UNIVERSIDADE PRESIDENTE ANTÔNIO CARLOS - UNIPAC
FACULDADE DE CIÊNCIAS JURÍDICAS E SOCIAIS DE BARBACENA-FADI
CURSO DE GRADUAÇÃO EM DIREITO

JOSÉ RENATO FAGUNDES DO NASCIMENTO

CRIMES PRATICADOS PELA INTERNET E A DEFICIÊNCIA DE UMA LEGISLAÇÃO ESPECÍFICA

BARBACENA
2016

JOSÉ RENATO FAGUNDES DO NASCIMENTO

CRIMES PRATICADOS PELA INTERNET E A DEFICIÊNCIA DE UMA LEGISLAÇÃO ESPECÍFICA

Monografia apresentada ao curso de Graduação em Direito da Universidade Presidente Antônio Carlos - UNIPAC, como requisito parcial à obtenção do título de bacharel em Direito.

Orientadora: Prof.ª Esp. Josilene Nascimento Oliveira

BARBACENA
2016

José Renato Fagundes do Nascimento

CRIMES PRATICADOS PELA INTERNET E A DEFICIÊNCIA DE UMA LEGISLAÇÃO ESPECÍFICA

Monografia apresentada ao curso de graduação em Direito da Universidade Presidente Antônio Carlos - UNIPAC, como requisito parcial à obtenção do título de bacharel em Direito.

Aprovada em ____/____/____

BANCA EXAMINADORA

Profª. Esp. Josilene Nascimento Oliveira
Universidade Presidente Antônio Carlos- UNIPAC

Prof. Esp. Paulo Afonso de Oliveira Júnior
Universidade Presidente Antônio Carlos – UNIPAC

Esp. Marcelo Sebastião de Paula
Servidor do Tribunal de Justiça de Minas Gerais – TJMG

Dedico este trabalho em homenagem a meus pais, José Fagundes do Nascimento e Luzia Margarida do Nascimento, que sempre me educaram no caminho do bem.

AGRADECIMENTOS

Agradeço a meus mestres por todo conhecimento e incentivo, à minha esposa, por todo apoio e compreensão e aos meus filhos, por lições de vida a cada dia.

A internet é a primeira coisa que a humanidade criou e não entende, a maior experiência de anarquia que jamais tivemos.

Eric Schmidt

RESUMO

Trata-se de trabalho que visa relatar como a internet se desenvolveu e se tornou, hoje, a maior e mais usada fonte de divulgação de conhecimentos, de idéias, de opiniões, uma das primeiras fontes em entretenimento, uma grande fonte de comércio e trabalhos e também uma grande oportunidade para o cometimento de delitos. Os crimes praticados por meio da internet são variados, inúmeros e quase sempre impunes. Trata-se de estudo monográfico com revisão bibliográfica, cujo foco principal é analisar se as leis que já existem para prevenir e reprovar a prática de delitos cometidos pela internet já são suficientes ou se haveria a necessidade de uma legislação específica para tratar do assunto com maior efetividade. Com o estudo realizado, constatou-se serem indispensáveis a modificação da legislação, bem como a capacitação de profissionais para o combate a crimes desta natureza.

Palavras-chave: Internet. Crimes. Legislação Específica. Insuficiência. Impunidade.

ABSTRACT

It is a work that aims to report how the internet has developed and has become, today, the largest and most used source of knowledge, ideas, opinions, one of the first sources of entertainment, a great source of commerce and work And also a great opportunity for the commission of crimes. The crimes practiced through the Internet are varied, numerous and almost always impunity. It is a monographic study with a bibliographical review, whose main focus is to analyze whether the laws that already exist to prevent and condemn the practice of crimes committed by the Internet are enough or if there would be a need for specific legislation to deal with the subject with greater Effectiveness. With the study carried out, it was verified that it is indispensable to modify the legislation, as well as the training of professionals to combat crimes of this nature.

Keywords: Internet. Crimes. Specific Legislation. Failure. Impunity.

SUMÁRIO

1 INTRODUÇÃO

Os crimes de internet estão cada vez mais comuns no Brasil e seu combate não está acompanhando seu crescimento, o que passa à sociedade uma visão cada vez maior de impunidade, já que os crimes de internet acometem as pessoas em lugares em que elas se sentiam seguras: em seu lar, em seu trabalho, em seu íntimo. Por isso este assunto é muito importante e contemporâneo.

No Brasil, há mais de um milhão de denúncias de crimes pela internet, como pedofilia e racismo, e esse número é ainda maior se acrescentar os crimes contra a honra e o patrimônio. O que causa esse aumento dessa criminalidade é a certeza da impunidade. Em todo País há apenas dezesseis delegacias especializadas em crimes cibernéticos. Há leis que punem esses crimes, mas não há como investigar com a falta de estrutura e organização do Estado.[1]

Um dos crimes que se tornou enorme em sua proporção é o crime contra a honra. Os crimes de internet contra a honra estão crescendo cada vez mais e as pessoas se sentem perdidas e desamparadas pela Justiça em meio à impunidade. Denegrir a imagem de alguém usando de calúnias, difamação e injúrias, tornou-se prática fácil pela internet, pois o acesso à internet é extremamente difundido e o agressor fica protegido atrás de seu teclado. E a boa reputação de uma pessoa pode ser totalmente destruída em pouco tempo e de forma encorajada pela certeza da impunidade.[2]

Crimes contra a honra praticados pela internet são fáceis de serem cometidos e difíceis de serem punidos haja vista a facilidade de acesso à internet, com proteção de anonimato ao agressor.[3]

A dificuldade do crime cibernético é de encontrar provas e o autor do crime, já que a internet permite a expressão de forma anônima. Isso contribui para a facilidade de cometer crimes e para a impunidade.[4]

Além dos crimes contra a honra, podem ser pensados: os crimes contra o patrimônio: quantas vezes se ocorrem reclamações, tais como : "_comprei pela internet e não recebi o

---

[1] ARANHA, Adalberto José Q.T. Camargo. **Crimes contra a Honra.** 3 ed. São Paulo: Saraiva, 2005.

[2] MIRABETE, Julio Fabbrini. FABBRINI, Renato N. **Manual de Direito Penal.** 25 ed. São Paulo. Atlas. 2007. V2, p 127.

[3] Id., ibid, 1.

[4] Id., ibid, 1.

produto e não consigo o dinheiro de volta.” Ou: “_o produto veio danificado e não consigo trocá-lo ou devolvê-lo.” ? Ou ainda: quantas notícias de quadrilhas ou bandidos cibernéticos invadem sites de bancos e saqueiam contas bancárias? Ou: quantas empresas já não foram invadidas ciberneticamente e roubadas ou prejudicadas?

Há também os crimes cibernéticos onde os delinquentes invadem sites, emails, blogs e os destroem ou simplesmente roubam informações que sejam úteis para outros crimes, bem como o de pirataria.

Existe, ainda, um dos crimes mais cometidos pela humanidade e talvez o menos penalizado, o crime contra a criança: pedofilia, aliciamento de menores, venda de crianças e menores para as diversas finalidades (sexo, adoção ilegal, tráfico de drogas, trabalho escravo e talvez outras que ainda não se tem conhecimento). Além de outros crimes contra a criança, como, por exemplo, a destruição da infância com corrupção de sua inocência. Em sites de jogos infantis são vistos jogos de destruição, de morte, de guerra. Em sites infantis são vistas cenas que estimulam a luxúria, a comercialização e a banalização dos sentimentos.

Como se demonstra, este tema é de extrema importância atual, pois está cada vez mais comum e atingindo mais e mais pessoas de diferentes classes sociais; é um assunto em pauta quando se trata de impunidade; há questões que envolvem também um terceiro, que não o autor e a vítima, que é o provedor.

Este presente trabalho tem como objetivo demonstrar um estudo de revisão literária sobre o assunto, demonstrar como é praticado e a importância de se combater esse tipo de crime, mostrar o que já tem no Brasil a respeito e tentar mostrar o que ainda há para se fazer e como combater a impunidade que cerca este assunto.

Os crimes pela internet, como dito, estão cada vez com mais espaço no Brasil e também no mundo. Durante a abordagem deste tema, serão elucidadas algumas questões que desde já se tornam importantes: 1- Qual a jurisdição responsável? 2- Existe lei específica para estes crimes? Quando e como surgiu ou o que se propõe hoje? 3- Quem cometem estes crimes? Quais os perfis destes agressores? 4- Como está sendo abordado este assunto pela Justiça e pelo Estado? 5- Quais são as vítimas? Como estão reagindo as vítimas destes crimes? Estão conseguindo se defender? 6- Como se dá a punição aos agressores que são descobertos e julgados? 7- Qual a proporção de casos punidos e não punidos? 09- O que tem se pensado para se combater a impunidade que rodeia estes crimes? 10-O que seria o ideal para se evitar esses crimes e para puni-los? 11- Qual é a extensão em número de pessoas no Brasil que realmente entendem sobre a cibernética e que estariam aptos tecnicamente a combater estes crimes?

2 HISTÓRIA DA INTERNET: UMA REVISÃO SUCINTA

Em 1979 a IBM lançou o computador pessoal PC-XT, capaz de executar 750000 funções por segundo e velocidade máxima de 8 MHz. Dezenove anos depois, em 1998, foi lançado o Pentium III, capaz de executar mais de 400 milhões de operações por segundo e velocidade superior a 500 MHz. Em 2002, a capacidade de processamento podia superar 2GHz.[5]

Esse surpreendente e explosivo desenvolvimento da tecnologia resultou na era da informação, sendo impressionante a maneira como a informação hoje é processada, utilizada e divulgada. A Internet foi algo fundamental para a globalização da informação e aceleração do desenvolvimento da tecnologia.

A Internet foi se desenvolvendo e, a partir daí, viu-se a necessidade de mais tecnologia e melhores computadores, para acompanhar seu crescimento.

A Internet é uma rede mundial de computadores: uma rede de computadores interligados entre si em escala mundial através de um protocolo comum chamado TCP/IP (Transmission Control Protocol/Internet Protocol).[6]

A Internet tem revolucionado o mundo dos computadores e das comunicações como nenhuma invenção foi capaz de fazer e representa um dos mais bem sucedidos exemplos dos benefícios da manutenção do investimento e do compromisso com a pesquisa e o desenvolvimento de uma infra-estrutura para a informação.[7]

A Internet nasceu nos EUA (Estados Unidos da América), na década de 60, época da Guerra Fria.[8] Em 1961, Leonard Kleinrock, do MIT (Massachussets Institute of Technology),

---

[5] CORRÊA, Gustavo Testa. **Aspectos jurídicos da Internet.** 2 ed. ver. São Paulo: Saraiva, 2002.

[6] CASTRO, Aldemário Araújo. (Procurador da fazenda nacional, Procurador geral adjunto da fazenda nacional, ex-coordenador geral da dívida ativa da União, professor da Universidade Católica de Brasília, vice-presidente do Instituto Brasileiro de Direito Eletrônico). **Informática Jurídica e Direito da Informática.** Livro virtual. Cap 4, Internet: conceito, histórico e funcionamento. 06 pg. 2007. Disponível em <http://www.aldemario.adv.br/infojur/c onteudo4texto.htm>. Acesso em 27 de julho de 2010.

[7] LEINER, Barry M.; CERF, Vinton, G.; CLARK, David D.; KAHN, Robert E.; KLEINROCK, Leonard; LYNCH, Daniel C.; POSTEL, Jon, ROBERTS, Larry G.; WOLFF, Stephen. (Idealizadores da Internet). **A Brief History of the Internet.** Texto traduzido. 15 p. Ano ? Disponível em <http://www.aisa.com.br/historia.html>. Acesso em 03 de junho de 2010.

[8] BOGO, Kellen Cristina. (Graduada em Ciência da Computação e Colaboradora da Almeida & Cappeloza Consultores Associados). **A história da Internet – Como tudo começou...".** Edição número 11. 05 pg. Matéria publicada em 01/07/2000. Disponível em <http://www.Kplus.com.br/materia.asp?co=11&rv=Vivencia>. Acesso em 17 de agosto de 2010.

publicou o primeiro trabalho sobre a teoria de troca de pacotes e convenceu Roberts da possibilidade teórica das comunicações usando pacotes ao invés de circuitos. Em um sistema de comutação de pacotes, os dados a serem comunicados são divididos em pequenas partes. Essas partes são identificadas de forma a mostrar de onde vieram e para onde devem ir e os pacotes possuem um tamanho máximo. Os pacotes são enviados de computador para outro até alcançar seu destino. Se algum for perdido, poderá ser reenviado pelo emissor original e para evitar retransmissões desnecessárias, o destinatário confirma o recebimento.

Em 1962, uma série de memorandos foram escritos por J.C.R. Licklider, do MIT, discutindo o conceito da "Rede Galáxica", onde previa vários computadores interconectados globalmente, pelo meio dos quais todos poderiam acessar dados e programas de qualquer local rapidamente. Ele foi o primeiro gerente de programa de pesquisa de computador do DARPA (Departamento de defesa norte-americano).

O passo seguinte, seria fazer dois computadores se comunicarem. Em 1965 Roberts e Thomas Merrill conectaram um computador em Massachussets com um na California com uma linha discada de baixa velocidade, foi o primeiro computador de rede do mundo. Eles viram, porém que o circuito do sistema telefônico era inadequado e confirmaram a convicção de Kleinrock sobre a necessidade de troca de pacotes.[9]

No final de 1966, Roberts começou a trabalhar no DARPA para desenvolver o conceito das redes computadorizadas e elaborou seu plano para o projeto ARPANet (rede para conectar os departamentos de pesquisa e as bases militares, desenvolvida pela empresa ARPA – Advanced Research and Projects Agency – sem ter um centro definido ou uma rota única para as informações, tornando-se quase indestrutível se a antiga União Soviética resolvesse cortar a comunicação da defesa americana).[10,11,12]

Em 1967 Roberts apresentou seu trabalho numa conferência, onde teve o conhecimento de mais dois trabalhos sobre o papel das redes de troca de pacotes: o projeto RAND (1962-1965. Paul Baran e outros) e o projeto da NPL (Nuclear Physics Laboratory) na Inglaterra (pelos ingleses Donald Davies e Roger Scantlebury). Estavam se desenvolvendo em paralelo sem que nenhum dos pesquisadores soubesse dos outros trabalhos.

