unanimidade. A que melhor expressa o conceito de crime virtual, é a do Secretário Executivo da Associação de Direito e Informática do Chile, que o define como sendo:

> [...] todas aquelas ações ou omissões típicas, antijurídicas e dolosas, tratando-se de fatos isolados ou de uma série deles, cometidos contra pessoas naturais ou jurídicas, realizadas no uso de um sistema de tratamento da informação e destinadas a produzir um prejuízo à vítima, através de atentados ao bom uso da

[1] *Vide* art. 17 da Lei de Introdução ao Código Civil – L.I.C.C.

[2] Define-se Direito Informático como o "conjunto de normas, princípios e instruções que regulam as relações emergentes da atividade informática". ALTMARK, Daniel R. *Informática y derecho*. Buenos Aires: Depalma, 1987, *apud* REIS, Maria Helena Junqueira. *Computer crimes*. Belo Horizonte: Del Rey 1996, p. 14.

> técnica-informática, o qual geralmente produzirão de maneira colaterais lesões em diversos valores jurídicos, reportando-se muitas vezes, em um benefício ilícito no agente, seja de caráter patrimonial ou não, atuando com ou sem ânimo de lucro (MANZUR, 2000).

Em outras palavras, são todos os atos ilícitos (positivos ou negativos) realizados totalmente ou parcialmente por meio da Internet, que tenham por objetivo causar algum dano à vítima, patrimonial ou não (PINHEIRO, 2001, p. 18).

Diante das inúmeras espécies de delitos, a doutrina divide os cybercrimes sob as mais diversificadas concepções. Entre os autores brasileiros, a classificação que predomina é aquela que os divide em três espécies: puros, mistos e comuns.

2.1. Os crimes virtuais puros

Os *crimes virtuais puros* são aqueles em que o objeto jurídico ofendido é um sistema de informática (*hardware* ou *software*). Para o advogado Marco Aurélio Rodrigues da Costa, crime virtual puro é:

> Toda e qualquer conduta ilícita que tenha por objetivo exclusivo o sistema de computador, seja pelo atentado físico ou técnico do equipamento e seus componentes, inclusive dados e sistemas (http://www.jus.com.br).

Neste sentido, destacam-se as condutas dos hackers e dos crackers. Enquanto que os primeiros "são programadores tecnicamente sofisticados, que dedicam boa parte de seu tempo a conhecer, dominar e modificar programas e equipamentos" (SAWAYA, 1999, p. 208), os últimos, são aqueles que:

> Usam o computador, maliciosamente como hobby e obtém acesso não autorizado a sistemas de computador como objetivo de derrotá-los. Podem roubar informações sobre contas bancárias e cartões de crédito ou destruir dados (SAWAYA, 1999, p. 105).

Não se pode olvidar que essa divisão, embora seja importante para a compreensão dessa espécie de crime, não tem grande relevância

para a esfera jurídica. Independentemente de a conduta ser característica de um *hacker* ou de um *cracker*, é, *a priori*, um crime virtual puro.

Os mais difundidos certamente são os vírus digitais, originariamente criados com o escopo de dificultar a distribuição de cópias ilegais de *softwares* (PAESANI, 1998). Todavia, posteriormente, vieram a difundir-se com bastante amplitude e diversidade.

Hodiernamente, os vírus digitais surgem com características e poder de destruição muitas vezes desconhecida. As tecnologias que se tem desenvolvido para combater os vírus digitais não têm sido suficientemente eficazes. Afirma Maria Helena Junqueira Reis que a "segurança total dos computadores ainda é um mito" (REIS, p. 54). A exemplo disso, foi a notícia amplamente divulgada pela imprensa, sobre o ataque do vírus *I Love You*, que se espalhava de forma involuntária por meio do correio eletrônico dos usuários infectados (O "VÍRUS"..., 2000, p. 1-14).

Outros vandalismos praticados pelos *cybercriminosos*, na esfera dos crimes virtuais puros, são os ataques aos *sites* da Internet. Alguns feitos com o objetivo de realizar algum tipo de protesto ou também para superar seus conhecimentos. Foi o que ocorreu nos *sites* do Supremo Tribunal Federal e do Palácio do Planalto, onde vândalos substituíram as informações tradicionais, por textos contrários ao governo (PIRATAS..., 2000, p. 07).

Entretanto, constata-se que a grande maioria das invasões tem por finalidade principal, o acesso indevido a dados e informações contidas no computador, ou em sistemas informáticos. Na maioria das vezes, são auxiliados pela falta de segurança, que conforme já mencionado, é deficiente.

