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

JOÃO VITOR VIDIGAL

FERRAMENTAS JURÍDICAS EM COMBATE À INSEGURANÇA DA REDE

BARBACENA
2013

FERRAMENTAS JURÍDICAS EM COMBATE À INSEGURANÇA DA REDE

João Vitor Vidigal*
Antônio Américo de Campos Junior**

Resumo

Este artigo consiste em um estudo a respeito da necessidade de especificação legislativa a respeito dos crimes cometidos utilizando meios virtuais, tal qual a internet ou *softwares,* utilizados a fim causar danos materiais ou psicológicos às suas vitimas, além de informar a respeito dos crimes mais ocorrentes e explicar ainda textos legais já vigentes em nosso país que se referem ao tema abordado. A pesquisa, de revisão bibliográfica, foi realizada através de artigos científicos online, doutrinas e sites institucionais do Supremo Tribunal Federal e Superior Tribunal de Justiça. Pode-se observar que o ordenamento jurídico brasileiro de forma harmônica mais uma vez propicia à justiça condições de desemprenhar seu papel vocacional de dar a cada um aquilo que lhe é devido.

Palavras-chave: Crimes Cibernéticos. Fraudes na Internet. Direito Moderno. Segurança Internet.

1 Introdução

Com o desenvolvimento tecnológico abrupto que ocorre desde a década de noventa, sobretudo em seu final, isto é com o início da popularização mundial da internet, vislumbramos uma nova relação social, sendo esta decorrente da interatividade virtual entre as pessoas. Porém, como é sabido, dentro de qualquer interação social não existem somente benefícios; encontramos, também, pessoas dispostas a se aproveitar da falta de conhecimento social quanto ao novo, e, através disso pode-se estranhar minha colocação quanto a chamar de novo o mundo

* Graduando do 10º período do Curso de Graduação em Direito da Universidade Presidente Antônio Carlos - UNIPAC/Barbacena. E-mail: jvvidigal@yahoo.com.br
**Professor Orientador, Mestre em Direito Administrativo e Professor da disciplina de Direito Administrativo do Curso de Graduação em Direito da Universidade Presidente Antônio Carlos - UNIPAC/Barbacena. E-mail: juniorcampos@uai.com.br

arquitetado no âmbito virtual. Porém, assim entendo todo aquele conhecimento que ainda não dominado pela fração maior da sociedade. Devemos, então, entender que por mais que algo já nos seja intimo, para outras pessoas continua sendo algo novo. E mesmo essa intimidade que consideramos ter com a própria internet, muitas vezes é uma prepotência que nos coloca em armadilhas lesivas a nosso patrimônio e sigilo de nossos dados.

Nosso Estado não se coloca totalmente omisso. Porém, ainda são poucas as leis especificas a respeito da segurança virtual, devendo muitas vezes ser a analogia a outra lei vigente. Devemos, então, nos perguntar: qual o papel do Legislativo neste âmbito?

Em virtude destas colocações pretendo dissertar sobre a necessidade de intervenção estatal para regulamentar e tipificar ações decorrentes das relações virtuais, a fim que de traga uma segurança social, para que diminua este novo instituto criminal, tal qual estabelecer métodos de fiscalização, sem atingir a liberdade da pessoa, e, por fim, discutir a eficácia das leis já vigentes desta matéria.

2 O que é a Internet?

Sabemos pesquisar, interagir, enfim, navegar. Mas acredito que não faz parte do conhecimento comum as origens e motivos da criação desta que a maior rede virtual que existe no mundo. Colocarei, então, uma explicação sobre seus fatos geradores.

Seguindo o disponível nos editoriais a cerca de tecnologia e informação do G1[1], a origem da internet se deu da necessidade das instituições militares norte-americanas, em meados dos anos sessenta, em plena guerra fria, criar um sistema de comunicação que não dependesse de padrões já estabelecidos, tal qual o rádio, e da descentralização das informações contidas no Pentágono, para evitar uma possível perda irreparável de documentos caso ecoasse uma guerra em solo americano. Foi criada, então, a ARPANET, a rede de conexão da DARPA - Agência de Projetos de Pesquisa Avançada dos Estados Unidos.