---

[9] Id., ibid, 7.

[10] Id., ibid, 7.

[11] Id., ibid, 8.

[12] Id., ibid, 6.

Em 1968, após Roberts e o DARPA terem refinado a estrutura para a ARPANET, foi feita uma seleção de grupos de estudiosos para desenvolver um dos componentes chaves: o Processador de Interface das Mensagens (IMP). Em 1969 foi escolhido o primeiro nó da ARPANET: a UCLA (Universit of California at Los Angeles) foi o primeiro servidor de computador conectado, após a instalação do primeiro IMP. No final de 1969, quatro servidores estavam conectados na ARPANET e os trabalhos se concentravam na rede em si e no estudo das possíveis aplicações da rede.[13]

Em 1971 foi concluído o primeiro protocolo servidor a servidor da ARPANET, chamado NCP (Network Control Protocol), um protocolo de comutação de pacotes. E os usuários puderam desenvolver suas aplicações.[14]

Em 1972, Kahn organizou uma demonstração sobre a ARPANET na Conferência Internacional de Comunicação entre Computadores e foi a primeira demonstração para o público. Neste ano também foi introduzido o Correio Eletrônico. E, neste mesmo ano, Kahn foi o primeiro a introduzir uma idéia chave que a Internet como conhecemos hoje incorpora: rede de arquitetura aberta, na qual a opção pela tecnologia de uma rede individual não é ditada por nenhuma arquitetura de rede particular e sim escolhida livremente pelo provedor, que a torna capaz de entrar em rede com outras redes.

O NCP não tinha a habilidade de endereçar redes e máquinas além da destinação IMP da ARPANET e deveria ser mudado. Então Kahn começou desenvolver um novo protocolo: TCP/IP (Transmission Control Protocol/Internet Protocol). Esse novo protocolo permitia o crescimento praticamente ilimitado da rede. Os protocolos TCP/IP torna possível uma infra-estrutura genérica na rede, na qual novas aplicações podem ser concebidas, como aconteceu com a World Wide Web. E essa infra-estrutura genérica da rede é também um conceito-chave da Internet de hoje.[15,16,17]

---

[13] Id., ibid, 7.

[14] Id., ibid, 7.

[15] Id., ibid, 7.

[16] Id., ibid, 8.

[17] TEXTO PUBLICADO NA INTERNET. **História da Internet.** 03pg. Ano? Disponível em <http://www.brasiescola.com/informática/internet.htm>. Acesso em: 14 de setembro de 2010.

Nos anos 70 as universidades e outras instituições que faziam trabalhos relativos à defesa tiveram permissão para se conectar à ARPANET. Em 1975 existiam aproximadamente 100 sites.[18]

Em 1980 o protocolo TCP/IP foi adotado. A transição do protocolo foi um desafio e no dia 01/01/1983 houve a transição imediata, requisitando todos os servidores em conversão simultânea. Esse protocolo é a base da Internet até hoje. Tal fato levou à divisão entre comunidades militar e não militar. A MILNET passou a suportar os requisitos operacionais e a ARPANET passou a suportar as necessidades de pesquisa.[19]

Em 1985, a entidade americana NSF (National Science Foundation) interligou os supercomputadores de seu centro de pesquisa a NSFNET, que em 1986 entrou para a ARPANET. Essas passaram a ser as duas espinhas dorsais (backbone) de uma nova rede, que junto com os demais computadores ligados a elas, formavam a Internet.[20]

Neste ano de 1985 a Internet já estava bem estabelecida como uma larga comunidade de suporte de pesquisadores e desenvolvedores e começava a ser usada por outras comunidades para comunicações diárias pelo computador e correio eletrônico já estava sendo utilizado por muitas comunidades. Houve grande expansão de comunidades e o setor comercial começou a se interessar pela Internet.[21]

Em 1988 iniciou um processo de aumento de redes privadas e auto-financiadas para usos comerciais. Em setembro de 1988 foi realizado o primeiro Interop trade show, onde 50 empresas expuseram e 5000 engenheiros de corporações consideradas clientes participaram para ver se tudo funcionava como prometido e funcionou, pois os fabricantes trabalharam para assegurar que o produto de todos operariam com todos os outros, mesmo aqueles dos seus competidores. O Interop trade show foi crescendo e hoje é realizado em sete locais no mundo e freqüentado por todos que querem aprender sobre os últimos produtos lançados e discutir as mais recentes tecnologias.[22]

Em 1990, o backbone ARPANET foi desativado e em seu lugar foi criado o backbone DRI (Defense Research Internet). Em 1991-1992 a ANSNET passou a ser o principal

---

[18] Id., ibid, 8.

[19] Id., ibid, 7.

[20] Id., ibid, 17.

[21] Id., ibid, 7.

[22] Id., ibid, 7.

backbone da Internet e nesta época começou o desenvolvimento de um backbone europeu EBONE, interligando alguns países da Europa à Internet.[23]

Em 1990, o engenheiro inglês Tim Bernes-Lee desenvolveu a World Wide Web, possibilitando a utilização de uma interface gráfica e a criação de sites mais dinâmicos e visualmente interessantes. A partir desse momento, a Internet cresceu em ritmo acelerado começou a alcançar o público em geral. A WWW tornou a Internet acessível e interessante, popularizando-a.[24,25]

A partir de 1993 a Internet deixou de ser uma instituição de natureza apenas acadêmica e passou a ser explorada comercialmente, com abertura a nível mundial.[26]

A partir de 1995 havia mais de 6 milhões de computadores permanentemente conectados à Internet, além de muitos sistemas portáteis e de desktop que ficavam online por apenas alguns momentos.[27]

O rápido crescimento da Internet tem como ponto chave o livre e aberto acesso aos documentos básicos, especialmente as especificações dos protocolos. E outro fator importante para seu crescimento é a disponibilidade de novos serviços que ajudam os usuários a descobrir as informações que precisam.

A partir de 2006 começou a era das redes sociais. O primeiro, o Orkut ganhou a preferência dos brasileiros. Nos anos seguintes surgiram outras, como o Facebook e o Twitter.[28]

E os navegadores de Internet mais usados atualmente são: Internet Explorer, Firefox, Google Chrome.

No Brasil, a história da Internet começou em 1991, com a RNP (Rede Nacional de Pesquisa), uma operação acadêmica subordinada ao MCT (Ministério de Ciência e Tecnologia). Até hoje a RNP é o backbone principal e envolve instituições, centros de pesquisa, universidades, laboratórios etc.

---

[23] Id., ibid, 17.

[24] TEXTO PUBLICADO NA INTERNET. **História da Internet.** 02pg. 20/08/2011. Disponível em <hppt//WWW.suap esquisa.com/internet/acesso em 20/08/2011.>

[25] Id., ibid, 5.

[26] Id., ibid, 17.

[27] Id., ibid, 8.

[28] Id., ibid, 24.

Em 1995 foi possível a abertura ao setor privado para exploração comercial da população brasileira, por uma iniciativa do Ministérios das telecomunicações e do Ministério da Ciência e Tecnologia:[29]

> No início a internet foi disponibilizada apenas para pesquisas, para algumas universidades, as mesmas poderiam utilizar para fins apenas de pesquisas. A internet só começou a ser comercializada uns anos mais tarde, em meados de 1994 quando começou a ser vendida pela empresa de telecomunicação Embratel. Em 1995 o ministério das telecomunicações em conjunto com o Ministério da Ciência e Tecnologia, começaram atividades para disponibilizar acesso à internet para a população brasileira.
> Foi a partir deste momento que a internet no Brasil começou a ser utilizada também para a educação, como por exemplo, oferta de cursos virtuais, web conferências sobre temáticas educativas, seminários online, como outros que foram surgindo, como é o exemplo da educação a distancia. Com incentivo do governo várias instituições desenvolveram cursos de formação continuada, cursos de longa duração e até mesmo curso de ensino superior sugiram com o beneficio da utilização da internet.[30]

> O grande boom da rede aconteceu ao longo do ano de 1996. Um pouco pela melhoria nos serviços prestados pela Embratel, mas principalmente pelo crescimento natural do mercado, a Internet brasileira crescia vertiginosamente, tanto em número de usuários quanto de provedores e de serviços prestados através da rede. Uma das provas de que a Internet realmente havia decolado no Brasil veio no dia 14 de dezembro de 1996, quando Gilberto Gil fez o lançamento de sua música Pela Internet através da própria rede, cantando uma versão acústica da música ao vivo e conversando com internautas sobre sua relação com a Internet. [31]

> Em 1996 foram lançados grandes portais e provedores de conexão à rede no Brasil e, em 1998, o país já ocupava o 19º lugar em número de hosts no mundo e o liderava o pódio na América do Sul. No continente americano, ficava atrás apenas dos Estados Unidos e Canadá. Já estava consolidado o uso da internet no Brasil. Quase dez anos depois, em 2007, o Brasil movimentava cerca de 114 bilhões de dólares em comércio eletrônico e possuía uma base de 40 milhões de computadores instalados no país. De acordo com o Ibope/NetRatings, tínhamos cerca de 18 milhões de internautas residenciais. [32]

Atualmente a internet está em nosso dia a dia, está presente em quase tudo o que fazemos. A internet tornou-se a mais poderosa forma de comunicação e o mais popular entretenimento entre as pessoas de todas as idades em todo país. Além disso, o comércio eletrônico passou a ser uma exigência para as empresas inclusive de pequeno porte.

---

[29] Id., ibid, 8.

[30] http://www. portaleducacao.com.br /informática / artigos/53793/historia-da-internet-no-brasil)

[31] https://www.oficinadanet.com.br/artigo/904/o_comeco_da_internet_no_brasil

[32] http://www.tecmundo.com.br / internet/8949-20-anos-de-internet-no-brasil-aonde-chegamos-.htm

A internet, portanto, se tornou um meio hábil e eficaz de comunicação e informação, transformando, assim, o cotidiano do homem moderno. Mas esta modernização estendeu-se também sobre o Direito, em especial no campo do Direito Penal. No limiar dessa evolução tecnológica é possível constatar que, atualmente, o Código Penal tende a lidar com situações criminosas que vão além do plano físico. Hoje, o agente delituoso não necessita ir às ruas para cometer determinados ilícitos como furto, racismo, crimes contra a honra, dentre outros.

Destarte, se houve um desenvolvimento da internet para favorecer a rapidez de disseminação das informações, facilitar as negociações, aumentar as interrelações humanas, expandir as maneiras de educação etc., em contrapartida todas essas facilidades também ficaram em disposição das mentalidades voltadas ao crime e que se aproveitam desta ferramenta poderosa e camuflada para dissiparem o mal.

3 HISTÓRICO DOS CRIMES VIRTUAIS

O universo dos crimes informáticos teve seus os primeiros indícios no século XX, mais precisamente em 1960, onde se deram as primeiras referências sobre tais modalidades de crimes nas mais diversas denominações, com maiores incidências em casos de manipulação e sabotagem de sistemas de computadores.

Na década de 70 a figura do hacker já era citada com o advento de crimes como invasão de sistema e furto de software, mas foi em 1980 que houve maior propagação dos diferentes tipos de crimes como a pirataria, pedofilia, invasão de sistemas, propagação de vírus, surgindo então com isso a necessidade de se despender maiores preocupações com a segurança virtual que exige uma atenção especial para identificação e punição dos responsáveis, que a essa altura estão em todos os lugares do mundo como foi o caso da caça desesperada do governo americano atrás de Kevin Mitnick1, um dos hackers mais famosos e que hoje trabalha para o governo Americano na área da segurança da informação. [33]

O ano que marca o início da internet como conhecemos hoje é 1985. É neste ano que as comunidades já existentes com computadores começam a se intercomunicar e começam as pesquisas tecnológicas para sua melhoria.

Pode-se observar que os crimes da internet têm seus primeiros indícios em 1960, ainda nos primórdios da estruturação da internet. Onde há meio e oportunidade, há pessoas para aproveitá-los para o bem ou para o mal, principalmente onde há meio seguro, de fácil esquiva, e certeza de continuar impune o mal age tranqüilo.

Em 1993, após criação da WWW, a internet teve expansão comercial e começou a se espalhar. Em 1980, antes mesmo da propagação da internet, já havia propagação dos crimes. Isto demonstra o poder que tem as pessoas que querem usar a internet para o mal.

O Brasil começou a se preocupar com esse assunto especialmente a partir das últimas décadas, com o aumento da popularização dessa inovação tecnológica, promulgando, na Constituição Federal de 1988, regras relativas à competência do Estado sobre questões de informática.

Atualmente, no ramo jurídico, alguns doutrinadores se posicionam na busca da conceituação para essa nova modalidade de crimes como PINHEIRO (2006); O crime virtual é, em princípio, um crime de meio, ou seja, utiliza-se de um meio virtual.” Em estudo

[33] Monteiro, César Macedo . **Classificação dos crimes de informatica ainda sem nota de rodapé.** 68 pg. 03 de novembro de 2013. Disponível em: <hppt//http://www.slideshare.net/cmacedomonteiro/classificao-dos-crimes-de-informatica-ainda-sem-nota-de-rodap.>. Acessado em 10 de novembro de 2013. Pg 2-3.

introdutório de Manuel Lopes Rocha, este define a criminalidade informática, como: "Aqueles que tem por instrumento ou por objeto sistema de processamento eletrônico de dados, apresentando-se em múltiplas modalidades de execução e de lesão de bens jurídicos.[34]

No Brasil, a propagação da internet a nível comercial se deu a partir de 1995. Mas, antes da explosão da internet, as autoridades já se alertavam para estes crimes à luz do que já estava acontecendo nos outros países. Todavia, somente nos últimos anos é que os estudos do direito estão se intensificando nesta área, frente às necessidades existentes.

Atualmente ainda sem a tipificação adequada e com a facilidade de acesso a rede mundial de computadores os crimes tradicionais relacionados à informática, previstos em nossa legislação não são suficientes para classificar os crimes cometidos contra o computador ou por meio dele frente às novas modalidades criminosas que surgiram e que merecem ser definidos em lei especial, para garantia da ordem legal.

