

RESUMO

Pesquisa exploratória que busca apresentar a legislação acerca da tipificação dos crimes de informática no contexto brasileiro. Enfocando que o Direito deve evoluir juntamente com as inovações tecnológicas, para que estas não permitam o julgamento do espaço virtual como um ambiente sem leis. Apresenta, ainda, as dificuldades nas demandas da Polícia Judiciária na investigação dos cibercrimes, considerando que parte das aplicações são baseadas em dispositivos não específicos e em alguns casos não possíveis de serem tipificadas por analogia às Leis vigentes no país. Também demonstra que na atual legislação existem lacunas acerca do tema. Assim como, busca ainda saber, como são tratados os crimes digitais na esfera penal, quais os principais delitos registrados, o perfil dos criminosos, como são tipificados estes crimes a partir das adequações a atual legislação e por fim quais os procedimentos que podem ser adotados por estas vítimas quando acometidas por tais crimes.

Palavras-chave: Crimes digitais, Crimes virtuais, cibercrimes, perfil vitimológico, tipificação de crimes.

DIGITAL CRIMES SITUATION OVERVIEW

ABSTRACT

Exploratory research that seeks to introduce legislation on the classification of computer crimes in the Brazilian context. Focusing on the Law must evolve along with technological innovations, so they do not allow the trial of the virtual space as a lawless environment. It also presents difficulties in the demands of the Judicial Police in the investigation of cybercrime, considering that some of the applications are based in non-specific and in some cases not possible to be typified by analogy to the laws of the country. It also shows that there are gaps in current legislation on the subject. Like, also seeks to know, are treated in criminal computer

¹ Discente do curso de Direito da FARN. E-mail: deborahmaia@gmail.com

crime, which are the major crimes reported, the profile of criminals, as these crimes are typified adjustments from the current law and order which procedures can be adopted when affected by these victims of such crimes.

Keywords: Digital crimes, Virtual crimes, Computer crime, cybercrime, victimology profile, crimes' classification.

INTRODUÇÃO

O Direito, ao longo dos séculos, sofreu modificações úteis e relevantes. Devido a essas transformações o Direito perdurou. Contudo, nem sempre essas transformações se deram de forma linear, ou seja, por vezes se deram com certo atraso, ou ainda, nem sempre o direito evoluiu na mesma velocidade que as transformações se deram. Atualmente “o tempo” tem sido denominado de “a era da tecnologia”, com inovações tecnológicas sendo desenvolvidas a cada dia-a-dia, sendo a mais robusta delas é a Internet, e com ela novos desafios aparecem, exigindo, assim, respostas do operador do Direito.

A Internet, como toda nova tecnologia, não trouxe só vantagens; igualmente trouxe desvantagens: espionagens industriais e comerciais, estelionatos, pornografia, plágio, venda de bens impossíveis ou inexistentes, transferências ilegais de contas bancárias, pedofilia, fraudes em leilões virtuais, falsificação.

Portanto, uma nova realidade se apresenta ao Direito, e este deve se adaptar a ela, a sociedade está migrando para o ciberespaço, e o Direito deve seguir esta migração. Como se diz em latim “*Ubi societas, ibi jus*”. Portanto se a sociedade está no ciberespaço, então o Direito deve estar lá também. No panorama da sociedade virtual existem os crimes digitais e no contexto atual são considerados alguns pressupostos constitucionais para tipifica-los: os incisos II, X, XII, XXV, XXXIX do art. 5º da Constituição Federal Brasileira. Estes incisos denotam a opção do Estado em direção da legalidade e a favor do princípio da inafastabilidade da jurisdição, incluindo nesta jurisdição também a Internet. Assim sendo, este pressupostos são assim definidos:

- I. Art. 5º, inciso II, de acordo com o qual "ninguém será obrigado a fazer ou deixar de fazer alguma coisa senão em virtude de lei";
- II. Art. 5º, inciso X, que afirma que "invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação";
- III. Inciso XII do art. 5º, pondera que "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";

IV. O dogma de que "A lei não excluirá da apreciação do Poder Judiciário lesão ou ameaça a direito", na forma do art. 5º, inciso XXV, da Constituição Federal; e

V. A garantia segundo a qual "Não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal" (inciso XXXIX, do art. 5º).

Assim, em havendo lesão ou ameaça as liberdades individuais ou ao interesse público, o Estado tem o dever de atuar para reprimir as práticas que violam esse regime de proteção, mesmo que efetivadas por meio de computadores.