No ano de 1973, o sistema elaborado pela DARPA foi aprimorado pelos cientistas Net Vinton Cerf e Bob Kahn, que descreveram a possibilidade de

[1]http://www.techtudo.com.br/artigos/noticia/2013/04/internet-completa-44-anos-relembre-historia-da-web.html

utilização dos protocolos TCP/IP, e já no ano de 1974, foi publicado o método para que estes fossem usados, método até atualmente utilizado, sendo desenvolvida somente a capacidade de acessos simultâneos à rede.

No início dos anos 80, o uso da internet saiu da exclusividade militar e passou a integrar ao meio universitário, para facilitar a troca de informações entre pesquisadores, professores e alunos, o que serviu também como um meio de desenvolver suas estruturas. Porém, em 1988, começou-se a olhar a internet com uma visão comercial, e surgiu a primeira popularização da rede, com a utilização do correio eletrônico e serviços de provedores online.

Com a comercialização da internet feita pelos Estados Unidos em 1989, entramos na década de 90, e logo em 1992 se deu, em meio a União Europeia, a criação do World Wide Web (www), que digitamos antes dos endereços. Também ocorreu a criação do Google, que atualmente é a ferramenta de busca mais acessada mundialmente, e uma das marcas mais valiosas no mercado econômico.

A partir dos anos 2000, a necessidade de se reinventar tornou-se rotineira na rede, e com isso surgiram as principais formas de interatividade social. Destaca-se o Orkut, que foi uma das primeiras redes sociais populares, dando lugar, posteriormente, ao concorrente Facebook, como o investimento das grandes desenvolvedoras de jogos em versões online, que possibilitava jogadores de todos os países interagirem em mundos virtuais e a utilização da internet como instrumento de intermédio comercial entre partes. Considerando estes benefícios, em contrapartida foram desenvolvidos também métodos para lesar as pessoas para benefício patrimonial.

3 Fragilidade social a respeito de crimes virtuais

Segundo pesquisa promovida pela agencia de jornalismo inglesa BBC[2], no ranking mundial de condições de uso da internet pela população, o Brasil ocupa a 61ª primeira posição, perdendo, dentro da América latina, para o Chile, ocupante da 40º posição.

Esta falta de infraestrutura pode ser considerada como a ponta do *iceberg* da desatenção que os Poderes Legislativo e Executivo brasileiro têm para os seus cidadãos que fazem uso da internet.

[2]http://www.bbc.co.uk/portuguese/noticias/2010/03/100325_rankinginternet.shtml

Há se de falar de políticas de inclusão digital, que ocorrem em escolas e instruem os jovens quanto ao seu uso; porém, esta inclusão é algo superficial, pois mostram a funcionalidade da internet, mas não os preparam para agir frente a uma situação que possa se caracterizar como um crime virtual. Sem citarmos, ainda, a falta de oportunidade para pessoas que já não estudam e que presenciaram a amplificação da internet já em idade adulta, e que, agora, passados quase vinte anos, ainda a consideram algo inacessível, colocando no âmbito intelectual.

A mídia, entretanto se preocupa com esta situação fragilizada; e conhecendo do elevado número de ocorrências a respeito de crimes virtuais, seja este em qualquer espécie, procura divulgar e promover métodos de autotutela dos internautas contra criminosos na rede, tomando para si esta função pública.

Consideramos, então, a falta de interesse público em estruturar o acesso físico à rede, somada à aprendizagem superficial promovida pelo Estado aos jovens, e à inexperiência quanto ao uso da internet por seus pais, como um ambiente fértil para a prática de atos criminosos por aqueles que buscam proveito próprio em virtude da desvantagem alheia. Considerando estes como os mais vulneráveis a se tornarem vitimas, podemos ressaltar que empresas de telefonia e agências financeiras também são alvos frequentes de crimes cibernéticos. Porém estas se protegem no próprio âmbito virtual, com desenvolvimento contínuo de programas que lhes tragam segurança na rede.

