INSTITUTO VALE DO CRICARÉ

FACULDADE VALE DO CRICARÉ

CURSO DE DIREITO

THAMYRES ALVES ZANDOMENEGO

“CRIMES VIRTUAIS: UMA ANÁLISE DA EVOLUÇÃO LEGISLATIVA NO BRASIL”

SÃO MATEUS

2015

THAMYRES ALVES ZANDOMENEGO

“CRIMES VIRTUAIS: UMA ANÁLISE DA EVOLUÇÃO LEGISLATIVA NO BRASIL”

Trabalho de conclusão de Curso apresentado ao Curso de Direito da Faculdade Vale do Cricaré, como requisito parcial para obtenção do grau de bacharel em Direito.
Orientador: Prof. Rui Edsiomar Alves de Souza.

SÃO MATEUS

2015

THAMYRES ALVES ZANDOMENEGO

CRIMES VIRTUAIS: UMA ANÁLISE DA EVOLUÇÃO LEGISLATIVA NO BRASIL

Trabalho de Conclusão de Curso apresentado ao Curso de Direito da Faculdade Vale do Cricaré, como requisito parcial para obtenção do grau de bacharel em direito.

Aprovado em ____ de dezembro de 2015.

BANCA EXAMINADORA

_____

PROF. RUI EDSIOMAR ALVES DE SOUZA

FACULDADE VALE DO CRICARÉ

ORIENTADOR

_____

PROF.

FACULDADE VALE DO CRICARÉ

_____

PROF.

FACULDADE VALE DO CRICARÉ

Dedico este trabalho a minha família, por tudo que fizeram por mim e pelo apoio dado durante esses cinco anos.

Primeiramente, agradeço a DEUS.

Ao meu orientador Rui Edsiomar Alves de Souza, pelo incentivo, apoio e atenção dispensada no auxílio às atividades e discussões acerca do andamento desta Monografia de Conclusão de Curso.

"As nuvens mudam sempre de posição, mas são sempre nuvens no céu. Assim devemos ser todo dia, mutantes, porém, leais com o que pensamos e sonhamos;"

Paulo Baleki

RESUMO

O objeto a que se destina essa Monografia é apresentar, e também informar, que os crimes virtuais estão se disseminando de uma forma nunca antes constatada, e que os Estados tem o dever de criar ferramentas precisas para impedir a prática de tais ilícitos. Há que se destacar a criação e aprovação de leis específicas, a exemplo das Leis nº 12.737/2012 e nº 12965/2014 (Marco Civil da Internet), que dispõe sobre a tipificação criminal de delitos informáticos, referentes ao assunto que estão eclodindo em nosso país que, por muitos anos, ficou à margem desse tipo de legislação. Não podendo deixar de falar também no projeto de lei nº 225/15 que está prestes a ser aprovado. Por derradeiro, porém, não menos importante, há que se salientar que, apesar das leis e dispositivos legais à espécie, todo usuário precisa tomar as devidas precauções de segurança quando entra em contato com a rede mundial de computadores, pois, a exemplo de sua vida real, não devemos baixar a guarda, nem admitir a presença de pessoas ou mesmo hipóteses não confiáveis para não sermos vítimas dos famigerados crimes virtuais.

Palavras-chave: Internet. Evolução. Crimes Virtuais. Lei. Usuário

LISTA DE ABREVIATURAS E SIGLAS

ADPF - Arguição de Descumprimento de Preceito Fundamental

CERT Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança

CRACKER - Termo usualmente utilizado para designar quem pratica a quebra (ou cracking) de um sistema de segurança

COOKIE - Grupo de dados trocados entre o navegador e o servidor de páginas eletrônicas, colocado num arquivo (ficheiro) de texto criado no computador do utilizador

DDoS Distributed Denial of Service DoS Denial of Service

DEEP WEB – Termo utilizado para designar o submundo da internet ECA – Estatuto da Criança e do Adolescente

E-COMMERCE – Comércio realizado por meio virtual/eletrônico HACKER – São indivíduos que elaboram e modificam softwares e hardwares de computadores, seja desenvolvendo funcionalidades novas ou adaptando as antigas

FBI Federal Bureau of Investigation

HARD DISK – Disco interno do computador, aonde se gravam e armazenam todos os tipos de informações

IP Internet Protocol

NCP - Network Control Protocol (Controle de Protocolo da Rede)

PASSWORD - Senha SITE – (sítio) Endereço eletrônico comumente utilizado na internet