[34] Kevin D. Mitnick ; Simon, William L ; Wozniak, Steve , The Art Of Deception , Ed. John Wiley & Sons, ed 2009 (Crimes Da Informática – Remy Gama Filho Editora: Copymarket.Com, 2000).

4 DIREITO: UMA VISÃO GERAL

A vida em sociedade e as conseqüentes interrelações pessoais exigem a formulação de regras de conduta que disciplinem a interação entre as pessoas com o objetivo de alcançar o bem comum e a paz e a organização sociais. Tais regras, chamadas normas éticas ou de conduta, podem ser de natureza moral, religiosa e jurídica. O direito constitui, assim, um conjunto de normas de conduta estabelecidas para regular as relações sociais e garantidas pela intervenção do poder público.[35]

As leis existentes são, por si só, abrangentes aos crimes cibernéticos ou serão necessárias novas leis ou até mesmo um código específico para estes crimes? Esta é uma questão polêmica que gera muitas discussões.

Primeiramente, como são tratados a maioria destes crimes pelo direito, hoje?

De acordo com o Decreto-Lei n. 4.657, de 04 de setembro de 1942, Lei de introdução ao Código Civil Brasileiro: "Art. 4º - Quando a lei for omissa, o juiz decidirá o caso de acordo com a analogia, os costumes e os princípios gerais do direito."

O direito usa uma ferramenta muito abrangente da inteligência humana: a analogia. É através da analogia que muitas leis, já estruturadas na era pré-cibernética, se tornam úteis aos crimes da internet. Por analogia se atribui a um caso não regulamentado a mesma disciplina que a um caso regulamentado que seja semelhante. Assim se explica a tendência de cada ordenamento jurídico a expandir-se, além dos casos expressamente regulamentados.

O Direito também usa, para julgar e decidir processos ligados ao Direito digital, por exemplo, o costume: uma decisão baseada no que se costuma fazer em decisões anteriores, semelhante a que se vai julgar. Para isto, usa uma outra ferramenta, a similaridade: compara os casos e usa o que eles tem de semelhança para adequá-lo a uma nova realidade. Para tais decisões a jurisprudência também tem papel importante: decisões anteriores de outros juízes também são tomadas como referência para casos semelhantes ao que se pretende julgar e não há regulamentação específica.

---

[35] RODRIGUES, JC. **Introdução ao Direito Digital.** 27pg. Aula introdutória sobre Direito Digital do curso de Comunicação Digital para graduação em Propaganda e Marketing - ESPM São Paulo. 30/10/2010. Disponível em <http://www.slideshare.net/carlos_rds/introduo-ao-direito-digital>. Acessado em 15 de fevereiro de 2013. Pg5.

E, quando tudo isso não satisfaz ao caso em questão, são tomados como apoio a uma decisão, para qual ainda não há leis, os princípios gerais do direito. Estes são alicerces do ordenamento jurídico e não estão definidos em nenhuma norma legal: [36]

- Ninguém pode causar dano e quem causar terá que indenizar.
- Ninguém pode se beneficiar da própria torpeza.
- Ninguém pode ser punido por seus pensamentos.
- Ninguém é obrigado a citar os dispositivos legais nos quais ampara sua pretensão, pois se presume que o juiz os conheça.
- Ninguém está obrigado ao impossível.
- Não há crime sem lei anterior que o descreva.

São muitos os recursos que o Direito tem para julgar estes casos de crimes digitais. Por isso, para muitos, não são necessárias leis específicas para estes crimes. Está sendo lícito julgá-los desta maneira e menos oneroso para o Estado, menos trabalhoso para os juristas e advogados, menos complicado para quem elabora as leis e para quem vota nelas.

Quando os crimes que envolviam a internet ainda eram poucos ou raros, ou de danos menores, era oportuno e sábio que estes recursos do direito fossem usados. Em poucos anos, desde que a internet surgiu no Brasil (1995) até hoje (2016) – são apenas 21 anos-, a internet se tornou abrangente em todo Brasil, atingindo todas as camadas sociais, se tornou o principal meio de comunicação para todos: desde grandes empresas, propagandas, até o simples cidadão (é raridade alguém mandar uma carta, só se recebe emails e mensagens de redes sociais); a internet se tornou a principal e mais importante forma de comércio e negócios; é também o principal difusor de idéias, de pensamentos, de informações e de conhecimento. A internet, hoje, é fundamental em nossas vidas.

Em meio a este grande emaranhado de informações e situações, que antes eram vividas somente pessoalmente e hoje são vividas através da internet, surgem situações e particularidades que o direito existente fica, de certa forma, num imbróglio. A internet traz algumas particularidades que os crimes comuns não possuem.

Diante de todas as possibilidades do mundo cibernético, a forma como o Direito vem tratando estes crimes parece arcaica e arbitrária. O mundo, a forma e o meio de cometer os

[36]Id., ibid, 32. Pg6.

crimes e o significado dos crimes e até mesmo os crimes são outros após a globalização feita pela internet. A denotação, a importância e dimensão de um crime praticado no mundo e na era digital são singulares. Como podem ser tratados eternamente como semelhantes? A grande impunidade gera sentimentos de revolta e de encorajamento. Revolta daqueles que sofrem e encorajamento daqueles que querem fazer o dano.

A aplicação jurídica das leis também seguem um raciocínio que depende das seguintes orientações: Vigência: "quando aconteceu tal fato?"; Territorialidade: "onde aconteceu?" e Pessoas: "quem praticou tal fato?". Com relação a estas questões, o direito tradicional não consegue respondê-las quando se trata de crime pela internet.

Nesse sentido:

> Relevante ressaltar, todavia, que, ao passo em que o Direito Penal ganhou novos entornos criminológicos com a internet sendo utilizada como instrumento de práticas delituosas, muitas questões afligem a comunidade jurídica, que teve suas discussões alavancadas sobre o presente tema com a nova Lei 12. 737/2012.[37]

> Assim, aos fatos que já possuem tipificação legal e consequentemente, bem jurídico protegido pelo ordenamento, com a internet, ficaram vistos apenas como uma nova instrumentalização da modalidade delitiva. É o caso dos crimes cometidos contra à honra, fraude, furto e estelionato Por outro lado, novas condutas que violam os direitos e garantias da sociedade e que vão além dos bens jurídicos tutelados pelo Direito Penal como dano informático, violação ao dispositivo informático dentre outros que não possuem seus bens jurídicos abarcados em nossa legislação, pela falta de previsão legal, quando ocorria alguma ofensa a estes bens não havia como punir, na medida em que, como cediço, o Direito Penal não tipifica condutas por analogia em nome do princípio da legalidade, conforme disposto em nossa Carta Magna, em seu art. 5º, XXXIX "Não há pena sem lei anterior que o defina, nem pena sem prévia cominação legal.[38]

Antes da Lei 12. 737/2012, que deu ensejo a um novo tipo penal e algumas alterações no Código Penal, existiram diversos outros projetos de lei no cenário político brasileiro na tentativa de dirimir tais condutas.

Dentre estes, houve o Projeto de Lei n. 89/2003, que chegou a tramitar por mais de 10 anos no Congresso Nacional e teve sua redação final aprovada pelo Senado Federal somente nos idos de 2008, na forma de um substitutivo. Tal projeto, todavia, desencadeou intensos embates jurídicos sobre o seu conteúdo, inclusive, recebeu inúmeras críticas dos internautas

---

[37] http://jus.com.br/ artigos / 25120/a-evolucao-criminologica-do-direito-penal-aspectos-gerais-sobre-os-crimes-cibernetico s-e-a-lei-12-737-2012

[38] http://jus.com.br/artigos/25120/a-evolucao-criminologica-do-direito-penal-aspectos-gerais-sobre-os-crimes-ciberneticos-e-a-lei-12-737-2 012.

ativistas que, conforme apontou o jornal câmara vinculado a Câmara dos Deputados, chegou a circular uma petição contrária a aprovação deste projeto com mais de 165 mil assinaturas.

Em razão disto, o projeto ficou conhecido como "AI-5 Digital", uma vez que suprimia a liberdade de expressão dos internautas e porventura enquadraria na tipificação penal um simples download. Sendo assim, em 2011 foi aprovado pela Câmara dos Deputados outro projeto, a saber, o Projeto de Lei n. 2793/2011 que, frisa-se, teve seu nascimento justamente para combater o Projeto de Lei n 89/2003 considerado, então, defasado e prolixo.

Em verdade, os autores deste projeto acreditavam que ele seria mais proveitoso para a sociedade, haja vista que continha poucas disposições legais sobres os cibercrimes ao ser comparado com o já mencionado Projeto de Lei n. 89/2003. Os autores do PL 2793/2011 argumentavam que boa parte dos delitos já praticados com o auxílio ou não da rede mundial de computadores já implicam numa repressão estatal prevista no ordenamento jurídico. Daí, a iniciativa em criar somente delitos que violavam certo bem jurídico ainda não amparado na legislação penal.

A problemática que circundava os projetos de lei, todavia, só teve fim com o episódio envolvendo a atriz global Carolina Dieckmann. Esta foi vítima de rakers que, em razão de seu computador estar vulnerável, ou seja, sem um sistema de segurança ativo contra vírus e spams, obtiveram a senha do seu e-mail e, por consequência, diversas fotos da atriz seminua e em posições em que expunha sua intimidade. Tais fotos foram disseminadas além dos delinquentes e foram parar, inclusive, em sites pornográficos.

A partir deste acontecimento as autoridades legislativas se mobilizaram e nasceu, assim, a Lei 12. 720/2012. Esta lei, ao contrário dos anteriores projetos de lei, traz poucas alterações ao Código Penal, senão vejamos:

> o único dispositivo criado que tipifica determinada conduta como crime é o art. 154-A que trata da "invasão de dispositivo informático". Entende que pratica-se esse crime, o agente que comete a seguinte conduta: "Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita".
> Por fim a presente lei alterou a redação dos arts. 266 e 298 do Código Penal para adequá-los a realidade cibernética. O art. 266 teve a sua titulação alterada para inserir a interrupção quanto aos serviços informáticos. Agora tal dispositivo trata do seguinte delito **"**Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública"**.** Quanto ao art. 298, em seu parágrafo único, o legislador equiparou como documento particular os cartões de crédito e débito no delito de falsificação de documento. Percebe-se que em razão do fato ocorrido com a atriz global ter ganhado repercussões midiáticas, a lei em comento foi criada na pressa, sem ao menos possibilitar a responsabilidade penal de provedores e dispor de outras condutas que possivelmente possam violar

> bens considerados relevantes para o homem moderno, como dano informático, o acesso não autorizado e a obtenção ilegal de dados/engenharia social."[39]

O problema da prevenção dos crimes pela Internet no Brasil é antes de mais nada o problema da repressão, ou seja, da efetiva aplicação da lei penal já existente às novas circunstâncias que se apresentam.

De nada vale criarmos leis para reprimirmos os novos crimes se elas não puderem ser aplicadas por falta de treinamento de policiais, de promotores de justiça e de magistrados. O melhor meio de se prevenir um crime é indubitavelmente o exemplo dado pela efetiva e correta aplicação da norma repressiva.

Há uma visível deficiência no Brasil de pessoal capacitado, com conhecimentos cibernéticos para investigar e combater este tipo de crime. O que retrata isso é o número ínfimo de delegacias especializadas, sendo apenas 16 em todo Brasil. Como isso, se o crime cibernético pode ocorrer a qualquer momento e em qualquer lugar? Alguns crimes digitais para a uma persecução eficiente, requerem especialização técnica nas investigações para facilitar a identificação do agente delituoso (virtual) e uma compreensão maior de como o crime acontece e consequente processamento.

Outra dificuldade que envolve os crimes cibernéticos é estipular a competência, a qual foro será julgado tal crime. Para definir o foro competente se faz necessário perceber qual circunstância e foro o crime foi concebido.

Segundo Celson Valin *apud* Aras, a problemática em torno da territorialidade da internet "reside no caráter internacional da rede. Na Internet não existem fronteiras e, portanto, algo que nela esteja publicado estará em todo o mundo. Como, então, determinar o juízo competente para analisar um caso referente a um crime ocorrido na rede?" Em regra, de acordo com a nossa atual jurisdição processual penal, nos moldes do art. 70 do Código de Processo Penal, a competência é definida pelo lugar em que a infração for consumada, ou, no caso de tentativa, pelo local em que foi praticado o último ato de execução.

Diante o exposto há de se constatar a primeira problemática, pois nos crimes cometidos na internet, o grau de dificuldade encontrado pelas autoridades policiais é imensurável na identificação do local em que se deu o crime. Isto porque, o agente delituoso geralmente não utiliza seu próprio computador para cometer as mais diversas infrações e sim, de lanhouses, bibliotecas em universidades, shoppings, ou seja, lugares públicos.

---

[39] http://jus.com.br/artigos/25120/a-evolucao-criminologica-do-direito-penal-aspectos-gerais-sobre-os-crimes-cibernetico s-e-a-lei-12-737-2012

Ainda assim, no processo investigatório é perceptível a utilização de dados e e-mails falsos e até mesmo a proliferação de vírus a fim de mascarar as condutas delitivas.

Neste sentido, a jurisprudência dos Tribunais Superiores já vem consolidando, em alguns julgados, determinadas diretrizes processuais no âmbito cibernético. A este tema, o Superior Tribunal de Justiça entendeu que a competência para processual e julgar crimes de racismo praticado na internet é o do local onde partiram as mensagens de cunho ofensivo racista.

Para julgar os crimes cibernéticos contra a Administração Pública, a exemplo do art. 313-A do Código Penal (inserção de dados falsos em sistema de informação), competente é a Justiça Federal. Também determinou a estes juízes federais o julgamento de crimes previstos em tratados ou convenção internacional, quando a infração for iniciada no País, o resultado tenha ou devesse ter ocorrido no estrangeiro, ou reciprocamente, conforme art. 109, inciso V da Constituição Federal.

Desta forma, crimes de racismo e pedofilia, por exemplo, que estão previstos em convenções internacionais, ficariam sujeitos a julgamento dos juízes federais em caso destes crimes serem cometidos no âmbito da internet e que os atos de execução do crime ou até a sua consumação fosse além das fronteiras nacionais.