Devemos nos lembrar do fato de que apesar de apontar um fragmento populacional como vulnerável, não podemos deixar de nos considerarmos potenciais vitimas, pois o simples fatos de desfrutarmos da troca de informações online já nos potencializam a figurar no polo passivo desta situação. Devemos, então, tomar todas as precauções possíveis e conhecidas para nos proteger, tais quais: utilização de antivírus e *firewalls,* além de não fornecer dados bancários sem antes de consultarmos a agência da qual somos filiados.

4 Delitos recorrentes na internet

Conceituando os crimes cibernéticos no Brasil, temos que são todos aqueles praticados mediante o uso de quaisquer meios referentes à informática, seja, computadores, celulares ou *tablets*.

Vejamos as palavras do Juiz Azevedo sobre o tema estudado (proferidas em AMAGIS, 2011)[3]:

> conceito de crime cibernético no Brasil é exatamente o fato consistente na prática de crime contra uma pessoa ou sociedade, mediante o uso da internet, passível de enquadramento nas leis penais brasileiras, para fins de punição efetiva, ou seja, aquele que sai do virtual e entra na realidade de todos.

Dividirei o estudo dos crimes em três segmentos: crimes contra o patrimônio e propriedade imaterial, crimes contra a honra e pedofilia, em virtude dos perfis do polo passivo e ativo que situa cada grupo especificando suas particularidades e forma de combate.

4.1 Dos crimes contra o patrimônio e propriedade imaterial

Iniciando este estudo com um trecho do livro a Arte da Guerra, quero ambientar o ensinado por Sun Tzu (2000, p.24) neste espaço que estou expondo, e afirmar que, conhecendo a forma de agir dos criminosos cibernéticos, conseguimos agir de uma forma contrária, a fim de nos proteger e informar a autoridades competentes da pratica de tais atividades delituosas.

Então vejamos esta passagem:

> Ciente de tuas capacidades e limitações, não inicies nenhuma empreitada que não possas levar a cabo. Decifra, com a mesma argúcia, o longe e o perto, para que o que se desenrola sobre seus olhos seja idêntico ao que deles está mais recôndito.

Este pensamento deve é relacionado visto que crackers utilizam a ignorância popular a fim de trazer, de forma silenciosa, sua perspicaz lesão ao patrimônio alheio. Prática comum deste meio se dá na movimentação de valores irrisórios de centenas de contas bancarias, a fim de maquiar suas ações sem que o dono sinta o dano, ou mesmo conseguindo acesso total a senhas, com as mais diversas finalidades, por meio de seus engenhosos programas. Encontramos, então, como práticas delituosas comuns dos crackers: estelionato, furto, violação de direito autoral, crimes contra a propriedade industrial, interceptação de comunicações de informática, interceptação de e-mail e crimes contra software.

---

[3]http://www.amagis.org.br/index.php?option=com_content&view=article&id=332%3Ao-combate-a-criminalidade-cibernetica-no-brasil-parametros-objetivos-de-tipicidade&catid=11&Itemid=30

O mais simples dos crimes cibernéticos é o estelionato, que é caracterizado pela fraude causada pelo agente contra a vitima. Vejamos sua definição, na visão do ilustríssimo Procurador de Justiça em Minas Gerais, Grecco (2011, p.232):

> Sendo a fraude o ponto central do delito de estelionato, podemos identifica-lo, outrossim, por meio dos seguintes elementos que integram a sua figura típica: a) conduta do agente dirigida finalisticamente à obtenção de vantagem ilícita, em prejuízo alheio; b) a vantagem ilícita pode ser para o próprio agente ou terceiro; c)a vitima é induzida ou mantida em erro; d) o agente se vale de um meio artificio, ardil ou qualquer outro meio fraudulento para a consecução do seu fim.

Esta definição já nos mostra o método de ação do agente, sendo esta a utilização de falsa identificação e, com isso, entrando em contato com a vítima de forma virtual, faz com que esta seja mantida em erro, e, usando de sua ignorância, transmita as informações necessárias, tal qual numeração documental ou senhas, a fim de fazer-se valer destas informações para trazer para si vantagem ilícita.