SaferNet Central Nacional de Denúncias de Crimes Cibernéticos

SPAM – Termo usado para referir-se aos e-mails não solicitados, que geralmente são enviados para um grande número de pessoas

SSL Secure Sockets Layer

STF – Supremo Tribunal Federal

STJ – Supremo Tribunal de Justiça

TCP/IP - Transmission Control Protocol/Internet Protocol (Transmissão do Protocolo de Controle/Protocolo da Internet)

WWW - World Wide Web

LISTA DE ILUSTRAÇÕES

LISTA DE GRÁFICOS

SUMÁRIO

INTRODUÇÃO

A presente monografia analisou o desenvolvimento e a criminalização do mundo virtual, seu surgimento, casos atuais, as leis e, em especial, sua atuação no Brasil, com a análise dos principais crimes e leis e, quanto à conclusão, fez uma análise mais abalizada no tocante a evolução legislativa dessa nova modalidade de atuação.

O intuito de se escolher tal tema se dá pela constante e rápida evolução que existe nessa área e, em especial, pela crescente onda de ilícitos provenientes do mundo virtual. Com isso, os direitos em concreto são atingidos, criando, no espaço virtual, uma “oportunidade” real para os fora da lei.

Tais práticas delituosas podem ocorrer das mais variadas formas, desde os tradicionais furtos e roubos, passando pela extorsão, crimes contra a honra, dentre outras formas comuns de ilícitos.

O assunto em tela tem a sua importância na medida em que tais crimes estão apenas em seu nascedouro, ou seja, são embriões de outros mais perigosos e devastadores que estão por vir.

A atividade da informática está incutida nas principais áreas dos setores cruciais de todo o mundo. A pergunta antes feita por centros de pesquisas aos entrevistados era: “Quantas horas por dia você passa conectado na internet?” hoje deve ser readequada para “Quantas horas por dia você não passa conectado na internet?”, pois todos estão “on-line” diuturnamente, o que nós traz momentos úteis e importantes, porém, também vários inconvenientes e infortúnios, como por exemplo falhas na conexão ou, de uma forma mais grave, sermos vítimas de crimes virtuais.

Conhecedor de todo o ocorrido, porém, menos ágil e rápido que o mundo tecnológico, o Governo Nacional tenta editar leis para frear essa onda que já dura há muito tempo, porém, a cada passo legal dado, tantos outros são dados ilegalmente pelos ciber infratores, o que torna as leis, em seu berço, já obsoletas e ineficazes.

Ressaltam-se as recentes leis, como por exemplo, as leis: nº 12.737de 2012, nº 12.965 de 2014, que somam um grande progresso no tocante a evolução legislativa da internet no Brasil.

Há que lembrar, também, que está em plena discussão, prestes a ser aprovado, o projeto de lei nº 225/2015 que, prevê alterações na lei do Marco Civil, como por exemplo, em matérias que versam sobre o direito ao esquecimento e a remoção de conteúdos da internet, conteúdo polêmico que está em discussão.

No tocante à metodologia, a mais amplamente utilizada no referido trabalho foi a denominada histórica, através da qual se pôde verificar a evolução virtual.

Igualmente, foram feitas pesquisas em jurisprudências, doutrinas, livros e sítios especializados, bem como em casos concretos atuais.

Por derradeiro, o trabalho em tela propõe uma análise desse novo mundo virtual a ser desbravado e da consequência evolução legislativa no Brasil.

1 HISTÓRICO DOS CRIMES VIRTUAIS

Existem diversos tipos de crimes virtuais, sendo difícil precisar quando houve a primeira ocorrência, porém há um consenso entre os autores de que os crimes virtuais têm origem na década de 60, segundo afirma Ferreira,

> Ulrich Sieber, professor da Universidade de Würzburg e grande especialista no assunto, afirma que o surgimento dessa espécie de criminalidade remonta à década de 1960, época em que aparecem na imprensa e na literatura científica os primeiros casos de uso do computador para a prática de delitos, constituídos, sobretudo por manipulações, sabotagens, espionagem e uso abusivo de computadores e sistemas, denunciados, sobretudo em matérias jornalísticas. Somente na década seguinte é que iriam iniciar-se os estudos sistemáticos e científicos sobre essa matéria, com o emprego de métodos criminológicos, analisando-se um limitado número de delitos informáticos que haviam sido denunciados, entre os quais alguns casos de grande repercussão na Europa por envolverem empresas de renome mundial, sabendo-se, porém da existência de uma grande cifra negra não considerada nas estatísticas. (FERREIRA, 2005)