O Estado deve positivar, nas esferas civil e penal, mecanismos para prevenir e reprimir práticas ilícitas, assim como os órgãos de persecução criminal devem passar a planejar setores especializados no repúdio à criminalidade por meio do computador.

Não se consegue imaginar uma sociedade em harmonia sem admitir ao mesmo tempo a aplicação de normas, mesmo na forma de simples regras de convivência ou costumes.

Nos dias de hoje, entretanto, existe uma lacuna no ordenamento jurídico brasileiro. Diante disto, o presente estudo, através de uma pesquisa exploratória, buscou apresentar a legislação acerca da tipificação dos crimes de informática, verificando os dispositivos legais aplicáveis ao caso específico, além, do objetivo já mencionado este trabalho se propõe ainda, a saber, como são tratados os crimes digitais na esfera penal, quais os principais delitos registrados, o perfil dos criminosos, como são tipificados estes crimes a partir das adequações a atual legislação e por fim quais os procedimentos que podem ser adotados por estas vítimas quando acometidas por tais crimes.

Buscando alcançar tais metas, foi feito um estudo de caráter qualitativo, através de um levantamento bibliográfico, jurisprudencial e julgados, além de entrevistas em delegacias da redondeza. Neste levantamento foi buscado por formas atuais de controle da criminalidade informática no contexto brasileiro no enfoque de saber como são tipificados estes crimes levando em consideração a legislação atual, qual a base jurídica adotada, os perfis dos criminosos. Em síntese almeja-se a proteção de bens jurídicos digitais e de outros que possam ser afrontados por meio de computadores.

Dois mitos bastante divulgados nos primórdios do ciberespaço era que a Internet é uma terra sem lei, ou seja, de que esta não poderia ser regulada pelo Estado e conseqüentemente seria um ambiente de liberdade absoluta. Contudo, este mitos puderam ser afastados com base nos preceitos constitucionais já citados acima, logo pode-se constatar que,

inclusive na Internet, o Estado brasileiro optou em prol dos princípios da inafastabilidade da jurisdição e da legalidade.

Assim, ressalte-se mais uma vez que em havendo lesão ou ameaça a liberdades individuais ou ao interesse público, o Estado deve agir para reprimir as práticas violadoras desse regime de proteção, ainda que efetivadas pelos meios digitais. Isto porque, tanto a rede quanto a máquina, são criações do homem e, como tais, têm dois aspectos, dependente do uso que se faça delas ou do destino que a elas sejam dados. Igualmente que aproxima as pessoas e ajuda na disseminação da informação, a Internet permite a prática de ilícitos à distância anonimamente, com um poderio lesivo muito mais expressivo que a criminalidade dita "convencional", em alguns casos.

Afirma CARVALHO, (Apud IOB, 2011) sobre os crimes digitais:

Sendo perguntado, por exemplo, se a Internet é um meio novo de execuções de crimes ‘velhos’ ou é, por si mesma, uma geradora de novos delitos, terei o atrevimento de dizer que as duas partes da pergunta se completam para a resposta: há crimes novos, contemporâneos da formação da rede mundial de computadores, mas estão acontecendo, pela net, delitos já de muito tempo conhecidos da sociedade, só que agora perpetrados com o requinte do bit.

DOS CRIMES DE INFORMÁTICA

Segundo ARAS (2001), não há consenso quanto ao *nomen juris* genérico das infrações digitais podendo nomea-las como: delitos computacionais, crimes de informática, crimes de computador, crimes eletrônicos, crimes telemáticos, crimes informacionais, ciberdelitos, cibercrimes. Tais infrações afrontam interesses relativos ao uso, à propriedade, à segurança ou à funcionalidade de computadores e redes de computadores, além de seus hardwares e programas.

Dentre essas denominações, as mais rotineiramente utilizadas têm sido as de crimes de informática ou de crimes informáticos, sendo que as expressões “cibercrimes” ou “crimes telemáticos” são mais adequadas para identificar delitos que abranjam redes de computadores ou a própria Internet ou que sejam executados por meio desta. Estes, então conhecidos na literatura como crimes à distância em sentido estrito (*stricto sensu*).