O crime que podemos considerar como um dos mais elaborados dentre os crimes cibernéticos é o de interceptação de comunicações de informática. Seu método de ocorrência pode se dar pela implantação de programas espiões no computador da vitima, seja isso feito de forma direta ou indireta pelo agente, com a finalidade de receber toda e qualquer informação a respeito de movimentações bancárias ou armazenamento de dados.

Tem por finalidade, quanto à intercepção dos dados, tirar vantagem por meio de chantagem contra a vítima, ameaçando expor situações de sua intimidade, ou mesmo vender tais dados aos interessados, ou simplesmente expor ao público o segredo alheio. Adianto-me dizendo que já existe legislação, ainda que escassa, vigendo a respeito deste disposto. (Lei Federal nº 12.737, de 2012)

O grau de elaboração do crime de interceptação de informação não se compara à engenhosidade tramada por Kevin Mitnick[4], que consistia no furto de um centavo de cada transação bancaria de seu banco alvo; isso lhe rendeu cerca de 80 milhões de dólares. Em virtude do alto valor arrecadado, Mitnick foi preso pela policia norte americana e cumpriu cinco anos de prisão. Existem também delitos cometidos para atingir de forma psicológica a vitima, sejam estes: calúnia, injúria, difamação, discriminação e ameaça. Ao contrário do primeiro grupo de crimes citados, temos neste um tipo alternativo de agentes, pois não são, muitas vezes,

[4]http://www.tecmundo.com.br/seguranca/17833-os-ladroes-do-seculo-xxi.htm

grandes entendedores de informática mas sim pessoas comuns que acabam por cometer tais delitos de forma insensata, e com total ignorância da consequência de seu ato.

4.2 Dos crimes contra a pessoa

Calúnia, injúria, e difamação são os três tipos penais que constituem os chamados crimes contra a honra. Para entender seu alvo, devemos estar cientes do que é a honra. Latif (2007, p.41) a conceitua honra como: “Conjunto de atributos morais, físicos e intelectuais da pessoa, que lhe conferem autoestima e reputação. Quando tratamos de autoestima, falamos de honra subjetiva. A reputação está relacionada com a honra objetiva”**.**

Colocando-os em meio à internet, podemos considerar, então, este com um dos maiores ocorrentes em redes sociais, quando desafetos trocam acusações e ofensas, ocorrendo pelo uso em sua maioria, situações fictícias.

Outro crime delito destacado na esfera psicológica é a ameaça. Em virtude do falso anonimato gerado na internet, as pessoas que buscam prejudicar outrem a utiliza para promover suas ameaças, ignorando o fato de que em caso investigação policial, há meios de o anônimo ser localizado.

Em pauta também devo citar o *bullying*, termo referente ao assédio psicológico sofrido por indivíduos em virtude de diferenças físicas ou sociais, e que pode acarretar em sérios danos mentais a vitima, gerando ate suicídios ou massacres em massa.

Assim como no crime de ameaça, o agente pode utilizar a internet para assediar sua vitima e se valer do anonimato referido ou ate mesmo aglomerar vários agentes que não medem suas atitudes a fim de prejudicar seu alvo.

4.3 Pedofilia

Por fim, infelizmente, há de se destacar a grande ocorrência dos crimes de pedofilia. Rogerio Grecco (2011, p.540) entende que:

> De todos os crimes que nos causam asco, que nos enojam que nos fazem ter um sentimento de repulsa, sem duvida alguma, a pedofilia se encontra no topo da lista. E fazendo uma ligação com o tema estudado, completa: Ultimamente, o mundo tem convergido esforços no sentido de combater os pedófilos que utilizam, principalmente, da internet para atrair suas vitimas inocentes.