5 CRIMES DE INTERNET

5.1 Conceitos e classificações

Primeiramente, é importante definir crime. A lei de introdução ao Código Penal esclarece:

> Art. 1.º Considera-se crime a infração penal que comina pena de reclusão ou de detenção quer isoladamente quer alternativa ou cumulativamente com a pena de multa; contravenção; a infração penal que a lei comina, isoladamente, pena de prisão simples ou de multa, ou ambas alternativas ou cumulativamente.

Com os avanços tecnológicos da informática, surgiram os denominados crimes cibernéticos. Porém, não existe uma nomenclatura uniformizada para os crimes dessa natureza, por isso esses crimes são denominados também de crimes de informática, crimes informáticos, crimes tecnológicos, crimes virtuais, delitos computacionais, crimes digitais, crimes virtuais, crimes cometido por meio eletrônico, entre outros.

E qual a definição de crime virtual? Com a chegada da Lei 12737/2012, passou a ser entendido o crime virtual como sendo qualquer ação em que o computador seja o instrumento ou parte do objeto do delito, ou então, qualquer crime ligado ao tratamento de dados.

Crime de informática pode ser definido, como qualquer ato ilegal onde o conhecimento especial de tecnologia de informática faz com que o sujeito da ação infratora tenha êxito na sua conduta. Ou, mais precisamente, crimes de informática são as condutas descritas em tipos penais realizadas através de computadores ou voltadas contra computadores, sistemas de informática ou os dados e as informações neles utilizados (armazenamento ou processamento). Em determinadas vezes o crime de informática, assemelha-se muito ao crime comum, ou definição de crime, tendo somente a diferença que o objeto utilizado para o êxito foi um computador ou algum sistema informatizado.[40]

Os crimes ligados à informática podem ser classificados em dois grandes grupos: puro (também chamado próprio) e impuro (também chamado impróprio).

Puro é o crime de informática que ao se utilizar um computador, visa pura e somente o ataque a qualquer outro computador ou sistema de informática. O sujeito ativo visa especificamente ao sistema de informática, em todas as suas formas. Neles, a informática

[40] Id., ibid, 30. Pg5.

(segurança dos sistemas, titularidade das informações e integridade dos dados, da máquina e periféricos) é o objeto jurídico tutelado.

Impuros são aqueles realizados com a utilização do computador, ou seja, por meio da máquina, para realização de condutas ilícitas que atinge todo o bem jurídico já tutelado. Crimes, portanto, já tipificados que são realizados, agora, com a utilização do computador e da rede. O agente se vale do computador como meio para produzir resultado que ofenda o mundo físico ou o espaço "real", ameaçando ou lesando outros bens, não-computacionais ou diversos da informática".

Constatar um crime digital e classificá-lo não é uma tarefa fácil, tendo em vista que ainda existem poucas conclusões a respeito, pois a tecnologia evolui a passos largos e, ano após ano, a opinião dos doutrinadores também muda conforme segue a evolução tecnológica. Existem condutas que utilizam os computadores como meio para o cometimento dos delitos, e há casos em que sem o uso do sistema informático não seria possível a consumação de determinados crimes.

Um conceito de classificação foi feita por um doutrinador estrangeiro Rovira Del Canto, o qual subdividiu os delitos em infrações à intimidade; ilícitos econômicos; ilícitos de comunicação pela emissão ou difusão de conteúdos ilegais ou perigosos; e, outros atos ilícitos. [41]

Há uma outra classificação, elaborada pelo Dr. Vladimir Aras (Procurador da República (Federal Prosecutor), Mestre em Direito - UFPE, Professor de Processo Penal - UFBA e editor do Blog do Vlad.Via Láctea · blogdovladimir.com), que divide os crimes da informática em três categorias: 1. Uma primeira, onde o computador constitui a necessária ferramenta de realização pela qual o agente alcança o resultado legal; 2. A segunda categoria de crimes do computador, poderia incluir todos aqueles comportamentos ilegítimos que atingem os computadores, ou mais precisamente, seus programas; 3. A última categoria deveria juntar todas as possíveis violações da reserva sobre a máquina. Aqui entram em consideração as habilidades de colheita e elaboração de todo tipo de dados. [42; 43]

---

[41] Id., ibid, 30. Pg10-11.

[42] Id., ibid, 30. Pg10-11.

[43] ARAS, Vladimir. Informações contidas em seu twiteer. https://twitter.com/VladimirAras. Acessado em 12 de novembro de 2013. 01pg.

Em todas as classificações há distinções a considerar e pontos em comum, algumas posições atribuem os meios eletrônicos como objeto protegido (bem jurídico) e meios eletrônicos como meio/instrumento de se lesionar outros bens.

A classificação destes crimes em puros ou impuros torna-se umas das mais oportunas, pois abrange se não todos, pelo menos a maior parte destes crimes.

5.2 Características dos crimes cibernéticos

Os crimes cibernéticos apresentam características que lhes proporcionam uma especificidade com relação aos crimes comuns. A seguir serão apresentadas algumas de suas características particulares mais importantes.

- Celeridade: os crimes cibernéticos são rápidos. Em questão de minutos podem ser enviados milhões de vírus que podem danificar sistemas, copiar dados, invadir informações confidenciais. É com muita rapidez que uma injúria ou calúnia pode se propagar e causar sérios danos morais. É também com muita rapidez que fotos de pedofilia são propagadas por todo planeta.
- Dinamismo: os crimes cibernéticos podem ser cometidos das mais variadas formas e estas formas mudam muito facilmente devido a alta tecnologia que é desenvolvida a cada momento. Por exemplo, pode-se mandar um determinado vírus e quando são criadas maneiras de se proteger contra aquele vírus, prontamente é criado um novo vírus. As mais variadas formas de se conectar à internet e os mais variados aparelhos que podem ser usados proporcionam, a cada momento, um novo arsenal que poderá ser usado.
- Poucas leis tipificando-os diretamente. Com a era digital e tantos recursos que os criminosos podem usar, a falta de leis tipificando-os diretamente abre brechas para a impunidade de muitos, se não da maioria, dos crimes virtuais.
- Transgressor aos limites de Vigência, Territorialidade e Pessoa. Vigência: quando aconteceu o ato delituoso? Territorialidade: onde ocorreu? Pessoa: quem é o responsável? A transgressão desses limites pode ser demonstrada através de um exemplo: 28/abril 02:45h – Buenos Aires (Argentina): Cracker brasileiro, em território argentino, dispara um cavalo de tróia para ‘escravizar’ computadores da Universidade de Berlim. 05/maio 22:05h – Houston (EUA): devido ao ataque, servidores deixam de funcionar e perdem dados de compra de 10 clientes. 06/maio 09:17h – Moscou

(Rússia): cliente, que efetuou uma compra na Amazon, percebe que seu pedido sumiu.[44]

- Falta de regulamentação para a guarda apropriada de provas. Por exemplo: o armazenamento dos dados de acessos de clientes seria de suma importância para uma maior efetividade nas ações policiais investigativas, e na produção de provas contra os acusados. Por outro lado, os provedores nacionais e internacionais alegam que seria muito oneroso o armazenamento permanente desses dados, tornando, assim, extremamente necessário uma legislação que estabeleça um período obrigatório para que os provedores mantenham armazenados esses dados facilitando assim o trabalho investigativo, já que atualmente esses dados ficam armazenados em média por apenas três meses, o que é muito pouco tempo ante ao vagaroso andamento dos procedimentos judiciais. [45] O uso da perícia forense eletrônica consiste no emprego de conhecimentos sobre computação e telecomunicações, por meio de métodos científicos e lógicos, para responder a questionamentos jurídicos. Para o sucesso da perícia eletrônica podemos citar principalmente o uso de métodos de identificação e rastreamento, a comprovação material, a técnica de detecção de intrusos e a recuperação de informações digitais. Além disso, na maioria das vezes, a perícia forense eletrônica irá lidar com documentos eletrônicos, fotografias digitais, locais de armazenamento de dados, como pen-drives e outras mídias digitais. Por isso, devido ao avanço da tecnologia e da própria sociedade como um todo, o conceito de documento necessita ser alargado. [46]
- Dificuldade de identificação de quem comete o crime. Para acessar a internet não há necessidade de identificação e o acesso, muitas das vezes pode ser feito usando internet de outra pessoa e usando os mais diversos aparelhos.

---

[44] Id., ibid, 32. Pg11.

[45] GATTO,Victor Henrique Gouveia. **Tipicidade penal dos crimes cometidos na internet.** Publicado em 01/08/2011 | Nº 91 - Ano XIV - AGOSTO/201. Disponível em: <http://www.ambitojuridico.com.br /site/?n_link=revista_artigos_leitura&artigo_id=9962&revista_caderno=17>. Acessado em 09 de julho de 2012.

[46] FREIRE, Antonio Carlos Pantoja. **Os desafios da perícia eletrônica forense como meio de prova no processo civil.** Publicado em 01/08/2011 | Nº 91 - Ano XIV - AGOSTO/2011. Disponível em: < http://www.ambito-juridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id =9966&revista_caderno=17 >. Acessado em 17 de julho de 2012.

Todas essas características já conferem ao direito digital particularidades que, em muitos casos fica difícil ou até impossível punir um ato digital delituoso apenas por analogia ou pelos princípios básicos do direito e jurisprudência.

5.3 O agente ativo e passivo no crime virtual

A definição do agente ativo ou como também é conhecido, o sujeito ativo, é aquele que pratica a conduta descrita na lei, ou seja, o fato típico. Só o homem, isoladamente ou associado a outros (coautoria ou participação), pode ser sujeito ativo do crime.

A capacidade geral para praticar crime existe em todos os homens, é toda pessoa natural independente da sua idade ou de seu estado psíquico, portanto também os doentes mentais. Quando se trata de crimes realizados na internet ou com auxilio dela, logo vem em nossa mente que são realizados por "experts", os chamados Crackers, porém com a popularização desse meio surgiram milhares de casos, produzido por pessoas com mínimo de conhecimento tecnológico.

Importante se faz ressaltar a diferenciação entre Hacker e Cracker, apesar da grande maioria das pessoas acreditarem que o hacker é o criminoso da informática. Essa afirmação não pode ser considerada verdadeira.

A nomenclatura Hacker é usada para definir o "individuo com amplo conhecimento em informática, que faz uso desse conhecimento para encontrar falhas e medidas de correção para essas falhas" o hacker geralmente trabalha no desenvolvimento de tecnologias de segurança, desenvolvendo antivírus, sistemas de bloqueio a acesso de dados não permitidos dentre outras funções, enquanto o Cracker é o criminoso do mundo virtual; "os Crackers também possuem um conhecimento avançado em informática, porem as suas atitudes são diferentes, os Crackers usam o seu conhecimento apenas para beneficio próprio ou destruição"[47]

Os Hackers podem ser considerados como pessoas de grande conhecimento informático que o utilizam para praticas lícitas enquanto os Crackers podem ser entendidos como os verdadeiros criminosos da internet.

Sujeito passivo do crime é o titular do bem lesado ou ameaçado pela conduta criminosa. Nada impede que em um delito dois ou mais sujeitos passivos existam desde que

[47] Id., ibid, 39.

tenham sido lesados ou ameaçados a seus bens jurídicos referidos no tipo. São vitimas de crime. Nos crimes de informática, poderá ser qualquer pessoa que utilize ou não do meio eletrônico, podendo haver mais de um individuo.

É muito importante ressaltar, portanto, a necessidade de proteção, não só ao simples usuário doméstico, mas também as empresas que muitas vezes ao se deparar com a clara impunidade imposta, tem em muitos casos a necessidade de se investir muito em segurança de rede, já que em muitas das vezes as empresas invadidas pelas ações desses Crackers, tem de contratá-los para fazer a segurança de sua rede já que este descobriu uma maneira de violá-la.

Atualmente qualquer pessoa pode figurar como agente ativo de um crime virtual. Existem centenas de fóruns nos quais se ensinam detalhadamente como agir para usurpar senhas de mensageiros instantâneos como Windows Live Messenger, ou mesmo envio de vírus, ou de conteúdo impróprio como nos casos de pornografia infantil. É comum se deparar com esse tipo de conteúdo, por vezes, mesmo que não se tenha a intenção de obter, como no caso que o envio dessas imagens é recebido via email.

Com essa facilidade na busca de informações e com a sensação cada vez mais clara de total anonimato, pessoas comuns cometem atos ilícitos seja para denegrir a imagem de algum desafeto, seja para fazer uma brincadeira com algum amigo.

A sensação de anonimato e de impunidade traz também para o mundo virtual, criminosos com baixo conhecimento informático, que conseguem, através do uso da internet, realizar negócios escusos, utilizando desse meio para aliciamento de menores para o trafico ou para o comércio sexual, causando total sensação de insegurança e desvirtuando a finalidade desse meio de comunicação imprescindível.

Além dessa grande dificuldade em se encontrar e definir com clareza o verdadeiro autor do crime, quando se tem a possibilidade fática de auferir essa localização, o aplicador do direito esbarra em outra grande dificuldade: a falta de enquadramento penal, já que o magistrado, na grande maioria das vezes, não encontra um tipo penal especifico para o crime realizado.

Torna-se importante a discussão sobre a responsabilidade dos provedores. O provedor é classificado como pessoa jurídica de direito privado com direitos e deveres inerentes a esta condição. Considera-se o provedor de acesso à Internet um serviço de valor adicionado, portanto, este não se caracteriza como serviço de telecomunicações.

A distinção legal entre serviço de valor adicionado e serviço de telecomunicações é que aquele afasta a incidência do sigilo constitucional, previsto no artigo 5º da Constituição Federal em seu inciso XII, que se refere à comunicação de dados feita por serviço de

telecomunicações. O produto mais comercializável e mais imediato relacionado com a Internet é o acesso a ela. A responsabilidade ou a corresponsabilidade dos provedores é assunto discutido em alguns países, sendo assunto também controverso. Uma posição que está se tornando a tendência sobre a responsabilidade penal dos provedores é a da responsabilidade limitada, onde, p.ex., sendo de conhecimento do provedor, conteúdo ilegal, seria de se esperar que este não divulgasse tal conteúdo ou o bloqueasse (tendo meios técnicos para isto). Não o fazendo, assumiria a corresponsabilidade pelo fato.