Diferentemente do que muitas pessoas pensam, a origem dos crimes cibernéticos podem não estar diretamente relacionado com o surgimento da internet, pois de acordo com Assunção,

> Em novembro de 1961, desenvolvedores do MIT (Instituto de Tecnologia de Massachussets) demonstravam o seu sistema experimental compatível com gerenciamento de tempo, o que permitia quatro usuários trabalhando em terminais rodar programas de outros usuários. No final dos anos 60, terminais conectados por modem poderiam ser facilmente invadidos, já que, na época, ninguém se preocupava em colocar senhas. (ASSUNÇÃO, 2008)

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 à 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 Mitnick, um dos hackers mais famosos do planeta e que hoje trabalha para o governo americano na área da segurança da informação.

Apesar dos crimes virtuais remontarem ao início dos anos 60, as autoridades passaram a dar mais importância a esse tipo de crime, somente na década de 80

quando as ações dos criminosos aumentaram consideravelmente, conforme afirma Ferreira,

> A evolução das técnicas nessa área e a sua expansão foram acompanhadas por aumento e diversificação das ações criminosas, que passaram a incidir, a partir dos anos 80, em manipulações de caixas bancários, pirataria de programas de computados, abusos nas telecomunicações, etc., revelando uma vulnerabilidade que os criadores desses processos não haviam previsto e que carecia de uma proteção imediata, não somente através de novas estratégias de segurança no seu emprego, mas também de novas formas de controle e incriminação das condutas lesivas. (FERREIRA, 2005)

A primeira prisão de um criminoso virtual ocorreu apenas em dois de novembro de 1988, quando o estudante Robert Tappan Morris Junior, foi condenado a cinco anos de prisão por ter transmitido um worm que contaminou cerca 6.000 computadores que usavam sistema operacional Unix.

Um dos criminosos virtuais mais famosos do mundo foi Kevin Mitnick, que ficou conhecido por burlar sistemas de telefonia, além de roubar um software secreto de uma empresa e crakear sistemas de informática do FBI. Kevin foi preso em 1995 e libertado em 2000, ficando em liberdade condicional durante três anos. Atualmente Kevin trabalha como consultor de segurança e participa de palestras em eventos pelo mundo.

No Brasil, de acordo com Nogueira (2008), o primeiro caso de crime cibernético ocorreu em 1997, “quando um analista de sistemas acusado de enviar centenas de e-mails com conteúdo erótico, juntamente com ameaças a integridade de uma jornalista, foi condenado a dar aula de informática para os novos policiais de uma Academia da Polícia Civil”.

Atualmente os crimes cibernéticos têm tido uma grande repercussão, principalmente os ligados a invasão de sites de grandes corporações e do governo, por um grupo de crakers que justificam os seus atos como uma resposta ao que eles consideram uma violação dos seus direitos.

Esses acontecimentos ocorreram após a prisão do australiano Julian Assange, cofundador do site wikileaks, acusado de divulgar documentos sigilosos do governo norte americano e, da prisão do fundador do site de gerenciamento de arquivos Megaupload, Kim Schmitz, acusado de pirataria on-line. Outro crime que vem tendo grande repercussão é a exposição da intimidade das celebridades na internet.

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, leis relativas à competência do Estado sobre questões de informática.

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.

1.1 CONCEITOS DE CRIMES VIRTUAIS

Para entender o que é um crime cibernético é preciso primeiramente entender o conceito de crime segundo a legislação brasileira, para isso a Lei de introdução do Código Penal define crime como “a infração penal que a lei comina pena de reclusão ou de detenção, quer isoladamente, quer alternativa ou cumulativamente com a pena de multa; contravenção, a infração penal a que a lei comina, isoladamente pena de prisão simples ou de multa, ou ambas: alternativa ou cumulativamente”, ou seja, pela ótica da legislação brasileira crime é qualquer infração em que a lei enseja pena de reclusão ou de detenção, que pode ser alternativa ou cumulativamente com pena de multa.

O conceito de Crimes Cibernéticos também conhecidos como Cibercrimes, crimes virtuais, crimes da informática, crimes informáticos, é muito amplo e tem as mais variadas descrições.