Tomando um foco diferente do exposto, Demócrito Reinaldo Filho (2003, p.174) cita:

> Os pedófilos têm se utilizado da Internet para trocar fotos e imagens que descrevam práticas sexuais com menores pré-púberes, não somente para simplesmente extravasar suas (doentias) fantasias sexuais e até mesmo para difundir uma espécie de filosofia pedófila.

O Estatuto da Criança e do Adolescente, em seu art. 241-A, tipifica a conduta de oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente. As duas visões apresentadas se completam e somadas a já colocação do E.C.A. em tipificar a atividade virtual vemos um indício de conscientização a respeito da necessidade de tipificar as condutas *online.*

5 Formas utilizadas para suprir lacunas legais

Em nosso ordenamento jurídico há lacunas legais, isto é, situações que ainda não estão sendo abrangidas pela norma jurídica. Para supri-las, podemos nos valer de fontes subsidiarias de Direito, sendo a mais comum, a analogia.

Fernando Capez (2011, p.53) conceitua analogia como “a aplicação em uma hipótese não regulada por lei disposição relativa a um caso semelhante” e completa “que na analogia, o fato não é regido por qualquer norma e, por essa razão, aplica-se uma de caso análogo”.

Esmiuçando então o conceito elaborado por Capez, vemos que a analogia é o uso de uma norma com mesmo objetivo em um caso ainda não vislumbrado legalmente, capacitando então para alguns casos de crimes cibernéticos a aplicação do texto expresso no Código Penal. Mas como é sabido, dentro do código penal brasileiro, não se pode fazer o uso da analogia quando se tratar de algo que prejudique judicialmente o réu, então se vê a dificuldade encontrada pelo Ministério Publico para enquadrar a tipificação penal dos crimes cibernéticos.

Para então evitar esse embate e trazer para a sociedade o sentimento de segurança para a utilização da rede, diminuindo a incerteza quanto à punibilidade dos agentes, e fixando penas justas para criminosos cibernéticos, necessitamos da ampliação destas leis, e considerando a lentidão legislativa de nosso país, entendo que o quanto antes se der inicio a essa ampliação, melhor será os resultados sociais.

Seguindo o conhecimento ministrado no inicio de qualquer faculdade de Direito, e dando voz a Maria Helena Diniz (2009, p.294) “O processo legislativo vem a ser um conjunto de fases constitucionalmente estabelecidas, pelas quais há de passar o projeto de lei, ate sua transformação em lei vigente”. O processo legislativo está localizado a partir do art. 59 de nossa Carta Magna.

Atualmente no Congresso Nacional tramita o Projeto de Lei nº 2126/11[5], chamado de Marco Civil da Internet. Seu texto já esta em discussão a cerca de dois anos e foi anexado junto a outro projeto de lei, sendo este o de número 5403/01, oque nos sugere a demora demandada dentro do processo legislativo nacional.

6 Leis já existentes a respeito da matéria estudada

Mudando de patamar, temos os textos legais que já dispõem à respeito de crimes cometidos por meio da internet, como o já citado texto do artigo 241-A do Estatuto da Criança e do Adolescente que trata de tipificar a conduta de pedofilia por meios virtuais, encontramos também a Lei Federal nº 12.735, de 2012 cujo texto é composto de quatro artigos, sendo de maior destaque o 4º, que o artigo que regulamenta a instalação de delegacias especializadas em combate a crimes cibernéticos. Assunto este que será tratado posteriormente em tópico específico.

E em conjunto a lei supracitada, foi promulgada também a Lei Federal nº 12.737, de 2012, norma esta popularmente conhecida como Lei Carolina Dieckmann.

6.1 Lei 12.737 de 30 de Novembro de 2012, a popular Lei Carolina Dieckmann

Em abril de 2012 foi externada, por meio da imprensa, a extorsão sofrida pela atriz Carolina Dieckmann, que após ter seu computador pessoal invadido por

[5]http://edemocracia.camara.gov.br/web/marco-civil-da-internet

crackers, estes encontraram, em meio a seus dados, fotos de momentos íntimos da atriz.