Os cibercrimes, portanto, como fenômeno oriundo do final do século XX, compreendem todas as naturezas de conduta ilegais concretizadas por meio do uso de um

computador, conectado ou não a uma rede, os exemplos compreendem desde a pirataria de programas de computador à manipulação de caixas bancários, passando por violações nos sistemas de telecomunicação. Todas essas condutas expõem uma vulnerabilidade que os autores desses processos não haviam previsto.

Os crimes praticados por meio do computador preocupam o mundo e tem clamado por definições. Para a OECD — *Organization for Economic Cooperation and Development* (Apud ARAS, 2001), o crime de computador é "qualquer comportamento ilegal, aético ou não autorizado envolvendo processamento automático de dados e, ou transmissão de dados", podendo implicar o manejo de dados ou informações, a sabotagem eletrônica, a falsificação e pirataria de programas, a espionagem virtual, o acesso e/ou o uso não autorizado de redes e computadores.

DOS IMPASSES PARA TIPIFICAÇÃO DOS CRIMES DE COMPUTADORES

Os crimes virtuais classificam-se em próprios ou impróprios, conforme disciplina CARVALHO (Apud IOB, 2011).

Os crimes ditos próprios são aqueles que somente podem ser praticados através da Internet, logo não há execução deste por qualquer outro meio. Pela insuficiente legislação pátria no que se refere aos crimes de informática e o Princípio da Tipicidade no Direito Penal, muitas práticas deixam de ser punidas por ausência de previsão legal expressa no ordenamento jurídico.

Já, os crimes virtuais ditos impróprios são aqueles em que a Internet é apenas um meio para a prática, de modo que a execução e a consumação podem se dá de outra forma. Nesses casos, em regra, os bens infringidos já são tutelados por legislação específica. Dentre outros, podemos citar a apropriação indébita, a calúnia e a pedofilia.

Em que pese a tentativa dos teóricos em classificar os cibercrimes de modo mais peculiar, se verifica que, independentemente da nomeação ou etimologia ofertada, os crimes digitais se manifestam de duas formas distintas: aqueles cometidos através do sistema de informação e aqueles cometidos contra o sistema de informação.

Por esta razão, a classificação mais usual, categorizando os cibercrimes como próprios ou impróprios, atende perfeitamente aos propósitos deste estudo, que tem em um de seus objetivos analisar a repercussão dos crimes digitais no ordenamento jurídico penal brasileiro,

ante as ausências legislativas e à inevitabilidade em se tipificar os crimes denominados próprios, em consonância com o que expõe PECK (2007, p. 251), quanto à “necessidade de tipificação penal de algumas modalidades em que, em razão de suas peculiaridades, merecem ter um tipo penal próprio”. Cumpre ressaltar mais uma vez que, tendo em vista a lacuna na legislação pátria específica, ao aplicar as normas penais existentes, muitas condutas ilícitas não serão alcançadas e, portanto, restarão impunes.

Segundo Scatolin (2007, p.4, Apud PRETO, 2008):

[...] tais crimes são de alta complexidade, tanto para prevê-los, identificá-los e tipificá-los quanto para preveni-los e contê-los. Portanto, só com um conhecimento avançado dos diversos meios de defesa, resultado de um alto investimento na área, ter-se-ia uma significativa redução desse tipo de conduta deplorável.

Portanto, do acima exposto, pode-se concluir que as dificuldades são imensas para a tipificação das condutas delituosas na esfera virtual. Começando pela obtenção de dados e localização do criminoso, pela indicação de onde foi consumado o crime. Pela leitura do art. 70 do Código de Processo Penal o local do crime é determinado pelo lugar da consumação da infração conforme se verifica da literalidade do mencionado artigo: “A competência será, de regra, determinada pelo lugar em que se consumar a infração, ou, no caso de tentativa, pelo lugar em que for praticado o último ato de execução”. Logo, com a ampla quantidade de informações que trafegam por todo o mundo, é comum que até a consumação do ato criminoso os dados empregados neste sejam usados para auxiliar nas práticas criminosas. Daí que tais dados são transmitidos e armazenados em servidores de diferentes países, tornando o trabalho de investigação junto aos provedores de acesso extremamente complexo e lento.

Por outro lado, quando se fala da identificação do criminoso responsável pela prática da ação o determinante é o endereço do Protocolo de Internet do computador utilizado na ação delituosa, ou seja, o endereço IP, que pode ser obtido junto aos provedores de acesso ou aos responsáveis pelo sítio eletrônico hospedado.