É o que propõe a Lei alemã que responsabiliza os provedores por divulgação de material ilegal, quando estes forem avisados oficialmente do conteúdo questionável e não tomarem providências para bloquear o acesso às informações ilegais. Os provedores da Internet têm um argumento muito sólido e realista, afirmando que o volume de dados dentro da Internet, como dentro das listas de discussões, é tão grande que o processo de checar e verificar a decência dos mesmos é humanamente impossível. A Comissão Federal de Comércio dos Estados Unidos (FTC) irá criar um laboratório dedicado à Internet 24 horas por dia, monitorando anúncios on-line para identificar fraudes. Com isso, a FTC espera inibir os golpes via Web e acionar o FBI se algum crime for caracterizado.

Atualmente existem cerca de 170 mil reclamações no banco de dados da FTC. A instituição já detectou 80 fraudes na Internet, envolvendo pirâmides da fortuna e compra de mercadorias pela rede que nunca foram entregues. Hoje temos programas para controle de acesso a páginas eróticas, p.ex., tornando-as inacessíveis a crianças e adolescentes.

Desta forma transfere-se a responsabilidade pelo acesso, aos pais. Mas quanto a divulgação de outros conteúdos ilegais, de negócios fraudulentos, sites que ensinam a produzir bombas, a conduzir campanhas terroristas e racistas? “O ciberespaço não é uma zona sem lei. Ninguém pode pensar que tecnologias especiais têm o poder de colocar as pessoas fora do alcance da lei”, palavras do Ministro da Educação e Pesquisa da Alemanha, Juergem Ruettgers, em 1996.

O que se discute não é a imputação de conduta delituosa a empresa provedora de Internet, mas sim a sua responsabilidade pela divulgação do material considerado ilegal ou ofensivo, desde que conhecedora do fato. Os Estados Unidos é um grande defensor da privacidade e da liberdade de expressão, tendo como filosofia no que diz respeito à Internet, de que esta por ser o maior veículo de expressão já desenvolvido até o momento, merece a maior proteção possível contra a intromissão governamental. No Japão, o parlamento aprovou em agosto deste ano uma lei polêmica que dá direito aos policiais de interceptarem e-mails e chamadas telefônicas. O governo insiste que a medida só será utilizada com o objetivo de

combater o crime organizado. Mas os japoneses temem que ela seja usada para quebra de privacidade, já que os criminosos usam criptografia forte, fora do alcance do governo.

Na Europa o Conselho da União Européia aprovou em dezembro de 1998 um plano de ação descrevendo iniciativas para promover o uso mais seguro da Internet, chamando em particular à colaboração dos profissionais da rede. O plano articula quatro ações principais: - criar um ambiente eletrônico mais seguro. De um lado o surgimento de "disque denúncias", onde os usuários poderiam denunciar conteúdos que julgassem ilegais, como já acontece na Inglaterra e França. Por outro lado, seriam convidados os provedores de acesso e serviços para desenvolverem um código de conduta com direito a selo de qualidade aos que aderissem ao referido código: - desenvolver e unificar os sistemas de segurança e filtrar as informações da rede.

Este efeito é previsto para encorajar a cooperação internacional, de forma que os sistemas futuros possam ser unificados; - fortalecer ações de sensibilização e informação ao público, em particular aos pais e profissionais da educação, sobre os perigos potenciais do uso da Internet; e discutir a cooperação européia e mundial sobre questões legais, como lei aplicável, liberdade de expressão, etc.

Tal iniciativa se dá no momento, como prioridade a auto regulação da rede, que é o modo provável mais eficiente de conter a propagação de conteúdo ilegal e prejudicial. Certos países regulam a Internet de maneira restritiva.

Vejamos alguns exemplos: CHINA - a pouco a China Continental eliminou para os seus cidadãos o acesso a mais de cem sites da Internet. Na China, as pessoas com acesso à Internet têm de apresentar-se as autoridades para a inscrição num registro especial. Além disso, todos os servidores Internet devem passar pelo Ministério de Telecomunicações. ALEMANHA - A Alemanha procurou controlar o acesso, proibindo-o, ao site da Organização Neonazista Zundel. Os americanos, defensores sempre da liberdade de expressão, copiaram o site Zundel nos computadores de universidades como a MIT, Stanford e Carnegie Mellon, sites que as autoridades alemãs não quiseram eliminar. Tudo isso deu publicidade ao site Zundel, resultado contrário ao esperado. ESTADOS UNIDOS - Com a Lei da Decência nas Comunicações (CDA) procurou a legislação dos Estados Unidos proibir entre outros atos a utilização de um serviço interativo de computadores para difundir, de maneira a fazê-la disponível a pessoas menores de 18 anos, matéria sexualmente explícita que segundo os princípios contemporâneos da ética da comunidade são claramente ofensivas. Na medida em que esta lei proíbe a transmissão de matéria indecente a pessoas menores, foi declarada inconstitucional pela Corte Federal do Estado da Pennsylvania. O Ministério Público apelou à

Corte Suprema. CINGAPURA - Este país publicou uma regulamentação limitando o acesso a sua população. ARABIA SAUDITA - Este país também censura parte da informação disponível na Internet. FRANÇA - O Conselho Constitucional declarou inconstitucional a Emenda "Fillon" à Lei Francesa de Telecomunicações, afirmando que regulamentação da Internet ficou deficiente por falta de precisão. Tratava-se de competência que se desejava atribuir ao Conselho do Audiovisual de propor princípios e diretrizes para a Internet. Também reconhece jurisprudência francesa que os provedores de acesso a Internet não são responsáveis pelo conteúdo da matéria publicada nos seus servidores.[48]

Como se pode verificar ainda é muito controversa a questão sobre a responsabilidade dos provedores. Poderia serem corresponsabilizados pelos fatos delituosos? Necessitaria, primeiramente, de terem condições de monitorarem cada informação que fosse passada. Mas mesmo assim ainda haveriam muitas questões a discutir, como por exemplo: quais informações poderiam ser barradas sem ofender o direito à expressão? Quem decidiria sobre essas questões?

5.4 Crimes de internet e a dificuldade de identificação do sujeito ativo

Os crimes virtuais podem ter definições puramente virtuais, mas seus efeitos são facilmente percebidos ao chamado mundo real, atualmente não se pode separar essas duas definições, pois os crimes virtuais têm grande reflexo no cotidiano da sociedade.

O que era anteriormente considerado um mundo surreal fantasioso, a internet se tornou fonte indispensável de pesquisa, ferramenta essencial de trabalho de uma grande massa de trabalhadores, várias empresas a utilizam como único meio de comunicação e transmissão de dados entre suas filiais, programas integrados de segurança, transporte, logística operacional dentre outras inúmeras funções.

Com o rápido impulso da informatização e com o aumento cada vez maior das redes sócias e de compartilhamento de arquivos e vídeos, expor sua vida social divulgar suas idéias, demonstrar seus trabalhos e se comunicar com o mundo ficou muito mais rápido e fácil através da internet.

Com a criação de páginas de relacionamentos como "orkut, twitter, facebook" dentre outros muitos, atraiu para internet o público jovem e infantil, aumentando assim o interesse de

[48] Id., ibid, 30. Pg41-44.

pedófilos, que sem controle algum se fazem passar por crianças, ganhando assim, a confiança destas para que então possam executar seus crimes.

Dentro desse contexto, surgiram vários outros crimes, muitos deles novos, os chamados crimes puramente informáticos, alguns já existentes em nosso meio, mas que aumentaram consideravelmente com o uso da internet, crimes como pirataria virtual de músicas, vídeos ou obras de autoria bibliográfica, que podem ser facilmente encontradas sem que haja nenhum pudor por parte dos falsificadores em esconder sua identidade.

A usurpação de senhas de comercio eletrônico e divulgação de imagens privadas muitas delas envolvendo crianças e adolescentes são um dos principais crimes cometidos na internet segundo dados do site safernet.org. br, que denuncia esses tipos de crimes.

Os criminosos na maioria das vezes se utilizam da inocência dos usuários para proliferar mensagens, coletando informações privilegiadas, ou mesmo, apenas com fulcro de causar dano que em grande parte das vezes vem acompanhado de um grande prejuízo para vitima.

No caso concreto, fica difícil mensurar os prejuízos de uma empresa que se utiliza de um sistema de redes integrado, como uma empresa de telefonia que tem seu sinal diretamente ligado a redes de internet ou mesmo uma transportadora que monitora seus caminhões, buscando os melhores trajetos para uma melhor logística, pode ser sensivelmente afetada no caso de um ataque ao seu sistema, abrindo um terrível precedente para uma disputa de mercado desleal entre empresas do mesmo ramo que podem se utilizar dessa alternativa, que reafirmo ainda não é considerado fato típico, portanto é um ato licito, para se sobrepor a sua concorrente.

A facilidade de se enviar e receber vírus pela internet são tão grandes que muitas vezes mesmo sem perceber a própria vitima de um ataque de cracker, acaba enviando via email ou mensagens instantâneas despercebidamente os mesmos vírus recebidos anteriormente. Além da questão cada dia mais crescente da pirataria que acaba tornando mesmo pessoas idôneas criminosas ao adquirir sem o devido respeito à propriedade intelectual, obras como livros, coletâneas musicais, filmes dentre outros.

Como não há a necessidade de nenhuma forma de identificação ou qualquer tipo de controle no acesso a internet, qualquer cidadão pode deliberadamente acessá-la usando pseudônimos muitas vezes taxativos sobre suas intenções.

Esse fato acaba evidenciando uma das maiores falhas que é a falta de identificação de usuários da internet pelo seu RG ou CPF, os usuários se conectam na internet por uma tecnologia conhecida como Tcp/ip (*transmission control protocol – internet protocol),* assim

conceituado Comer Douglas, renomado conhecedor do sistema de segurança e rede de computadores: o software Tcp/ip normalmente reside no sistema operacional, onde pode ser compartilhado por todos os programas e aplicativos executados na máquina, ou seja, o sistema operacional contem uma só cópia do código de um protocolo como o Tcp/ip e outros vários programas podem chamar esse código. [49]

É através desse protocolo que é único para cada acesso a internet, que se pode detectar de onde o usuário esta acessando, podendo precisar com exatidão a localidade em que foi realizado, insta salientar, porém, que com a tecnologia de redes sem fio podendo ser facilmente encontrada em instituições de ensino, hotéis e até mesmo sendo fornecida por municípios, como é o caso da orla de Ipanema no Rio de Janeiro ficou praticamente impossível detectar e punir um usuário em especifico já que varias pessoas se utilizam dessa mesma rede, para o acesso a internet ou mesmo para transmissão de dados pessoais pela rede.

Sendo assim o criminoso se conecta de qualquer desses lugares sem a devida necessidade de identificação, podendo em alguns minutos proliferar milhares de vírus, ou como é comum milhões de vírus em apenas minutos, além de acessar dados pessoais de outros computadores invadindo a intimidade das pessoas, e em muitos casos subtraindo dados desse computador para posterior envio na internet de dados como CPF, RG e informações em geral, de acordo com a vulnerabilidade e a quantidade de dados enviados pela vitima, podendo ferir o principio da intimidade de tal forma a expor fotos e vídeos da intimidade de outros usuários, na grande maioria das vezes sem a intenção de criar prejuízos financeiros, mas sim com intuito de causar dano a vitima seja ele moral ou material.

Assim, o indivíduo que quer praticar o mal passa a usar indiscriminadamente esse meio, pois sabe que ao remover o cabo do seu computador, desconectando-se da internet esse individuo que há poucas horas praticou vários crimes, não pode ser mais identificado, pois ao conectar novamente ao computador, será criado um novo protocolo Tcp/Ip, podendo assim voltar a cometer condutas ilícitas, muitas vezes até da mesma localidade onde começou a praticar os anteriores.

[49] Id., ibid, 39.

6 CRIMES CIBERNÉTICOS E O DIREITO

O espaço virtual, que se mostra tão propício para a prática dos mais variados crimes, apesar da falta de legislação específica, é relativamente protegido juridicamente, pois se encontram no ordenamento jurídico brasileiro algumas normas que tratam da matéria, como por exemplo: a Lei nº 11.829/08, que combate a pornografia infantil na internet; a Lei nº 9.609/98, que trata da proteção da propriedade intelectual do programa de computador; a Lei nº 9.983/00, que tipificou os crimes relacionados ao acesso indevido a sistemas informatizados da Administração Pública; a Lei nº 9.296/96 disciplinou a interceptação de comunicação telemática ou informática; e a Lei nº 12.034/09, que delimita os direitos e deveres dentro da rede mundial, durante as campanhas eleitorais. [50]

Além disso, os aplicadores do direito têm feito incidir a legislação já existente, como o Código Penal, aos crimes cometidos no meio virtual. Exemplos de crimes cibernéticos já tipificados na legislação penal que são cometidos através de computadores e outros meios tecnológicos são, entre outros, o crime de calúnia, ameaça, difamação, apologia a crime ou criminoso, injúria, constrangimento ilegal, falsa identidade.

A aplicação da legislação já existente, como do Código Penal, para enquadrar os crimes cibernéticos ocorre porque os operadores do direito entenderam que, em alguns casos, a conduta praticada é aquela já tipificada pelas nossas leis, e o que muda é o meio, o instrumento utilizado na conduta criminosa: a informática, o computador. Pois, no Direito Penal, não se aplica por analogia as normas incriminadoras, que são aquelas que estabelecem a conduta ilícita e atribuem a sua respectiva sanção. Isso ocorre porque, como essas normas "sempre restringem a liberdade do indivíduo, é inadmissível que o juiz acrescente outras limitações além daquelas previstas pelo legislador. Em matéria penal, somente é admissível a analogia quando beneficia a defesa.