Seguinte a este fato, fortaleceu-se uma critica ao legislativo nacional pela inépcia frente à insegurança no ambiente virtual, e este clamor social deu origem a esta que foi a norma referente a crimes cibernéticos mais destacados dentre as demais já mencionadas.

A título de curiosidade, a Lei Federal nº 12.735 de 2012 teve seu processo legislativo iniciado no ano de 1999. Em contrapartida, o projeto de lei que culminou na Lei Federal nº 12.737, fora apresentado em 29 de novembro de 2011, o que nos deixa claro a influência da mídia e do clamor social na celeridade de produção legislativa em nosso país.

Seu texto lei é composto por quatro artigos, sendo referentes à tipificação penal, tramite do processo criminal, falsificação de cartões bancários e interrupção de serviços ligados à rede de telecomunicações.

Apesar de sua pequena abrangência, podemos considerar esta como a primeira lei com real cunho de penalizar aqueles que cometem crimes cibernéticos nos seguintes termos:

> Art. 154-A. 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 vulnerabilidade para obter vantagem ilícita:
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.

Fica clara então a ambientação virtual no tipo apresentado, assegurando então seu cunho de criminalizar a ação do cracker.

Porém, mesmo com ocorrendo esta ambientação, Cabette (2013, p.3493) defende que:

> O bem jurídico tutelado é a liberdade individual, eis que o tipo penal está exatamente inserido no capítulo que regula os crimes contra a liberdade individual [...] Pode-se afirmar também que é tutelada a privacidade das pessoas (intimidade e vida privada), bem jurídico albergado pela Constituição Federal em seu artigo 5º. X.

Então se percebe que apesar da ambientação virtual, o tipo penal ainda segue protegendo bens externos à rede mundial de computadores, fato este que já supera o uso de analogia ao atual código penal brasileiro, vez que já elimina possível matéria de discussão difusa ao mérito objetivado em processos penais.

7 Necessidade da atuação social no inicio do combate

Levantar a discussão sobre a criação das leis específicas nos coloca frente a outro ponto importante acerca do tema, que é a questão da atuação policial em meio às ações efetuadas pelos criminosos cibernéticos. Levando em consideração que a criação de delegacias especializadas no combate a crimes cibernéticos se tornou obrigatório somente no ano de 2012, no texto da Lei Federal nº 12.735, de Novembro de 2012, nosso pais ainda não se encaixa no perfil de fiscalização ostensiva, que é a atuação policial de forma visível, mostrando para a sociedade que este presente, tendo com o objetivo inibição da ação criminosa.

Dependemos então do combate posterior, que é aquele com que a vitima se vê diante de uma possibilidade lesiva e denuncia às autoridades a prática delituosa. Porem a inexistência das normas específicas nos traz aos dizeres de Carneiro (2012, p.99):

> Ocorre que atualmente a maioria dos crimes praticados ainda não são divulgados seja por conta da não disseminação dessas informações ou pela falta de denuncia, como, por exemplo: grandes empresas evitam a divulgação sobre possíveis ataques virtuais ou mesmo invasões para não demonstrarem fragilidade quanto à segurança, e quanto às pessoas físicas vemos que por falta da devida punibilidade aos infratores e a falta de mecanismos de denuncia apesar de já existirem as vítimas acabam não denunciando o que facilita a propagação desses crimes.

Então, seguindo seu entendimento, caso se torne publica a punibilidade dos criminosos referidos, a população começara a denunciar tais praticas com maior frequência, e em conjunto com a criação de leis especificas que punam criminosos cibernéticos, poderemos então combater e diminuir tais práticas até que a estruturação física policial seja completada e passe a exercer o policiamento ostensivo, que é a chave para a tranquilidade social.

Segue a baixo uma lista com informações acerca das delegacias especializadas no combate de crimes cibernéticos na região sudestes e distrito federal, disponibilizados no site safernet[6].