Contudo, a aquisição de dados junto a estes provedores é uma empreitada árdua e demorada, devido a alegação por parte dos provedores, de forma equivocada, que os dados alusivos aos usuários estão resguardados pelo sigilo constitucional das informações, o que atrapalha ainda mais o processo de averiguação.

Entretanto, a aquisição dessas informações não é anticonstitucional, posto que a violação do sigilo das correspondências e das comunicações em sistema de informática

(Analogicamente ao Art. 5º, XII da CF/88), protege o teor das informações e não a confidencialidade de acesso, ou seja, o anonimato do autor do crime. E, aliás, não violam a intimidade da honra, da vida privada e/ou da imagem dos usuários (Art. 5º, X da CF/88), pois a intenção é conseguir somente dados fundamentais do usuário, como nome, endereço e numeração de documentos, dados estes que não são resguardados pelo sigilo constitucional, dados que, comumente são fornecidos em simples cadastros ou compras, por exemplo.

Comprovando que realmente não é anticonstitucional a aquisição de informações básicas dos usuários segue jurisprudência que relata um caso específica de requisição destes dados a provedores de acesso.

MANDADO DE SEGURANÇA – CRIMES CONTRA A HONRA PRATICADOS PELA INTERNET – REQUISIÇÃO DE ORDEM JUDICIAL PARA QUE O PROVEDOR FORNEÇA A IDENTIFICAÇÃO DO TITULAR DE DETERMINADAS CONTAS DE E-MAILS – CONCESSÃO DA SEGURANÇA – Como corolário do princípio da dignidade da pessoa humana, a Constituição Federal atual assegurou o direito à intimidade, proclamando no art. 5º, inciso XII, a inviolabilidade do sigilo das comunicações telegráfica de dados e telefônica – Apesar da magnitude do direito em destaque, de cunho constitucional, é sabido que as liberdades públicas estabelecidas não podem ser consideradas como tendo valor absoluto cedendo espaço em determinadas circunstâncias, sobretudo quando utilizadas para acobertar a prática da atividade ilícita – **O fornecimento de dados cadastrais em poder do provedor de acesso à Internet, que permitam a identificação de autor de crimes digitais, não fere o direito à privacidade e o sigilo das comunicações, uma vez que dizem respeito à qualificação de pessoas, e não ao teor da mensagem enviada.** (TJMG – MS 1.0000.04.414635-5/000 – 3ª C.Crim. – Rel. Des. Paulo Cezar Dias – DJMG 18.08.2005 – p. 03) (Grifos não presentes no original)

Após a identificação do IP de onde foi originado o acesso, prima-se pela identificação da pessoa que o realizou e praticou o ato criminoso. Contudo, nem sempre o acesso é realizado de um ambiente onde residem poucas pessoas, o acesso pode ocorrer de empresas, *Lan Houses* ou até mesmo por meio de dispositivos de telefonia móvel. Frequentemente os delinquentes têm se utilizado de locais públicos para a realização de seus atos, que com a difusão dos *hotspot* em aeroportos e shopping centers, que, desta forma, tornam-se um local perfeito para obstacular a descoberta de sua autoria.

DOS PRINCIPAIS DELITOS REGISTRADOS

Conforme se mencionou acima, com o advento da Internet algumas demandas já conhecidas e outras novas surgiram no meio informático, destaque-se: venda de bens impossíveis ou inexistentes, espionagens industriais e comerciais, pornografia, pedofilia, transferências ilegais de contas bancárias, fraudes em leilões virtuais, plágio, falsificação, estelionatos. Destes, segundo o Núcleo de Combate aos Cibercrimes do Paraná (Nuciber) mais de 70% das ocorrências são de crimes contra o patrimônio, que envolvem desvios de dinheiro de contas bancárias e estelionatos, seguidos dos crimes contra a honra, como a exibição de imagens ou de material que atingem a imagem da vítima.

A tabela a seguir, proposta por PECK (2005, Apud PRETO, 2008), apresenta algumas infrações digitais com suas respectivas tipificações na legislação brasileira.