Ademais, ressalta-se, que em recente pesquisa realizada nos Estados Unidos pelo F.B.I. (*Federal Bureau of Investigation*), constatou que de 273 empresas de comércio eletrônico (*e-commerce*) entrevistadas, 90% já tinham sofrido algum tipo de ataque. Destas, cerca de 70% admitiram que houve grave quebra de segurança (HACKERS..., 2000).

2.2. Os crimes virtuais mistos

Os *crimes virtuais mistos* são aqueles em que o uso da Internet é condição *sine qua non* para a efetivação do delito, embora o bem jurídico visado seja diverso do ambiente informático. Pratica um crime virtual misto, por exemplo, o agente que realiza transferências ilícitas de valores, por meio de uma *home-banking*.

Há que se observar, nesta modalidade de crime, que o crescimento das compras por meios eletrônicos (e-commerce), tem contribuído para o aumento destes delitos, haja vista que o consumidor, na maioria das vezes, não conhece profundamente a Internet, e conseqüentemente, não consegue identificar se determinado site é dotado de um sistema devidamente seguro para o envio e armazenamento de dados. Por conseguinte, amplia-se a possibilidade de que os dados pessoais e bancários dos "e-consumidores" sejam indevidamente utilizados para a subtração de valores ou delitos congêneres.

2.3. Os crimes virtuais comuns

Os crimes virtuais comuns são, pois, assim entendidos, porque utilizam a Internet apenas como instrumento para a realização de um delito. A Rede Mundial de Computadores torna-se mais um meio para a realização de um crime comum, já tipificado na lei penal. Bem a propósito entende o promotor de justiça Augusto Rossini, que o crime virtual comum é um crime semelhante ao cometido por outros meios (apud FERNANDES, 1999, p. 05).

Ocorre por exemplo, nos casos de pornografia infantil, onde o crime já é tipificado pela legislação (art. 241 E.C.A.), mas que hodiernamente, vem sendo também cometido na Internet por meio dos *sites*, salas de bate-papo e fóruns de discussão (*news-group*). Do mesmo modo, destacam-se delitos como as correntes ou pirâmides, *spam*[3], que causam algum dano e a divulgação de textos que façam apologia a algum crime pela Rede.

---

[3] *Spam* é o envio indiscriminado e não solicitado de mensagens publicitárias por meio de correio eletrônico. *Vide* BIANCHI, Adriano Smid. *E-dictionary*, p. 207-208.

3. Os meios utilizados para responsabilizar o *cybercriminoso*

Com o crescente aumento da criminalidade na Internet, as autoridades coercitivas estatais começaram iniciaram diversas tentativas para reprimir e responsabilizar o criminoso virtual por suas condutas. Entretanto, mister se faz observar que as dificuldades enfrentadas para a realização desta repressão são bastante grandes, haja vista que as leis específicas que regem a matéria são quase inexistentes. Nesse sentido, assinala Antônio Scarance Fernandes que "por enquanto a repressão se restringe ao enquadramento desse tipo de infração nos delitos tipificados pelo Código Penal" (CYBERCRIMES..., 2000, p. 04).

Vale lembrar que o art. 1. º do Código Penal prescreve que: "Não há crime sem lei anterior que o defina. Não há pena sem prévia cominação legal". A analogia também não é admitida, sob pena de praticar analogia *"in malam partem"*. Logo, a conduta de um *hacker* que invade um sistema informático, por exemplo, é atípica, pois a lei penal não tipifica tal ação.

Por outro lado, alguns estudiosos têm entendido que, em muitos casos, é possível a aplicação do atual Código Penal nos crimes de informática. Embora o Código Penal seja de 1941, portanto, anterior aos *cybercrimes,* é contemporâneo em grande parte dos delitos. É necessário que os aplicadores do Direito façam um exercício de interpretação entre a Lei e os tão atuais delitos, pois como bem afirma Karl Larenz, "quem interpreta a lei em certo tempo busca nela uma resposta para as questões de seu tempo" (1989 p. 382).

Todavia, essa ferramenta hermenêutica, embora seja perfeitamente aplicável em nosso ordenamento, também apresenta dificuldades na tipificação dos crimes virtuais. Exemplo claro é o dado pelo advogado Renato Opice Blum, demonstrando que o art. 155 do Código Penal, que prescreve o crime de furto, exige a "coisa alheia móvel" para a caracterização do tipo. E completa, que "em se tratando de dados digitais na Internet, nem sempre se pode falar em coisa corpórea" (VASCONCELOS, 2000, p. 45).