Brasília	DICAT - Divisão de crimes de Alta tecnologia	Setor Áreas Isoladas Sudoeste, Bloco D - Brasília (DF).	(61) 3462-9531

[6]http://www.safernet.org.br/site/prevencao/orientacao/delegacia

Belo Horizonte	DERCIFE - Delegacia Especializada de Repressão a Crimes contra Informática e Fraudes Eletrônicas	Av. Antônio Carlos, 901, Lagoinha - Belo Horizonte (MG)	(31) 3201-5892
Rio de Janeiro	DRCI - Delegacia de Repressão aos Crimes de Informática	Rua da Relação, 42, 8º andar, Centro - Rio de Janeiro (RJ)	(21) 3399-3201
São Paulo	DIG/DEIC – Delegacia de Delicos Cometidos por Meios Eletrônicos	Av. Zaki Narchi, 152 - Carandiru (SP)	(11) 2221-7030
Vitória	Delegacia de Repressão a Crimes Eletrônicos	Av. Nossa Senhora da Penha, 2290, Santa Luiza, Vitória (ES)	(27) 3137-26077

8 Considerações Finais

Em um primeiro momento, mostrei o ambiente e as fragilidades sociais que envolvem o meio utilizado para as praticas delituosa, afirmando que a falta de informação da sociedade é utilizado como arma para *crackers*.

Após a ambientação, explanei sobre as praticas delituosas mais ocorrentes dentro do meio virtual, mostrando que a forma silenciosa de atuação do criminoso também age como um artificio para a concretização de seu dano.

Citando os métodos utilizados para punir criminosos cibernéticos, abordei sobre o enquadramento analógico, vez que ainda não vislumbramos normas especificas que tipificam as condutas, o que torna a punibilidade difusa, deixando puramente a cargo do Poder Judiciário, sem a devida assistência legal, penalizar. E abordei, ainda, a dificuldade que se da na fiscalização e combate a tais crimes.

Enlaçando, então, os pontos sutra citados, chegamos ao que atrai tanto os criminosos para o meio virtual, que são: a ignorância social, anonimato e por fim a falta da legislação especifica que iniba a atuação criminosa por meio da punibilidade.

Visto o grau de elaboração intelectual das praticas e do conhecimento especifico empregado pelos criminosos podemos considerar que estes o fazem, pela facilidade de agir, e não pela necessidade, tal qual alguém que comete furto para

sustentar sua família, e saindo da questão de necessidade, temos grandes traficantes que, mesmo esbanjando sua riqueza, não podem se mostrar publicamente, por terem a policia em seu encalço.

Isto me leva a crer que com a legislação especifica, e com isso a exposição da punibilidade aplicada no meio prático, inibirá a atuação dos criminosos cibernéticos, pois ele colocará na balança o benefício ganho com a ação delituosa e a penalização aplicável. Além de, como já abordado, uma vez que for fixada a punição, a sociedade se sentirá mais segura para denunciar novos golpes que venham a ocorrer na rede. Isto, então, acarretará na diminuição significativa da quantidade de criminosos cibernéticos, facilitando o trabalho estatal na identificação e investigação daqueles que ainda persistirem no meio criminoso.

LAWS AGAINST NETWORK'S INSECURITY

Abstract

This article consists of a study about the need for legislative specification regarding crimes that occur in virtual environments, such as the Internet or software, used to cause material or psychological damage to the victims, as well as giving information about the most common crimes and explaining legal texts already in validity in Brazil that refer to the subject. The documents used were: online print; doctrines; and the official websites of the Supremo Tribunal Federal and Superior Tribunal de Justiça. It is noted that Brazilian law efficiently provides means to play its vocational role of giving everyone their due.

Keywords: Cybercrimes. Scams on the Internet. Modern Law. Internet Security

Referencias

AREF, Omar Abdul Lafif. Dos crimes contra a honra. **Âmbito Jurídico**, Rio Grande, v.10, n. 41, maio 2007. Disponível em: <http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=1829>. Acesso em: 24 out. 2013.

AZEVEDO, Robson Barbosa de. **O combate à criminalidade cibernética no Brasil**: Parâmetros Objetivos de Tipicidade. Disponível em: <http://www.amagis.org.br/index.php?option=com_content&view=article&id=332%3Ao-combate-a-criminalidade-cibernetica-no-brasil-parametros-objetivos-de-tipicidade&catid=11&Itemid=30> Acesso em: 22 de out. 2013.