TABELA DE INFRAÇÕES DIGITAIS MAIS FREQUENTES NA VIDA COMUM DO USUÁRIO DO BEM		
Descritivo da Infração	Infração	Tipificação na Lei Positiva da
Entrar na rede da empresa ou de concorrente e mudar informações (mesmo que com uso de um software)	Adulterar dados em sistema de informações	Art.313-B do CP
Enviar um e-mail dizendo que vai pegar a pessoa	Ameaça	Art.147 do CP
Criar uma Comunidade para ensinar como fazer "um gato"	Apologia de crime ou criminoso	Art.287 do CP
Colocar foto em Comunidade Online com aquele "dedo"	Ato obsceno	Art.233 do CP
Falar em um chat que alguém cometeu algum crime (ex. ele é um ladrão...)	Calúnia	Art.138 do CP
Usar logomarca de empresa em um link na página da internet, em uma comunidade, em um material, sem autorização do titular, no todo ou em parte, ou imitá-la de modo que possa induzir a confusão.	Crime contra a propriedade industrial	Art.195 da Lei 9.279/96

Empregar meio fraudulento, para desviar, em proveito próprio ou alheio, clientela de outrem, por exemplo, uso da marca do concorrente como palavra-chave ou link patrocinado em buscador.	Crime de Concorrência Desleal	Art.195 da Lei 9.279/96
Usar cópia de software sem ter a licença para tanto	Crimes Contra Software "Pirataria"	Art.12 da Lei 9.609/98
Enviar um vírus que destrua equipamento ou conteúdos	Dano	Art.163 do CP
Dar forward para várias pessoas de um boato eletrônico	Difamação	Art.139 do CP
Enviar um e-mail para terceiros com informação considerada confidencial	Divulgação de segredo	Art.153 do CP
Criar uma Comunidade Online que fale sobre pessoas e religiões	Escárnio por motivo de religião	Art.208 do CP
Se você recebeu um spam e resolve devolver com um vírus, ou com mais spam	Exercício arbitrário das próprias razões	Art.345 do CP
Enviar e-mail com remetente falso (caso comum de spam)	Falsa identidade	Art.307 do CP
Divulgar um banner para sites pornográficos	Favorecimento da prostituição	Art. 228 do CP
Fazer um saque eletrônico no internet banking com os dados de conta do cliente	Furto	Art.155 do CP
Criar uma Comunidade dizendo "quando eu era criança, eu roubei a loja tal..."	Incitação ao Crime	Art.286 do CP
Enviar um e-mail para a Pessoa dizendo sobre características dela (gorda, feia, vaca,...)	Injúria	Art.140 do CP
Fazer cadastro com nome falso em uma loja virtual	Inserção de dados falsos em sistema de informações	Art.313-A do CP
Monitoramento não avisado previamente, coleta de informações espelhadas, uso de <i>spoofing</i> <i>Page</i>	Interceptação de comunicações de informática	Art.10 da Lei 9.296/96

Participar do Cassino Online	Jogo de azar	Art.50 da L.C.P.
Ver ou enviar fotos de crianças nuas online (cuidado com as fotos de seus filhos e dos filhos de seus amigos na net)	Pedofilia	Art.247 da Lei 8.069/90 "ECA"
Falar em um Chat que alguém é isso ou aquilo por sua cor	Preconceito ou Discriminação Raça-Cor-Etnia-Etc.	Art.20 da Lei 7.716/89
Copiar um conteúdo e não mencionar a fonte, baixar MP3 que não tenha controle como o WMF	Violação ao direito autoral	Art.184 do CP

Tabela 1 – Infrações digitais mais frequentes na vida comum do usuário do bem

DO PERFIL DO CRIMINOSO

Durante muito tempo, o perfil dos criminosos cibernéticos estava estritamente relacionado à capacidade e habilidade do agente em manejar conhecimentos informáticos. Não por outra razão, normalmente os crimes digitais se limitavam a invasões de sistemas, encarados pelos hackers como desafios para a demonstração de sua capacidade e inteligência.

Se antes o cibercriminoso se restringia àquele usuário com conhecimento de informática acima da média, motivado pela demonstração de sua capacidade e habilidade – um exemplo disso foi o criador do vírus Melissa, David Smith, que, em 1999, causou um prejuízo correspondente a US\$ 80 milhões às vítimas do vírus; porém, não obteve lucro algum, pois a sua motivação era a disseminação em escala do vírus, apenas para demonstração de vasto conhecimento da fragilidade dos usuários da Internet – nos dias atuais, o traçado do perfil do criminoso não ignora nenhum dos usuários da Rede, mesmo aqueles com conhecimento mínimo dos sistemas de informática; sejam eles motivados pelo egocentrismo ou inspirados pela possibilidade de obtenção de lucro.