De outro lado, a repressão aos crimes virtuais também encontra barreiras pertinentes aos limites geográficos da aplicação da lei. Não existe a possibilidade de se empregar a lei pátria em território estrangeiro, e, por conseguinte, os delitos praticados por meio de

servidores de outros países não poderão sofrer qualquer sanção; ressalvados os casos, é claro, em que exista uma lei tipificando a conduta naquele país, ou ainda, quando a cooperação de organismos internacionais é possível. Órgãos como o F.B. I e a Interpol têm colaborado muito na investigação dos crimes na Internet, mesmo sem existir de fato um tratado internacional, algo que alguns aplicadores do Direito julgavam ser a única forma para tal repressão.

Cabe ressaltar também, que o provedor de acesso, é também elemento decisivo para a repressão destes crimes. No ambiente virtual, ao contrário do que se pensa, o usuário não é anônimo. O provedor grava a entrada do número do IP (*Internet Protocol Number*), [4] em seu servidor. Assim, se determinado usuário se porta de forma ilícita em uma sala de bate-papo, *news-group*, *web-page* ou *e-mail*, certamente, o seu *IP* será identificado, e através do acesso ao cadastro de clientes do provedor, o *cybercriminoso* poderá ser identificado.

Ocorre que, na maioria das vezes, o provedor tem interesses econômicos na prestação de serviços de acesso à Internet (mesmo que o acesso seja gratuito), e, por conseguinte, utiliza os dados e informações que cotidianamente são obtidas, sempre com essa finalidade. Logo, as informações de entrada de usuários no provedor ou de transmissão de dados são excluídas de seus bancos de dados, em um curto espaço de tempo.

Essa conduta do provedor, todavia, deve necessariamente ser responsabilizada, uma vez que minimizará as possibilidades de que medidas judiciais eficazes sejam tomadas contra o *cybercriminoso*. A prova material de que a vítima necessita para a comprovação do crime virtual pode já não mais existir. Daí a urgente necessidade de uma legislação que obrigue o provedor de acesso a conservar tais informações, por um período superior a seis meses.

4. Da necessidade de uma legislação que tipifique os crimes virtuais

A necessidade de uma legislação específica vem sendo defendida por diversos profissionais no Brasil. Com a atual lei penal,

---

[4] *Internet Protocol Number* é uma combinação de números que possibilita identificar de forma única, uma máquina que esteja conectada à Internet.

muitas são as dificuldades que os operadores do Direito estão sujeitos, haja vista, que persistem muitas dúvidas e a lei não é de fácil interpretação.

Embora o Brasil ocupe o sétimo lugar em número de usuários no mundo,[5] na América Latina, o Brasil é um dos poucos países que ainda não possui uma lei que tipifique tais crimes. Conseqüentemente, os cybercriminosos brasileiros tornaram-se responsáveis por diversos ataques realizados em sites, no Brasil e no Mundo. Segundo noticiava o Jornal O Estado de São Paulo, dos 66 ataques realizados em grandes portais da Internet, cerca de 41 teriam sido causados por grupos brasileiros (JUSTIÇA..., 2000, p. B6).

Por corolário, não tardaram em surgir pressões internacionais sobre o governo brasileiro, no sentido de que se crie uma lei que tipifique o crime na Internet. A reunião dos Ministros da Justiça e Procuradores promovidos pela OEA (Organização dos Estados Americanos), já diagnosticava tal posicionamento, pois um dos principais temas abordados foi à criação de mecanismos para coibir a criminalidade na Internet. Assim, o governo brasileiro deseja, o mais depressa possível, criar uma lei que possa punir com maior rigor esses crimes.

Em matéria legislativa, diversos Projetos de Lei foram propostos no Congresso. Atualmente, cerca de 20 projetos de lei pertinentes aos crimes virtuais tramitam nas casas legislativas (CRESCE..., 2000, p. 28).

Destes, destacam-se dois projetos, que vêm recebendo bastante atenção por parte dos meios de comunicação. Um deles, pertencente ao Deputado Federal Luiz Piauhylino, tipifica, dentre outras coisas, o dano a dados ou programas de computador, acesso indevido ou não autorizado a redes de computadores, o desenvolvimento ou inserção de dados com fins nocivos e a vinculação de pornografia através de redes de computadores. Observa ainda, em sua justificativa, que não se pode permitir que pela falta de lei, pessoas inescrupulosas continuem usando computadores e suas redes para propósitos escusos e criminosos (PL, n. 84/1999).

---

[5] Dados verificados em Dezembro de 1999 pela *Computer Industry Almanac*. Disponível em: <http://www.c-i-a.com/199911iu.htm>.