BARROS, Thiago. **Internet completa 44 anos**; relembre a história da web. Disponível em:<http://www.techtudo.com.br/artigos/noticia/2013/04/internet-completa-44-anos-relembre-historia-da-web.html> Acesso em: 29 out. 2013.

BBC, **Brasil cai duas posições em ranking global de internet**. Disponível em <http://www.bbc.co.uk/portuguese/noticias/2010/03/100325_rankinginternet.shtml> Acesso em: 22 de out. de 2013.

BRASIL. Constituição (1988). **Constituição da Republica Federativa do Brasil.** Brasília, 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>

_____. Lei Nº 11.829, de 25 de Novembro de 2008. Altera a Lei nº 8.069, de 13 de julho de 1990 - Estatuto da Criança e do Adolescente, para aprimorar o combate à produção, venda e distribuição de pornografia infantil, bem como criminalizar a aquisição e a posse de tal material e outras condutas relacionadas à pedofilia na internet. **Diário Oficial [da] Republica Federativa do Brasil**, Poder Executivo, Brasília, DF, 25 de Novembro de 2008. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/lei/l11829.htm>

_____. Lei Nº 12.735, de 30 de Novembro de 2012. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências. **Diário Oficial [da] Republica Federativa do Brasil**, Poder Executivo, Brasília, DF, 30 de Novembro de 2012. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12735.htm>

_____. Lei Nº 12.737, de 30 de Novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. **Diário Oficial [da] Republica Federativa do Brasil**, Poder Executivo, Brasília, DF, 30 de Novembro de 2012. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.html

CABETTE, Eduardo Luiz Santos. Primeiras impressões sobre a Lei nº 12.737/12 e o crime de invasão de dispositivo informático. **Jus Navigandi**, Teresina, ano 18, n. 3493, 23 jan. 2013. Disponível em: <http://jus.com.br/artigos/23522>. Acesso em: 28 out. 2013.

CÂMARA DOS DEPUTADOS. **Marco Civil da Internet**. Disponível em: <http://edemocracia.camara.gov.br/web/marco-civil-da-internet>. Acesso em: 22 out de 2013.

CARNEIRO, Adeneele Garcia. Crimes virtuais: elementos para uma reflexão sobre o problema na tipificação. **Âmbito Jurídico**, Rio Grande, v. 15, n. 99, abr. 2012. Disponível em: <http://www.ambito-juridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=11529>. Acesso em: 23 out. 2013.

CAPEZ, Fernando. **Curso de Direito Penal:** Parte Geral. 15. ed. São Paulo: Saraiva, 2011. 645 p.

DINIZ, Maria Helena. **Compêndio de introdução à ciência do direito.** 20. ed. São Paulo: Saraiva, 2009. 595 p.

GRECO, Rogério. **Curso de Direito Penal:** Parte Especial. 8. ed. Niteroi: Impetus, 2011. 808 p.

KARASINSKI, Lucas. **Os Ladrões do Século XXI**. Disponível em: <http://www.tecmundo.com.br/seguranca/17833-os-ladroes-do-seculo-xxi.htm> Acesso em: 22 de out. 2013.

MOURA, Pamela Aline Rocha. **Crime Cibernético e Seus Aspectos no Universo Jurídico.** 2012. 41 f. TCC (Graduação) - Curso de Ciências Jurídicas e Sociais, Universidade Presidente Antônio Carlos, Barbacena, 2012.

REINALDO FILHO, Demócrito. **O crime de divulgação de pornografia infantil pela Internet:** Breves comentários à Lei nº 10.764/03. **Jus Navigandi**, Teresina, ano 8, n. 174, 27 dez. 2003 . Disponível em: <http://jus.com.br/artigos/4680>. Acesso em: 24 out. 2013.

TZU, Sun. **A Arte da Guerra.** Porto Alegre: L&PM, 2000. 152 p