O perfil estereotipado do cibercriminoso que perdurou durante muito tempo não corresponde, em sua totalidade, ao traçado atualmente. Embora as características comuns ainda sejam aplicadas a alguns agentes, é equivocada a ideia de que os cibercriminosos são,

normalmente, adolescentes do sexo masculino, pacíficos, socialmente ineptos e que detêm avançado conhecimento técnico.

Em que pese ser imensamente válida a construção de um perfil criminoso, não se pode encarar determinado perfil como verdade absoluta. Por vezes, existirão infratores que divergem dos perfis traçados, no tocante à ocupação, às experiências de vida, à aparência física, à formação acadêmica, ao sexo e ao estado civil. Desta forma, vê-los como um grupo com características comuns seria uma atitude errônea, visto que os cibercriminosos atuam em diferentes países e culturas impulsionados por diferentes motivações. Decerto que, independentemente da motivação que impele o agente infrator, para o ordenamento jurídico resta evidente que o cibercriminoso atua de modo desprendido e consciente com vista a atingir seus objetivos ilícitos.

Por certo vale conferir trecho de uma entrevista, retirada de Revista da Web (2002) onde a criminosa conta quais foram suas motivações e razões para a execução do crime, do relato abaixo percebe-se claramente que o perfil traçado não é definição absoluta de um cibercriminoso.

"Eu sou uma hacker! Estudo de manhã, passo a tarde inteira na faculdade e chego em casa por voltas das 8 horas da noite, esgotada, querendo cama e travesseiro. Ainda dou uma morgadinha antes da mutação. No silêncio da madrugada quando toda minha família está capotada, eu me transformo numa pirata da Internet. [...] Às vezes penso por que faço isso. Poderia dormir mais tempo, evitar as olheiras, levar uma vida mais saudável. Mas esse mea-culpa termina assim que ligo a máquina. Tenho orgasmos cibernéticos, só em pensar que invadirei algum site. A trama, a estratégia, a organização, a execução. É tudo muito excitante.

Sou do bem. O hacker verdadeiro é do bem, uma pessoa curiosa. [...] Na pele de um cracker, o hacker do mal, cometi um roubo virtual, roubei um cartão de crédito. Sem pedir licença, entrei no computador de um cara, fuzei a vida dele e, por fim, sursurpiei o número de seu cartão para comprar uma coleção de CDs de música clássica, no valor de 400 reais. Se pedisse o dinheiro para os meus pais, com certeza conseguiria, porque temos um padrão de vida confortável. Fiz isso só para me sentir poderosa, a bambambã do pedaço.

Evidente que a criação de perfis, embora não atenda a todos os criminosos, é de grande valia para a investigação policial, pois associada às informações coletadas acerca do crime, pode contribuir para a delimitação do campo de investigação e de suspeitos, e para a correlação com outros crimes de idênticas características. Assim, o perfil do cibercriminoso,

per si, não garante o êxito das investigações e não fundamenta um processo criminal. Há que se considerar o conjunto probatório para se atingir a Justiça.

DOS PROCEDIMENTOS PARA NOTICIAR CRIMES DIGITAIS

O documento eletrônico não se vincula ao meio físico em que está armazenado, possuindo autonomia em relação a ele. O documento eletrônico é, então, uma sequência de bits que, trazida por meio de determinado programa de computador, seja representativa de um fato. Da mesma forma que os documentos físicos, o documento eletrônico não se resume em escritos: pode ser um texto escrito, como também pode ser um desenho, uma fotografia digitalizada, sons, vídeos, enfim, tudo que puder representar um fato. Diante disto, qualquer arquivo pode se prestar a provar fatos relacionados aos crimes digitais.

A notificação dos crimes praticados por meio de computadores é de grande importância para a construção de uma legislação acerca do tema, pois quanto mais a população se prontifica a denunciar estes crimes mais o Estado é forçado a criar leis ou, no pior caso, fazer interpretações na legislação atual para enquadrar tais crimes.

Portanto, quando vítima de um cibercrime, deve o paciente agrupar a maior quantidade de provas para noticiar este crime, uma vez que estas são determinantes para encontrar o criminoso e reconhecer sua autoria. Dentre as provas que podem ser juntadas pelas vítimas é possível destacar as negociações realizadas por e-mail, imagens das telas dos sites, ou seja, deve-se salvar todo o material que possa servir como meio de prova antes que estas sejam apagadas ou retiradas da rede. Também é possível ir ao cartório lavrar uma ata notarial que comprove a veracidade dos documentos. Além disso, deve procurar uma delegacia para abrir um boletim de ocorrência.