Diante dos avanços tecnológicos, do uso rotineiro da internet e dos meios eletrônicos no cotidiano das pessoas e, conseqüentemente, da propagação de crimes relacionados a esse cenário, o Brasil se mostra atrasado por ainda não possuir uma legislação específica para

---

[50] MENDES, Maria Eugenia Gonçalves; VIEIRA, Natália Borges. **Os crimes cibernéticos no ordenamento jurídico brasileiro e a necessidade de legislação específica.** Disponível em: < http://www.gcpadvogados.com.br/artigos/os-crimes-ciberneticos-no-ordenamento-juridico-brasileiro-e-a-necessidade-de-legislacao-especifica-2 >. Acessado em 15 de agosto de 2012.

disciplinar os crimes cibernéticos. “Vários países já apresentam legislação específica que tratam dos crimes cibernéticos, como Estados Unidos, Portugal, Inglaterra, entre outros.”[51]

Com a entrada em vigor das leis 12.735 e 12.737, ambas de 2012, tem-se a aplicação penal de normas específicas sobre os crimes digitais próprios, aqueles cometidos contra dados, informações ou sistemas de informação.

Agora o usuário deve ter mais cuidado em proteger suas informações e ferramentas, bem como há maior capacidade de responsabilização daqueles que invadem dispositivos alheios para pegar dados. As penas variam de detenção de 3 meses até reclusão de 2 anos. Os agravantes para aumento de pena são prejuízo econômico, divulgação ou vazamento dos dados na internet ou resultar na obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas ou o controle remoto não autorizado do dispositivo invadido.

A Lei 12.737/2012, apelidada de Lei Carolina Dieckmann, sobre crimes na internet, altera o Código Penal para tipificar como infrações uma série de condutas no ambiente digital, principalmente em relação à invasão de computadores, além de estabelecer punições específicas, algo inédito até então. Proposta pelo deputado Paulo Teixeira (PT-SP), a lei ganhou o nome "extraoficial" porque, na época em que o projeto tramitava na Câmara de Deputados, a atriz teve fotos pessoais divulgadas sem autorização. A nova lei classifica como crime justamente casos como esse, em que há a invasão de computadores, tablets ou smartphones, conectados ou não à internet, "com o fim de obter, adulterar ou destruir dados ou informações". [52]

A lei define também que o crime existe quando o usuário não autoriza o acesso ao aparelho ou quando o criminoso "instala vulnerabilidades para obter vantagem ilícita". A pena nesses casos é de três meses a um ano de detenção, além de multa.

Também está prevista punição de seis meses a dois anos de reclusão, além de multa, para quem obtiver dados "de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas", após a invasão ou controle da máquina invadida remotamente.

---

[51] Id., ibid, 41.

[52] **''Lei Carolina Dieckmann'' sobre crimes na internet entra em vigor.** Do UOL, em São Paulo 02/04/2013. Disponível em http://tecnologia.uol.com.br/noticias/redacao/2013/04/02/lei-carolina-dieckmann-sobre-crimes-na-internet-entra-em-vigor.htm#fotoNav=1>. Acessado em 10 de outubro de 2013.

Resumindo, a lei 12.737 trouxe o tipo penal da invasão ilegítima de sistemas de informação, ampliou o tipo do crime de indisponibilização de serviço público (art. 266 do Código Penal) e equiparou o cartão magnético a um documento particular, para que a falsificação de cartões de débito e crédito, *per si*, seja punível. No entanto, o tipo penal de invasão necessita de algumas condições para que o crime seja configurado, deve haver obtenção, exclusão ou modificação de dados sem a devida autorização, resultando em crime no artigo 154 do Código Penal.

Ainda, receberá as mesmas penas da invasão aquele que instala uma vulnerabilidade em um sistema de informação para obter vantagem indevida, por exemplo, um backdoor ou uma configuração para que algumas portas de comunicação à internet fiquem sempre abertas. As empresas possuem maior proteção jurídica contra a espionagem digital, pois a obtenção de segredos comerciais e ou informações sigilosas definidas por lei agora também se enquadram na legislação.

A punição branda foi criticada por Renato Opice Blum, especialista em direito digital e presidente do Conselho de Tecnologia da Informação da Fecomercio-SP (Federação dos Comércios de Bens, Serviços e Turismo do Estado de São Paulo). Segundo ele, a pena para quem comete crimes cibernéticos, que prevê de três meses a dois anos, além de multa, deveria ser mais severa. Outro problema apontado por especialistas em direito digital é a lei definir que o infrator deve romper algum tipo de barreira de segurança para que haja crime, o que impedirá a punição a quem usa computadores de terceiros. Por exemplo, um colega de trabalho que se aproveite da ausência do usuário do computador, que não deixou a máquina travada com senha, para roubar dados.

Também entrou em vigor a Lei 84/99, que equipara a prática de roubo de dados de cartão de crédito ao de falsificação de um documento particular. Quem for acusado de cometer este crime estará sujeito à reclusão de um a cinco anos de prisão ou a pagar multa.

O texto também estabelece punição para quem fornecer informações relacionadas à estratégia militar para o inimigo por meios eletrônicos.

A lei 12.735, reconhecida como Lei Azeredo, também entrou em vigor na mesma data, mas carregou pouca coisa de seu projeto original, restando somente duas disposições jurídicas. A primeira indicando que as Polícias Judiciárias mediante regulamentação deverão se preparar para o combate de crimes digitais e que em casos de crime de discriminação (lei 7.716 de 1989), o Juiz poderá solicitar a retirada de conteúdo discriminatório não somente de rádio, TV ou internet, mas de qualquer meio possível.

7 A QUESTÃO DA IMPUNIDADE NO BRASIL

"No Brasil, dos 83,4 milhões de usuários de Internet, 90,8% acessam as redes sociais. Entre as redes mais acessadas, a que mais ganhou novos usuários nos últimos três meses foi o Facebook, contando com mais de 50 milhões de brasileiros conectados. Com números tão expressivos não é de se estranhar que pessoas, mal intencionadas ou que desconhecem a existência de leis que regem o ambiente virtual, executam diversos crimes nas redes.[53]

Entre os crimes virtuais mais praticados nas redes sociais estão:

- INSULTOS: falar mal ou insultar alguém que pode gerar processo com base no Artigo 140 do Código Penal, que pune "*a injúria que ofende a dignidade ou decoro*";
- CALÚNIA: inventar histórias falsas sobre alguém pode ser enquadrado no Artigo 138 do Código Penal;
- DIFAMAÇÃO: associar uma pessoa a um fato que ofende sua reputação. Artigo 139 do Código Penal;
- DIVULGAÇÃO DE SEGREDO: revelar segredos de terceiros na internet ou divulgar material confidencial de documentos/correspondências que possam causar danos, pode levar a processo com base no Artigo 153 do Código Penal;
- ESCÁRNIO POR MOTIVO DE RELIGIÃO: criar comunidade *online* que menospreze ou zombe de pessoas religiosas e religiões. Artigo 208 do Código Penal;
- FAVORECIMENTO DA PROSTITUIÇÃO: Artigo 228 do Código Penal;
- ATO OBSCENO: Artigo 233 do Código Penal;
- ESCRITO OU OBJETO OBSCENO: Artigo 234 do Código Penal;
- INCITAÇÃO AO CRIME: Artigo 286 do Código Penal;
- APOLOGIA DE CRIME: criar comunidades virtuais (fóruns, blogs, etc) para ensinar como burlar a legislação ou divulgar ações ilícitas realizadas no passado, que estão sendo realizadas no presente ou serão realizadas no futuro: Artigo 287 do Código Penal;
- FALSA IDENTIDADE: criar um perfil falso pode levar a processo judicial com base no Artigo 307 do Código Penal;
- PRECONCEITO OU DISCRIMINAÇÃO: comentar em chats, e-mails blogs e outros, de forma negativa sobre raças, religiões, etnias, etc. Artigo 20 da Lei 7.716/89;

[53] http://www.crimespelainternet.com.br/crimes-virtuais-nas-redes-sociais/

- PEDOFILIA: troca de informações ou imagens envolvendo crianças ou adolescentes. Artigo 241-A/241-B/241-C/241-De241-E da Lei nº 8.069/90 ECA;

Outro ponto importante é que muitas pessoas ainda têm dúvidas sobre o assunto e não sabem reconhecer um crime virtual, e acabam sendo vítimas por não saberem como agir.

Além disso, muitos usuários cometem deslizes nas redes, revelando dados pessoais para pessoas totalmente desconhecidas. Ao fazer isso, elas compartilham informações valiosas como: endereço particular, e-mail pessoal, data de nascimento, nome de solteiro e muitas outras informações que podem ser usadas por possíveis mal intencionadas.

É também muito desconhecido como proceder em caso de ser vítima de um crime cibernético. A recomendação é procurar uma delegacia especializada em crimes eletrônicos da região e registrar o boletim de ocorrência (esta é uma grande dificuldade, já que são pouquíssimas em todo Brasil) e para validar a denúncia é preciso levar levar qualquer material que comprove o crime virtual, como um print de tela e o endereço da internet onde a ação criminosa aconteceu.Após o registro da ocorrência, é importante procurar um advogado especializado em Direito Digital para que o profissional guie os próximos passos da vítima no alcance da justiça e punição aos infratores (sinceramente, como as pessoas são informadas sobre essas questões e como tem capacidade cognitiva e condições financeiras para conseguirem fazer todos esses passos? Sinceramente, quantos advogados entendem sobre cibernética no Brasil?)

Além de todos esses crimes das redes sociais, não podemos esquecer sobre os crimes comerciais (onde pessoas enganam outras e roubam-lhes oferecendo bens e serviços que não existem), crimes de invasão de dados bancários e desvios de grandes somatórios, crimes de invasão de sites onde são inseridos informes falsos e levam a enormes prejuízos a empresas, invasão de sistemas públicos e sistemas de defesa, venda de pornografia envolvendo menores, crimes contra a criança (sexuais, comerciais, morais), dentre muitos outros crimes onde a criatividade e a inteligência para o mal não tenham limitites.

Todos estes crimes parecem estar impunes. A impunidade no Brasil não se restringe aos crimes cibernéticos, posto que se tem a clara visão de que ricos e detentores do poder sempre saem ilesos e esta é a sensação que se tem da justiça brasileira. Vemos garotos ricos atirarem fogo em um mendigo e nada repercutir seriamente sobre eles; vemos estudante embriagada que atropela e mata dois trabalhadores e foge e nada acontece à liberdade dela, pois pode pagar fiança de 15 mil reais e sair da prisão (e esse dinheiro não deve ser nem ao menos direcionado para pagar as despesas com os funerais dos trabalhadores mortos); vemos

políticos serem condenados pelo Supremo Tribunal Federal e depois de algum tempo serem libertos por outro juiz do STF; vemos crianças espancadas, negligenciadas, abusadas sexualmente, torturadas fisicamente e psicologicamente serem devolvidas aos agressores pela própria justiça; vemos criminosos disfarçados de policiais (policiais que servem ao crime) trabalhando para o crime, compactuando com bandidos e que não são presos e nem expulsos da polícia; vemos delinqüentes das ruas que matam pessoas indefesas e inocentes por causa de droga ou por alguns trocados que são tidos como viciados e não pagam por seus crimes, por uma política de limpeza das ruas, usando os vícios como escudo para tirarem temporariamente essas pessoas da rua, parecendo que, como viciados eles nunca terão condições de pagarem por seus crimes; vemos líderes do governo e seus comparsas (servidores contratados por eles) desviarem verbas que vem dos bolsos dos cidadãos trabalhadores e nada acontecer com eles. A impunidade parece moda e parece que todos são criminosos, que ninguém é honesto e bom e que ninguém luta por justiça; já que todos são criminosos, quem pode apontar o erro do outro?

Somado a todos esses sentimentos de globalização da criminalidade, tem-se a dificuldade técnica de fazer valer a lei. Para que existir lei, se não se pode fazer cumpri-la? Para poucos a lei funciona ou passa existir. As pessoas comuns (que não são celebridades, não são ricas e não tem poder social ou econômico, que não tem nenhum padrinho) sofrem caladas, sofrem descaso, sofrem duplamente: o crime e a indignidade de não poderem ser protegidas pela Lei. A pessoa comum sofre: tem que esperar, tem que calar, tem que ser o último da fila (pois na frente da fila tem os mais bonitos, mais ricos, mais poderosos, os mais de direito), tem que se contentar em não estar morta e se morre por causa criminal vale apenas como dado estatístico. Essa é a sensação nacional sobre a justiça.

A impunidade do crime cibernético é grande e tem por causa variados fatores: número cada vez mais crescente de crimes, dificuldade em se identificar o criminoso, falta de pessoas qualificadas tecnicamente com conhecimentos cibernéticos atuando a favor da justiça e do bom cidadão, falta de consenso no direito sobre todas as formalizações de leis para regerem esta gama de controvérsias no que tange os crimes cibernéticos e a certeza do criminoso cibernético de que ficará impune por todas essas falhas presentes em nosso sistema de proteção.

De acordo com o levantamento da Trend Micro, o **Brasil** é o quarto país com o maior índice de ataques virtuais. No primeiro trimestre deste ano, **7%** de todos os crimes virtuais

envolvendo roubo de dados de contas bancárias aconteceram no Brasil. **EUA** ficaram em primeiro, seguido por **Japão** (2º) e **Índia** (3º).[54]

Sobre o tema:

> Faz-se necessário a imediata tipificação em nosso ordenamento jurídico, de condutas criminosas praticadas por meio da internet. O Brasil está atrasado no aspecto jurídico, mas em progresso na criminalidade realizada por meios virtuais, devendo-se igualar aos países que já possuem legislação específica para crimes virtuais, para que não sejamos um paraíso aos criminosos desse setor. A jurisprudência nacional tem se mostrado a favor da responsabilização/condenação dos indivíduos que cometem delitos por meio da internet, mas por haver lacunas na lei a respeito do tema, ainda existem criminosos que não podem ser condenados. Estamos entre os dez países que mais utilizam a internet, em um mercado promissor e crescente, sem uma legislação que defina e classifique quantos e quais são os crimes cometidos virtualmente, para amparar os usuários desse serviço.[55] **.**

[54] http://www.tudocelular.com/tecnologia/ noticias/n35791/brasil-quarto-maior-em-crimes-bancarios.html

[55] http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=9963 - Os crimes virtuais e a impunidade real : Luiz Gustavo Caratti de Oliveira, Marília Gabriela Silva Dani. Rio Grande, 30 de Outubro de 2015

8 RESULTADOS

A Internet é uma rede mundial de computadores: uma rede de computadores interligados entre si em escala mundial através de um protocolo comum chamado TCP/IP (Transmission Control Protocol/Internet Protocol). A Internet tem revolucionado o mundo dos computadores e das comunicações como nenhuma invenção foi capaz de fazer. A partir de sua criação é que foram se desenvolvendo a tecnologia em computação, para atender às suas necessidades.