O seu projeto, é resultado de diversos estudos realizados juntamente com especialistas na área e pela Comissão de Ciência e Tecnologia, Comunicação e Informática. Em março deste ano, a iniciativa do Deputado recebeu o apoio do então Ministro da Justiça, José Carlos Dias, que decidiu designar uma comissão para estudar o assunto. Afirmava o ministro que "a articulação entre o Legislativo e o Executivo é fundamental" (COMBATE..., 2000, p. 26).

O Senador Renan Calheiros, como conseqüência de sua atuação como Ministro da Justiça, também elaborou um projeto de lei no qual tipifica os delitos informáticos. O projeto traz basicamente o mesmo conteúdo que o do Deputado Piauhylino, especialmente no que se refere aos crimes de violação de dados e de informações em sistemas de informática. Ademais, o Senador dedica especial atenção a justificação de seu projeto, entendendo que "a tipificação desse tipo de delito pelas legislações de todos os países é medida urgente e que não pode esperar mais" (PL, n. 76/2000).

Entretanto, há que se ressalvar em ambos os projetos, que as matérias por eles tipificadas, tratam, principalmente, dos crimes virtuais mistos e comuns, ou seja, paradoxalmente entendem que as legislações precisam estar preparadas para este tipo de delito, mas, no entanto, tratam principalmente de crimes que podem ser punidos pela vigente lei penal brasileira.

Por outro lado, na esfera dos crimes virtuais puros, os referidos projetos poderão significar expressivo avanço para a legislação pátria, haja vista, que crimes como a violação de dados e informações de sistemas de informática, ainda são condutas atípicas. Embora também atípica seja a prática de *spam* que cause dano, nenhum dos projetos de que se tem conhecimento tratam da matéria.

Ressalta-se também, alguns excessos constantes no projeto do Senador Renan Calheiros, onde define em seu art. 2º. § 6. º, inciso II (dos crimes contra a moral pública e opção sexual), a *divulgação de material pornográfico.* A pornografia infantil e a pedofilia na Rede devem ser combatidas pelo legislador e não a simples "divulgação de material pornográfico", que é uma conduta admitida até mesmo no ambiente real. No entanto, entende-se que o ilustre senador quis expressar na letra da lei, o crime de divulgação de material pornográfico *ilícito*.

Deve-se levar em consideração a relevância do problema que esses delitos representam para a Internet brasileira, e assim, o legislador possa perceber os reais efeitos dos atos delituosos na Internet e se proceder de maneira a produzir uma legislação que atenda às exigências e anseios necessários ao bom uso da Rede Mundial de Computadores.

5. Conclusão

No ambiente virtual, os defeitos e os atos ilícitos dos usuários se produzem com a mesma facilidade que no ambiente real. Ao pretender tutelar o bem jurídico do cidadão, o Direito precisa, necessariamente, se modernizar paulatinamente ao desenvolvimento das sociedades, a fim de garantir o bom uso da Rede Mundial de Computadores.

Dessa forma, o que é proibido *off line,* também deve igualmente ser em ambiente *on line,* pois a Internet não pode ser instrumento de impunidade, para os que a utilizam indevidamente.

Os projetos de lei que se apresentam no Congresso Nacional, são iniciativas importantes para a repressão e o desestímulo a prática desses delitos. Porém, a criação de uma legislação específica, por si só, não garante a tutela do bem jurídico do cidadão na Internet. É preciso também que as empresas de comércio eletrônico possuam mecanismos eficazes de segurança para seus *sites*, de maneira que a transmissão e armazenamento de dados e informações dos usuários/clientes, sejam procedidos de forma segura. O desenvolvimento das assinaturas digitais e da criptografia irá, igualmente, contribuir para que a segurança na transmissão de dados e informações seja estabelecida na esfera virtual.

O Comitê Gestor, que é órgão responsável pelo desenvolvimento de serviços da Internet no Brasil, também deve atuar de forma mais rígida, exigindo dos provedores de acesso, um monitoramento mais efetivo às páginas pessoais, salas de bate-papo e similares, que por eles são hospedadas.

Com a popularização da Internet, a interconectividade tornou-se elemento imprescindível para o desenvolvimento das sociedades globais. Contudo, a possibilidade de violação de um bem jurídico por um *cybercriminoso,* não pode estabelecer um ambiente de

insegurança, nem muito menos interromper o normal progresso das relações que a Internet, em sua totalidade, propicia. A prevenção e a boa-fé, numa nova postura ética e social, certamente farão a diferença nas relações do mundo digital.

5. Referências

BIANCHI, Adriano Smid. **E-dictionary**: dicionário de termos usados na internet. São Paulo: Edicta, 2001.