A prova eletrônica é apta a evidenciar a ocorrência de um fato e, se colhida corretamente, faz prova mais eficaz do que aquela colhida por outro meio. Diante do exposto é possível citar algumas jurisprudências que comprovam a eficácias de tais provas.

—Responsabilidade civil subjetiva. Contrato de Subagência marítima. Fato jurídico que pode ser provado mediante presunção que não contrarie as provas dos autos. **Correio eletrônico que serve de documento probatório.** Atuação culposa da apelante configurada, quando não observa conhecimentos exigíveis, ocasionando a retenção da mercadoria no porto por falta de documentação adequada. Subagente que não se desincumbiu de seu ônus probatório no sentido

de ter operado sem culpa. Sentença mantida. Recurso ao qual se nega provimento. (TJ/RJ, Relator Antonio Iloizio B. Bastos, Apelação nº 0066203-29.2006.8.19.0001, Julgado em 17/08/2010) (Grifos Nossos)

—REPARAÇÃO DE DANOS. INTERNET. VINCULAÇÃO DE PÁGINA NO SITE DE RELACIONAMENTOS ORKUT A COMUNIDADE OFENSIVA. MONTAGEM E DISPONIBILIZAÇÃO DE FOTO DA AUTORA. OFENSA À HONRA DA AUTORA. DANO MORAL IN RE IPSA. DEVER DE INDENIZAR. QUANTUM INDENIZATÓRIO MANTIDO. SENTENÇA CONFIRMADA POR SEUS PRÓPRIOS FUNDAMENTOS. 1. Terceiro não identificado apropriou-se da senha do "perfil" da autora na rede de relacionamentos Orkut. A aludida página serviu para proferir ofensas à dignidade da autora, causando-lhe danos, os quais devem ser indenizados. 2. Tendo a empresa ré hospedado a página ofensiva, não providenciando sua exclusão mesmo após diversas solicitações feitas pela própria autora através do site, é aquela responsável pelos danos ocasionados à demandante, ainda que o "perfil" falso tenha sido confeccionado por terceira pessoa. 3. A verba indenizatória arbitrada pelo juízo singular (R\$ 6.000,00) mostra-se proporcional à ofensa sofrida, pois, ainda que a comunidade ofensiva tenha permanecido disponível por sete dias apenas, houve divulgação da mesma para várias pessoas do relacionamento da autora, como se pode verificar pelos documentos de fls. 131 a 148. Imperioso, assim, a manutenção do valor da indenização fixada. Sentença mantida por seus próprios fundamentos. Recurso improvido. (TJ/RS, Relator: Saldanha da Fonseca, Recurso Cível nº 71002090603, Julgado em 17/09/2009)

CONCLUSÃO

Ao longo desse estudo, evidenciou-se que a necessidade de regulação em se estabelecer normas para o provimento do serviço de Internet, o seu funcionamento e o controle do conteúdo veiculado na Rede surgiu em função dos avanços tecnológicos e não por uma imposição legal. Apontou-se, ainda, para a necessidade de tipificação, no ambiente virtual, de crimes e penalidades correspondentes no mundo real, bem como para a inevitabilidade de se encarar o Direito Penal Digital sob uma nova ótica jurídica.

A temática envolvendo os cibercrimes ainda se encontra em estágio embrionário, mas os debates acerca da matéria têm permitido a exploração dessa nova realidade que assola a sociedade.

É certo que se faz necessária a construção de uma política continuada abrangente, envolvendo segurança da informação e demais aspectos jurídicos e técnicos, bem como que se estabeleçam garantias e proteção aos bens jurídicos maculados pelo advento da Internet e seu caráter transnacional.

Ressalte-se que o Ministro Gilmar Mendes ressaltou que os problemas envolvendo o uso da Internet no Brasil são responsáveis pela maior preocupação dos magistrados, considerando a excessiva judicialização que ocorre no país.

Como exposto ao longo dessa pesquisa, somente um conjunto de ações conscientes poderá culminar num efetivo combate repressivo aos crimes digitais. A mera tipificação de novas condutas delituosas – embora importante e necessária – não garante a consecução da reprimenda aos cibercriminosos.