A Internet nasceu nos EUA (Estados Unidos da América), na década de 60, época da Guerra Fria. Em 1961, Leonard Kleinrock, do MIT (Massachussets Institute of Technology), publicou o primeiro trabalho sobre a teoria de troca de pacotes e convenceu Roberts da possibilidade teórica das comunicações usando pacotes ao invés de circuitos. Em 1962, uma série de memorandos foram escritos por J.C.R. Licklider, do MIT, discutindo o conceito da "Rede Galáxica", onde previa vários computadores interconectados globalmente.

A partir daí foram surgindo tecnologias para seu desenvolvimento. Em 1985 a Internet já estava bem estabelecida como uma larga comunidade de suporte de pesquisadores e desenvolvedores e começava a ser usada por outras comunidades para comunicações diárias pelo computador e correio eletrônico já estava sendo utilizado por muitas comunidades. Houve grande expansão de comunidades e o setor comercial começou a se interessar pela Internet. Em 1990 foi criada a WWW e a internet ganhou popularidade e passou a ser explorada comercialmente, com abertura a nível mundial.

No Brasil, a internet teve seu início em 1991, passando a ter abertura para a população em 1995.

Interessante é que desde o início da criação da internet já se tinha conhecimento de crimes cibernéticos. No início, no entanto, quem praticava esses crimes eram experts da informática e eram crimes mais voltados para sistemas de computadores.

Na década de 70 a figura do Hacker já era citada com o advento de crimes como invasão de sistema e furto de software, mas foi em 1980 que houve maior propagação dos diferentes tipos de crimes. Em 1993, após criação da WWW, a internet teve expansão comercial e começou a se espalhar. Em 1980, antes mesmo da propagação da internet, já havia propagação dos crimes. Isto demonstra o poder que tem as pessoas que querem usar a internet para o mal.

O Brasil começou a se preocupar com esse assunto especialmente a partir das últimas décadas, com o aumento da popularização dessa inovação tecnológica.

Em poucos anos, desde que a internet surgiu no Brasil (1995) até hoje (2013) – são apenas 18 anos-, a internet se tornou abrangente em todo Brasil, atingindo todas as camadas sociais, se tornou o principal meio de comunicação para todos: desde grandes empresas, propagandas, até o simples cidadão; a internet se tornou a principal e mais importante forma de comércio e negócios; é também o principal difusor de idéias, de pensamentos, de informações e de conhecimento. A internet, hoje, é fundamental em nossas vidas.

Em meio a este grande emaranhado de informações e situações, que antes eram vividas somente pessoalmente e hoje são vividas através da internet, surgem situações e particularidades que o direito existente fica despreparado. A internet traz algumas particularidades aos crimes que a envolvem, que os crimes comuns não possuem.

Crime de informática pode ser definido, como qualquer ato ilegal onde o conhecimento especial de tecnologia de informática faz com que o sujeito da ação infratora tenha êxito na sua conduta. Em determinadas vezes, o crime de informática assemelha-se muito ao crime comum, ou definição de crime, tendo somente a diferença que o objeto utilizado para o êxito foi um computador ou algum sistema informatizado.

E quais são os sujeitos ativos dos crimes de informática? Quando se trata de crimes realizados na internet ou com auxilio dela, logo vem em nossa mente que são realizados por "experts", os chamados Crackers, porém com a popularização desse meio surgiram milhares de casos, produzido por pessoas com mínimo de conhecimento tecnológico. E qual seria a responsabilidade dos provedores? Uma posição que está se tornando a tendência sobre a responsabilidade penal dos provedores é a da responsabilidade limitada, onde, p.ex., sendo de conhecimento do provedor, conteúdo ilegal, seria de se esperar que este não divulgasse tal conteúdo ou o bloqueasse (tendo meios técnicos para isto). Não o fazendo, assumiria a corresponsabilidade pelo fato.

Os provedores da Internet têm um argumento muito sólido e realista, afirmando que o volume de dados dentro da Internet, como dentro das listas de discussões, é tão grande que o processo de checar e verificar a decência dos mesmos é humanamente impossível. O que se discute não é a imputação de conduta delituosa da empresa provedora de Internet, mas sim a sua responsabilidade pela divulgação do material considerado ilegal ou ofensivo, desde que conhecedora do fato.

É muito controversa a questão sobre a responsabilidade dos provedores. Poderia serem corresponsabilizados pelos fatos delituosos? Necessitaria, primeiramente, de terem condições de monitorarem cada informação que fosse passada. Mas mesmo assim ainda haveriam muitas

questões a discutir, como por exemplo: quais informações poderiam ser barradas sem ofender o direito à expressão? Quem decidiria sobre essas questões?

Os crimes ligados à informática podem ser classificados em dois grandes grupos: puro (também chamado próprio) e impuro (também chamado impróprio). Puro é o crime de informática que ao se utilizar um computador, visa pura e somente o ataque a qualquer outro computador ou sistema de informática. Impuros são aqueles realizados com a utilização do computador para realização de condutas ilícitas que atinge todo o bem jurídico já tutelado. Crimes, portanto, já tipificados que são realizados, agora, com a utilização do computador e da rede.

Os crimes cibernéticos apresentam características que lhes proporcionam uma singularidade com relação aos crimes comuns. A seguir serão apresentadas algumas de suas características particulares mais importantes: 1-Celeridade: os crimes cibernéticos são rápidos. 2-Dinamismo: os crimes cibernéticos podem ser cometidos das mais variadas formas e estas formas mudam muito facilmente devido a alta tecnologia que é desenvolvida a cada momento. 3-Poucas leis tipificando-os diretamente. 4- Transgressor aos limites de Vigência, Territorialidade e Pessoa. 5- Falta de regulamentação para a guarda apropriada de provas. 6-Dificuldade de identificação de quem comete o crime. Todas essas características já conferem ao direito digital particularidades que, em muitos casos fica difícil ou até impossível punir um ato digital delituoso apenas por analogia ou pelos princípios básicos do direito e jurisprudência.

Uma das maiores falhas da internet é a falta de identificação de usuários pelo seu RG ou CPF, ou outra identificação. Como não há a necessidade de nenhuma forma de identificação ou qualquer tipo de controle no acesso a internet, qualquer cidadão pode deliberadamente acessá-la usando pseudônimos muitas vezes taxativos sobre suas intenções.

O espaço virtual, que se mostra tão propício para a prática dos mais variados crimes, apesar da falta de legislação específica, é relativamente protegido juridicamente, pois se encontram no ordenamento jurídico brasileiro algumas normas que tratam da matéria, como por exemplo: a Lei nº 11.829/08, que combate a pornografia infantil na internet; a Lei nº 9.609/98, que trata da proteção da propriedade intelectual do programa de computador; a Lei nº 9.983/00, que tipificou os crimes relacionados ao acesso indevido a sistemas informatizados da Administração Pública; a Lei nº 9.296/96 disciplinou a interceptação de comunicação telemática ou informática; e a Lei nº 12.034/09, que delimita os direitos e deveres dentro da rede mundial, durante as campanhas eleitorais.

Além disso, os aplicadores do direito têm aplicado a legislação já existente, como o Código Penal, aos crimes cometidos no meio virtual. Exemplos de crimes cibernéticos já tipificados na legislação penal que são cometidos através de computadores e outros meios tecnológicos são, entre outros, o crime de calúnia, ameaça, difamação, apologia a crime ou criminoso, injúria, constrangimento ilegal, falsa identidade.

O Brasil se mostra atrasado por ainda não possuir uma legislação específica para disciplinar os crimes cibernéticos. Vários países já apresentam legislação específica que tratam dos crimes cibernéticos, como Estados Unidos, Portugal, Inglaterra, entre outros.

Com a entrada em vigor das leis 12.735 e 12.737, ambas de 2012, temos a aplicação penal de normas específicas sobre os crimes digitais próprios, aqueles cometidos contra dados, informações ou sistemas de informação. As penas variam de detenção de 3 meses até reclusão de 2 anos. Os agravantes para aumento de pena são prejuízo econômico, divulgação ou vazamento dos dados na internet ou resultar na obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas ou o controle remoto não autorizado do dispositivo invadido.

A Lei 12.737/2012, apelidada de Lei Carolina Dieckmann, sobre crimes na internet, altera o Código Penal para tipificar como infrações uma série de condutas no ambiente digital, principalmente em relação à invasão de computadores, além de estabelecer punições específicas, algo inédito até então. Tipicidade é a correspondência exata, a adequação perfeita entre o fato natural concreto e a descrição contida na lei. Como o tipo penal é composto não só de elementos objetivos é indispensável que não só o fato objetivamente considerado, mas também a sua antijuridicidade, e os elementos subjetivos que se subsumam a ele. A lei 12.737 trouxe o tipo penal da invasão ilegítima de sistemas de informação, ampliou o tipo do crime de indisponibilização de serviço público (art. 266 do Código Penal) e equiparou o cartão magnético a um documento particular, para que a falsificação de cartões de débito e crédito, *per si*, seja punível.

A Lei 12.735, reconhecida como Lei Azeredo, também entrou em vigor na mesma data. Ela indica que as Polícias Judiciárias mediante regulamentação deverão se preparar para o combate de crimes digitais e que em casos de crime de discriminação (lei 7.716 de 1989), o Juiz poderá solicitar a retirada de conteúdo discriminatório não somente de rádio, TV ou internet, mas de qualquer meio possível.

Mas várias modalidades de crimes cometidos por meio da internet não estão tipificadas, ou seja, não podem ser passíveis de punição. É comum nestes casos o uso da analogia jurídica para

adequar crimes sem tipificação aos já descritos em nosso ordenamento jurídico. Como exemplo, a destruição de dados eletrônicos equiparando o mesmo ao crime de dano ao patrimônio.

Fica evidente que esse tipo de analogia por muitas vezes não pode ser aplicado à realidade dos fatos, uma vez que a intensidade das condutas praticadas com o uso da internet, tais como, a disseminação de mensagens racistas, homofóbicas e discriminatórias de qualquer forma, o uso indevido da imagem, dentre outros exemplos, é muito maior. São inúmeras as formas ilícitas que, com o uso da internet, se proliferam com velocidade espantosa, se diferenciando da ação cometida por intermédio de outros meios de informação. Uma informação falsa veiculada pela internet, ou um fato difamatório ou injurioso destinado a uma pessoa ou a uma determinada classe da sociedade, certamente terá uma exposição muito mais rápida e vultosa, do que se esse mesmo fato fosse veiculado por outros meios, que não pelo uso da internet como meio de proliferação.

Cumpre frisar também que a analogia jurídica aplicada na norma penal incriminadora não pode ser considerada válida, nos casos prejudiciais ao réu.

Portanto, essa analogia na maioria dos casos não se efetiva, pois, se o juiz não pode aplicar pena a fato que não seja típico, este também não poderá julgar por analogia crime que seja atípico, até por que no Direito Penal, a analogia só pode ser usada em beneficio do réu, o que prejudica substancialmente o fundamento jurídico da decisão do juiz, que sem este embasamento, que é caráter essencial da sentença penal, deverá proceder com a absolvição do acusado, sob pena de não o fazendo, considerar-se nulo o processo.

9 CONSIDERAÇÕES FINAIS

A internet começou a surgir na década de 60 nos Estados Unidos e logo surgiram os primeiros crimes de informática. Neste início, em que a internet ainda não era difundida popularmente, quem cometia os crimes era quem entendia profundamente de informática. Na década de 90, a internet começou a ser difundida mundialmente e os crimes também aumentaram em número e formas. Se antes quem cometia esses crimes era somente os experts, hoje em dia qualquer pessoa, com o mínimo de conhecimento em informática, pode cometer um crime.

Em um mundo que se torna cada vez mais globalizado, podemos conferir à internet grande responsabilidade para concretização dessa mudança. A facilidade com que as informações podem ser trocadas por este meio de comunicação, com agilidade e baixo custo, faz com que o uso da internet cresça de maneira exorbitante em todo mundo.

Com aumento considerável de pessoas que utilizam essa tecnologia, tanto como meio de trabalho, quanto para o entretenimento, a internet se tornou um meio indispensável em nossa sociedade, trazendo questões desconhecidas pelos operadores do direito. Essa inovação tecnológica fez transparecer a necessidade eminente do direito de acompanhar as mudanças da sociedade.

A liberdade de expressão e as garantias individuais protegidas pela Constituição Federal devem ser resguardadas também no mundo virtual, pois a internet não pode ser considerada território imune ao direito, nem tampouco um mundo surreal de fantasia.

Nesse sentido, cumpre salientar que a carência de legislação específica para punir quem utiliza desse meio para praticar atividades delituosas acaba trazendo consigo a sensação de impunidade, que estimula substancialmente a prática de delitos repudiados pela sociedade. Cumpre frisar que a jurisprudência pátria tem adotado nos casos em que há lacunas nas normas do direito, o julgamento por analogia.

Mas muitos desses crimes ficam impunes, surgindo assim à criação de comunidades criminosas, os denominados C*rackers* que, graças ao anonimato, muitas vezes se vangloriam de crimes por eles praticados na internet sem o menor pudor, crimes estes que nem sempre visam a satisfação material mas, na grande maioria das vezes, a satisfação pessoal, como nos crimes puramente informáticos em casos de invasão de sites da internet com mero objetivo de demonstrar que conseguiu transpor uma barreira de segurança.

Todavia, há que mencionar os crimes que, mesmo já tipificados em nosso ordenamento jurídico, ganham projeção muito maior ao ser exposto na internet, tais como os

crimes contra honra; injúria, difamação, e calúnia, que devido a rapidez na divulgação da mensagem atentatória, ganham visibilidade alcançando um maior numero de pessoas.