BRASIL, Decreto-lei n. 4.657, de 04 de Set. de 1942. **Lei de introdução ao código civil brasileiro**. Diário Oficial da União, 09 de Setembro de 1942.

COMBATE aos 'hackers' desafia legislador. **Jornal Tribuna do Direito**, n. 84, Abril de 2000, p. 26.

COMPUTER Industry Almanac. Disponível em: <http://www.c-i-a. com/199911iu.htm>.

COSTA, Marco Aurélio Rodrigues da. Crimes de Informática. **Revista Eletrônica Jus Navigandi**. Disponivel em: <http://www.jus.com.br>. Acesso em: 07.02.2001.

CRESCE número de projetos contra crimes. **Jornal Tribuna do Direito**, n. 88, Agosto de 2000, p. 28.

DELMANTO, Celso. **Código penal comentado**. São Paulo: Ed. Freitas Bastos, 1986.

FERNANDES, Antônio Scarance. **Crimes praticados pelo computador**: dificuldade na apuração dos fatos. Palestra apresentada na XVII Conferência Nacional da OAB. Rio de Janeiro, Setembro de 1999. [Gentileza do autor].

_____. Cybercrimes: legislar ou auto-regulamentar? **Revista RT Informa**, ano II, n. 06, edição de Março/Abril de 2000.

HACKERS deixam rastro de prejuízos. **Jornal da Tarde**. Edição de 30.03.2000. Disponível em: <http://www.jt.com.br/>.

JESUS, Damásio Evangelista de. **Direito penal**: parte geral. 21. ed., vol. I. São Paulo: Saraiva, 1998.

JUSTIÇA vai criar comissão para punir 'hackers'. **Jornal O Estado de São Paulo**, edição de 02.03.2000, p. B6.

LARENZ, Karl. **Metodologia da ciência do direito**. 2. ed., Lisboa: Fundação Calouste Gulbenkian, 1989.

LOPES, Mauricio Antonio Ribeiro Lopes (coord.). **Código penal**. 6. ed. São Paulo: Revista dos Tribunais, 2001.

MANZUR, Claudio Líbano. Chile: los delitos de hacking en sus diversas manifestaciones. **Revista Electrónica de Derecho Informático**, n. 21, Abril del 2000. Disponível em: <http://publicaciones.derecho.org/redi>. Acesso em: 15.05.2000.

O "VÍRUS" DO AMOR. **Jornal Folha de São Paulo**, edição de 06.05.2000, p. 1-14.

PAESANI, Liliana Minardi. **Direito de Informática**: comercialização e desenvolvimento internacional do software. São Paulo: Ed. Atlas, 1998.

PINHEIRO, Reginaldo César. Os crimes virtuais na esfera jurídica brasileira. **Boletim do Instituto Brasileiro de Ciências Criminais**. Ano 8 n. 101, pp. 18-19, Abril de 2001.

PIRATAS invadem os sites do STF e da presidência da república. **Jornal Folha do Paraná**, edição de 19.06.2000, p. 07.

REIS, Maria Helena Junqueira. **Computer crimes**: a criminalidade na era dos computadores. Belo Horizonte: Ed. Del Rey, 1996.

SAWAYA, Márcia Regina. **Dicionário de informática e Internet**. São Paulo: Ed. Nobel, 1999.

VASCONCELOS, Nelson. Na mira da lei. **Revista Internet.br**, n. 48, p. 45-46, edição de Maio de 2000.

ZARICH, Faustina. (org.). **Derecho informático**. Buenos Aires: Editorial Juris, 2000.

ABSTRACT:

The present study proposes oneself to investigate the principles juridical aspects of the crimes practiced for the middle of Internet and consequently the verification of responsibility proportioned for the conduct criminal of the users. The inexistence of specifies laws that typify the crimes on the Internet and the impossibility in many cases, to adapt the conducts to laws existents in the ordainment juridical paternal, consist of an undeniable impediment to the interpreted and to the applicator of law. The methodology used in the elaboration of present study will be the deductive method, be initiating in the principles considered true and unquestionable to reach a conclusion of way absolutely formal with the support of bibliographic investigation. With this, pass oneself to contribute to diffusion of knowledge of Penal Law of Informatics, notedly, the cyber crimes, indicating the best mechanics to their repression and the tutelage respective of juridical well of citizen in the ambit of Internet, with observance in ordainment brazilian juridical.

KEYWORDS:

Internet – Delict – Penal Responsibility – Legislatives Proposals – Prevention.

Artigo recebido para publicação em: 27/05/2002
Artigo aceito para publicação em: 21/06/2002