Ademais, a prestação jurisdicional deverá estar associada a ações como: a criação de base de dados unificadas no âmbito da polícia judiciária; a preservação de dados dos usuários pelos provedores de Internet; a identificação digital obrigatória dos usuários, coibindo o irrestrito anonimato; o aumento de pena e indenização, considerando que na Internet os danos e a exposição são significativamente maiores; a criação de delegacias especializadas, que disponham de profissionais especialistas e treinados; a criação da ciberpolícia com atuação no ciberespaço; a constituição de setores específicos para apuração de denúncias de fraudes envolvendo pequenos valores para a elaboração e identificação de um possível padrão; e, por fim, a realização de constantes campanhas instrutivas em escolas, empresas e sociedade.

Sem a união de todas essas medidas, é provável que a sociedade continue a ser vitimada pela ação inescrupulosa dos cibercriminosos.

Finaliza-se, pois com o importante alerta ofertado por Lima e Silva (Apud BEZERRA, 2011) “a sociedade tem que ter em mente que o crime sempre, sempre está um passo a frente da polícia, e o que define se essa polícia é eficiente, ou não, é a distância desse passo, o chamado *gap* entre o crime e a polícia.”

Tendo em vista o que aqui restou explanado, conclui-se que o estudo dos crimes digitais requer maior atenção da sociedade e dos representantes políticos do país, de modo que o debate não seja mais um entrave no combate ao crime, mas uma forma de repressão aos criminosos que oportunamente agem em uma terra ainda considerada “sem lei”.

Portanto, existem caminhos para a solução dos problemas inseridos em nosso meio pelos abusos tecnológicos, contudo é necessário muito estudo sobre o tema.

Assim sendo, é preciso conviver com a ambivalência dos computadores, pois isto é um fato. E primando pela convivência, o Direito se exhibe com uma possível solução para as ditas inquietações do ciberespaço. Porquanto, na realidade atual é indispensável a atuação do Direito e em alguns casos a incidência da norma penal como garantia de compromisso social aqui e no mundo virtual.

REFERÊNCIAS

ARAS, Vladimir. **Crimes de Informática** – Uma nova criminalidade. Disponível em < <http://jus.com.br/revista/texto/2250/crimes-de-informatica> >. Acessado em 12 nov 2011.

BEZERRA, Ana Cristina. **Cibercrime no Brasil**. São Paulo: Ed. Independente, 2010.

BRASIL. Constituição Federal, 1988. Disponível em < http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm >. Acessado em: 07 nov 2011.

BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Código Penal. Disponível em < <http://www.planalto.gov.br/ccivil/decreto-lei/Del2848.htm> >. Acessado em 07 nov 2011.

BRASIL. Decreto-Lei nº 3.689, de 3 de outubro de 1941. Código de Processo Penal. Disponível em < <http://www.planalto.gov.br/ccivil/decreto-lei/Del3689.htm> >. Acessado em 07 nov 2011.

CERT.br – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Disponível em: <<http://www.cert.br>>. Acesso em: 16 nov 2011.

INELLAS, Gabriel Cezar Zaccaria. **Crimes na Internet**. 2 ed. São Paulo: Ed. Juarez de Oliveira, 2009.

INFORMAÇÕES OBJETIVAS PUBLICAÇÕES JURÍDICAS LTDA – IOB. **Juris Síntese DVD**, São Paulo: Ed. IOB. nº 90 (Jul-Ago/2011). DVD-ROM

MITNICK, Kevin D.; SIMON; William L. **A arte de enganar**. São Paulo: Pearson Education do Brasil, 2006.

PRETO, Vagner de Oliveira. **Problemas e Dificuldades Tecnológicas e Legislativas na Tipificação e Elucidação de Crimes Digitais nos Atos de Polícia Judiciária**. 2008. Trabalho de Conclusão de Curso (Tecnólogo) – Faculdade de Tecnologia da Zona Leste, São Paulo, SP.

PERC, Patrícia. **Direito Digital**. 2. ed. São Paulo: Ed. Saraiva, 2007.

RAMOS, Carlos Henrique. “Eu roubei um cartão de crédito”. Revista da WEB. São Paulo: Ed. Abril, 2002.

VIEIRA, Jair Lot. Crimes na Internet: Interpretados pelos Tribunais. 1 ed. São Paulo:Ed. Edipro, 2009.