Embora já tenham sido tomadas certas medidas emergenciais, como a criação de normas que regulam algumas dessas condutas criminosas que ocorrem no meio virtual, apesar, também, da aplicação do Código Penal para alguns crimes cibernéticos, é necessária uma legislação específica que englobe com eficiência todas essas condutas, até porque o nosso Código Penal é de 1940, época em que não existiam as tecnologias que utilizamos nos dias de hoje.

A entrada em vigor da Lei nº 12.737/12 acaba por ser um primeiro avanço à tutela jurídica existente para coibir e ao mesmo tempo sancionar os crimes praticados no ambiente virtual.

Logo, a legislação pátria passa a contar com novas ferramentas de apoio à sociedade que antigamente se reservava à esfera cível para buscar alguma espécie de reparação/sanção.

Valendo-se da informação prestada no parágrafo anterior aproveita-se ainda para esclarecer que a existência de previsão legislativa no âmbito penal não inviabiliza ou coloca em desuso as tutelas presentes na esfera cível, já que é facultado à parte buscar a sanção do agente ativo do crime no âmbito criminal, bem como pleitear uma reparação financeira, ou ainda, uma retratação pública no âmbito civil.

No Direito Privado, o que se objetiva é a reparação de dano em prol da vítima; no Direito Penal, como regra, busca-se a punição e a melhor adequação social em prol da sociedade. Sendo assim, conclui-se que a entrada em vigor da Lei nº 12.737/12, além de demonstrar uma evolução de nossa legislação pátria, por tratar de assunto contemporâneo a nossa sociedade, demonstra apta a complementar os institutos jurídicos existentes, tornando ainda mais eficaz nosso ordenamento jurídico do ponto de vista de apresentar resguardo no âmbito civil e agora criminal no tocante a infrações cometidas em ambiente virtual.

Contudo, observa-se que as penas são pequenas, o que permite o enquadramento dos crimes como sendo de menor potencial ofensivo, o que não se coaduna com a proteção dos ativos intangíveis, a pedra angular da sociedade da informação. Muitas vezes uma apropriação indevida de dados pode ser mais prejudicial que um furto comum e, por isso, não deveria ter pena mais branda,sobretudo em casos de espionagem que podem levar à concorrência desleal.

Cumpre ressaltar o aumento da intensidade e da rapidez com que se propagam os crimes já tipificados em nosso ordenamento jurídico, que por meio da internet atingem um número muito maior de vitimas em menor tempo, muitas vezes com a prática de uma só ação, como o envio de um email destinado a milhares de pessoas, merece uma maior reprovação.

Como os crimes cibernéticos ocorrem no mundo inteiro e pelo fato de não respeitarem fronteiras, além da legislação específica, é necessário a adesão em tratados internacionais que disciplinam a matéria: o Brasil precisa ser signatário de um tratado que permita a colaboração externa, como a adesão à Convenção Internacional de Cibercrime – diploma internacional assinado em Budapeste, pelos países europeus, Estados Unidos e Canadá.

REFERÊNCIAS

ARANHA, Adalberto José Q.T. Camargo. **Crimes contra a Honra**. 3 ed. São Paulo: Saraiva, 2005.

BOGO, Kellen Cristina. **A história da Internet – Como tudo começou**...". Edição número 11. 05 pg. Matéria publicada em 01/07/2000. Disponível em <http://www.Kplus.com.br/materia.asp?co=11&rv=Vivencia>. Acesso em 17 de agosto de 2010.

CASTRO, Aldemário Araújo. **Informática Jurídica e Direito da Informática**. Livro virtual. Cap 4, Internet: conceito, histórico e funcionamento. 06 pg. 2007. Disponível em <http://www.aldemario.adv.br/ infojur/c onteudo4texto.htm>. Acesso em 27 de julho de 2010. MIRABETE, Julio Fabbrini. FABBRINI, Renato N. **Manual de Direito Penal**. 25 ed. São Paulo. Atlas. 2007. V2, p 127.

CORRÊA, Gustavo Testa. **Aspectos jurídicos da Internet**. 2 ed. ver. São Paulo: Saraiva, 2002.

FREIRE, Antonio Carlos Pantoja. **Os desafios da perícia eletrônica forense como meio de prova no processo civil.** Publicado em 01/08/2011 | Nº 91 - Ano XIV - AGOSTO/2011. Disponível em: < http://www.ambito-juridico.com.br/site/?n_link=revista _artigos_leitura& artigo_id =9966&revista_caderno=17 >. Acessado em 17 de julho de 2012.

GATTO, Victor Henrique Gouveia. **Tipicidade penal dos crimes cometidos na internet.** Publicado em 01/08/2011 | Nº 91 - Ano XIV - AGOSTO/201. Disponível em: <http://www.ambitojuridico.com.br/site/?n_link=revista_artigos_ leitura&artigo_id=9962&revista_caderno=17>. Acessado em 09 de julho de 2012.

KLEINROCK, Leonard; LYNCH, Daniel C.; POSTEL, Jon, ROBERTS, Larry G.; WOLFF, Stephen. **A Brief History of the Internet**. Texto traduzido. 15 p. Ano ? Disponível em <http://www.aisa.com.br/historia.html>. Acesso em 03 de junho de 2010.

''Lei Carolina Dieckmann'' sobre crimes na internet entra em vigor. Do UOL, em São Paulo 02/04/2013. Disponível em http://tecnologia.uol.com.br/noticias/redacao/2013/04/02/lei-carolina-dieckmann-sobre-crimes-na-internet-entra-em-vigor.htm#fotoNav=1>. Acessado em 10 de outubro de 2013.

LEINER, Barry M.; CERF, Vinton, G.; CLARK, David D.; KAHN, Robert E.;

MENDES, Maria Eugenia Gonçalves; VIEIRA, Natália Borges. **Os crimes cibernéticos no ordenamento jurídico brasileiro e a necessidade de legislação específica.** Disponível em: < http://www.gcpadvogados.com.br/artigos/os-crimes-ciberneticos-no-ordenamento-juridico-brasileiro-e-a-necessidade-de-legislacao-especifica-2 >. Acessado em 19 de agosto de 2012.

MONTEIRO, CÉSAR MACEDO . **Classificação dos crimes de informatica ainda sem nota de rodapé.** 68 pg. 03 de novembro de 2013. Disponível em: <hppt//http://www.slideshare.net/cmacedomonteiro/classificao-dos-crimes-de-informatica-ainda-sem-nota-de-rodap.>. Acessado em 10 de novembro de 2013. Pg 2-3.

KEVIN D. MITNICK ; SIMON, WILLIAM L ; WOZNIAK, STEVE . The Art Of Deception , Ed. John Wiley & Sons, ed 2009 (**Crimes Da Informática** – Remy Gama Filho Editora: Copymarket.Com, 2000).

TEXTO PUBLICADO NA INTERNET. **História da Internet**. 03pg. Ano? Disponível em <http://www.brasie scola.com/informática/internet.htm>. Acesso em: 14 de setembro de 2010.

TEXTO PUBLICADO NA INTERNET. **História da Internet**. 02pg. 20/08/2011. Disponível em <hppt//WWW.suap esquisa.com/internet/acesso em 20/08/2011.>. Acessado em 03 de outubro de 2011.

TEXTO PUBLICADO NA INTERNET. RODRIGUES, JC. **Introdução ao Direito Digital.** 27pg. Aula introdutória sobre Direito Digital do curso de Comunicação Digital para graduação em Propaganda e Marketing - ESPM São Paulo. 30/10/2010. Disponível em <hppt// http://www.slideshare.net/carlos_rds/introduo-ao-direito-digital>. Acessado em 15 de fevereiro de 2013. Pg6.

ANEXO I

LISTA DE DELEGACIAS ESPECIALIZADAS EM CRIMES CIBERNÉTICOS

- **Rio Grande do Sul**: possui delegacia específica, criada em 28/05/2010. É a Delegacia de Repressão aos Crimes Informáticos do Departamento Estadual de Investigações Criminais - DRCI/DEIC. A DRCI fica na Av. Cristiano Fischer, 1440, Bairro Jardim do Salso em Porto Alegre, na mesma sede do DEIC. O telefone de contato é (0xx51) 3288-9817, e-mail drci@pc.rs.gov.br.

- **Paraná**: Nuciber da Polícia Civil do Paraná, sito na Rua José Loureiro, 376, 1º andar – sala 1 – Centro – 80010-000 – Curitiba-PR, Tel:(41) 3323-9448 – Fax: (41) 3323-9448, e-mail cibercrimes@pc.pr.gov.br. O Núcleo de Combate aos Cibercrimes do Paraná é dirigido pelo Dr. Demétrius Gonzaga de Oliveira;

- **São Paulo**: existe, além da Delegacia Eletrônica para registro de ocorrências,a 4ª Delegacia de Delitos Cometidos por Meios Eletrônicos **DIG/DEIC, localizada na** Avenida Zack Narchi,152 - Carandiru, São Paulo/SP (CEP: 02029-000), telefone: (0xx11) 2221-7030 e e-mail 4dp.dig.deic@policiacivil.sp.gov.br;

- **Rio de Janeiro**: possui a **Delegacia de Repressão aos Crimes de Informática (DRCI), com** endereço na Rua Professor Clementino Fraga, nº 77 (2º andar), Cidade Nova (prédio da 6ª DP), Rio de Janeiro/RJ (CEP: 20230-250), telefones (0xx21) 2332-8192, 2332-8188 e 23328191 e e-mails drci@pcivil.rj.gov.br;

- **Espírito Santo**: **Delegacia de Repressão a Crimes Eletrônicos (DRCE)**, com endereço na Av. Nossa Senhora da Penha, 2290, Bairro Santa Luiza, Vitória/ES (CEP: 29045-403), telefone (0xx27) 3137-2607 e e-mail drce@pc.es.gov.br.

- **Minas Gerais**: **DEICC – Delegacia Especializada de Investigações de Crimes Cibernéticos**, com endereço na Av. Nossa Senhora de Fátima, 2855 – Bairro Carlos Prates – CEP: 30.710-020, Telefone (31) 3212-3002 e (31)3201-7584, com titularidade dos Drs. Cesar Duarte Matoso (titular da 2ª DEICC/MG) e Felipe Dias Falles Gomes Pinto (titular da 1ª DEICC/MG). E-mail dercifelab.di@pc.mg.gov.br.

- **Piauí**: possui a **Delegacia Especializada de Repressão aos Crimes de Alta Tecnologia - DERCAT**. Titular é a Delegada de Polícia Cristiane Fonteles. Fica na Rua Barroso, nº 241, Centro de Teresina e possui os telefones 086-3216-5212 (Recepção), 086-3216-5225 (Plantão Geral) e 086-3216 5272 (Fax).

- **Pará**: possui a **Delegacia de Repressão aos Crimes Tecnológicos**, com a titularidade pela Dra. Vanessa Lee. A DRCT é vinculada à Diretoria de Repressão ao Crime Organizado, que está situada na Rua Oliveira Belo, 807, entre Travessa 9 de janeiro e Av. Alcindo Cacela, Bairro Umarizal, Belém-PA, com telefone de contato 91-3222-7567 e e-mail drc tp a @ po li ciacivil.pa.gov.br e drctpa@gmail.com.
- **Tocantins**: possui a **Divisão de Repressão a Crimes Cibernéticos**, que possui como responsável a Delegada de Polícia Liliane Albuquerque Amorim. A Delegacia possui como telefone de contato 063-3218-6986 e e-mail deic.drcc@ssp.to.gov.br.
- **Maranhão**: há o **Departamento de Combate aos Crimes Tecnológicos**, vinculado à Superintendência Estadual de Investigações Criminais - DCCT/SEIC. Em breve mais dados.
- **Pernambuco**: possui uma Delegacia Interativa, para registros de ocorrências online. Possui a **Delegacia de Polícia de Repressão aos Crimes Cibernéticos** e possui como responsável o Delegado de Polícia Leonardo Roque da Mata Monteiro Gama. O telefone de contato é 081-3184-3206 ou final 3207 e e-mail dpcrici@policiacivil.pe.gov.br. Está localizada na Rua da Aurora, 487, Boa Vista, Recife/PE.
- **Sergipe**: possui a Delegacia de Repressão a Crimes Cibernéticos e fica localizada no Complexo Especializado de Polícia Civil, na Rua Laranjeiras, 960, Centro, Aracaju, Sergipe, com telefone de contato 079-3198-1158.
- **Bahia**: Criou o Grupo Especializado de Repressão aos Crimes Eletrônicos (GME) em 05/05/2012. Titularizado pelo Delegado de Polícia Charles Leão, telefone 071-3117-6109 e e-mail charles.leao@pcivil.ba.gov.br. Mais detalhes em outro post deste blog: Criado Grupo Especializado de Repressão aos Crimes por Meios Eletrônicos na Polícia Civil da Bahia

- **Mato Grosso**: criou, em outubro de 2010, a GECAT (Gerência Especializada de Crime de Alta Tecnologia), órgão similar ao existente no Distrito Federal. O responsável é o Delegado de Polícia Anderson Veiga. O telefone de contato é o (65) 3613-5699.
Os demais Estados fazem orientações de como investigar os delitos informáticos através de seus serviços de Inteligência Policial Judiciária. Ministrei aula em vários deles.
- **Goiás**: embora no site do Safernet tenha menção, o setor dentro da DEIC não está ativo, funcionando mais diretamente dentro da Gerência de Inteligência da Polícia Civil, mais precisamente no Setor de Análise (0xx62) 3201-6352 e 6357). Recentemente fiz um treinamento com o pessoal de lá, com 23 alunos entre alunos e delegados. Portanto, caso o

registro seja feito nas Delegacias certamente elas procurarão orientação com a área de inteligência sobre como proceder nas investigações.

- **Rondônia**: não possui um órgão específico, mas formou duas turmas de alunos, entre agentes e delegados, em Agosto/Setembro de 2009, habilitando profissionais de várias delegacias. Portanto, você pode se dirigir a qualquer DP e registrar o fato que, certamente, não ficará sem apuração. Rondônia também possui uma Delegacia Interativa, para registro de ocorrências online;