Uma acepção muito ampla de Crimes Cibernéticos é dada por Ferreira,

> As várias possibilidades de ação criminosa na área de informática, assim entendida no seu sentido lato, abrangendo todas as tecnologias de informação, dos processamentos e transmissão de dados, originaram uma forma de criminalidade que, apesar da diversidade de suas classificações, pode ser identificada pelo seu objeto ou pelos meios de atuação, os quais lhe fornecem um dominador comum, embora com diferentes denominações nos vários países ou nos diferentes autores. (FERREIRA, 2005)

Segundo Ferreira (2002) “apesar das diferentes denominações o conceito de Crimes Cibernéticos pode ser identificado pelo seu objeto ou pelos meios de atuação”, já Rosa tem uma definição mais específica para Cibercrimes,

> É a conduta atente contra o estado natural dos dados e recursos oferecidos por um sistema de processamento de dados, seja pela compilação, armazenamento ou transmissão de dados, na sua forma, compreendida pelos elementos que compõem um sistema de tratamento, transmissão ou armazenagem de dados, ou seja, ainda, na forma mais rudimentar; 2. o „Crime de Informática" é todo aquele procedimento que atenta contra os dados, que faz na forma em que estejam armazenados, compilados, transmissíveis ou em transmissão; 3. nos crimes de informática, a ação típica se realiza contra ou pela utilização de processamento automático de dados ou a sua transmissão. Ou seja, a utilização de um sistema de informática para atentar contra um bem ou interesse juridicamente protegido, pertença ele à ordem econômica, à integridade corporal, à liberdade individual, à privacidade, à honra, ao patrimônio público ou privado, à Administração Pública, etc. (ROSA, 2002)

Do ponto de vista jurídico Crimes Virtuais podem ser definidos, segundo Daoun e Lima (2012), "como ação típica, antijurídica, e culpável, cometida contra ou pela utilização de processamento automático de dados ou sua transmissão".

Atualmente no ramo jurídico alguns doutrinadores se posionam 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 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". (crimes da informática – Remy Gama FilhoEditora: CopyMarket.com, 2000)

1.2 PRINCÍPIO DA LEGALIDADE

Também conhecido como princípio da reserva legal, o princípio da legalidade, consagrado no artigo 5º, inciso II da Constituição Federal "ninguém será obrigado a fazer ou deixar de fazer alguma coisa senão em virtude de lei", é um dos princípios mais importantes do ordenamento jurídico Pátrio e um dos sustentáculos do Estado de Direito.

Segundo Jesus,

> O Princípio da Legalidade (ou de reserva legal) tem significado político, no sentido de ser uma garantia constitucional dos direitos do homem. Constitui a garantia fundamental da liberdade civil, que não consiste em fazer tudo o que se quer, mas somente aquilo que a lei permite. À lei e somente a ela

> compete fixar as limitações que destacam a atividade criminosa da atividade legítima. Esta é a condição de segurança e liberdade individual. Não haveria, com efeito, segurança ou liberdade se a lei atingisse, para puni-los, condutas lícitas quando praticadas, e se os juízes pudessem punir os fatos ainda não incriminados pelo legislador. (JESUS, 1991)

Tal princípio visa garantir que somente a lei determine o que é uma conduta ilícita e que somente em virtude dela uma pessoa possa ser obrigada a fazer ou deixar de fazer alguma coisa, ou seja, se uma lei não proíbe alguma conduta o cidadão está livre para praticá- la sem ser punido por causa disso.

Capez ensina que,

> Nenhuma outra fonte subalterna pode gerar a norma penal, uma vez que a reserva de lei proposta pela Constituição é absoluta, e não meramente relativa (...) somente a lei, na sua concepção formal e estrita, emanada e aprovada pelo Poder Legislativo, por meio de procedimento adequado, pode criar tipos e impor penas. (CAPEZ, 2011)

De acordo com o artigo 5º, inciso XXXIX da Constituição Federal “Não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal”, ou seja, de acordo com o princípio da legalidade alguém só poderá ser punido, se anteriormente ao fato praticado existir lei que o considere como crime, ainda que o fato seja imoral, antissocial ou danoso não haverá possibilidade de punir o autor.

Para que haja um crime é necessário que uma lei anterior o defina como tal, essa prerrogativa aliada à morosidade dos políticos brasileiros em tipificar condutas em desacordo com valores morais e éticos da nossa sociedade acaba por criar um precedente de impunidade, estimulando condutas danosas ao bem estar social.

1.3 TIPICIDADE PENAL

A tipicidade penal é o princípio penal básico e está amparada no princípio da legalidade. Significa a descrição de uma conduta considerada proibida, para qual se estabelece uma sanção.

Mirabete conceitua tipicidade penal como sendo

> 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. (MIRABETE, 2005)

Destarte, 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.

Vale lembrar que o uso de analogia não pode ser considerado válido, nos casos prejudiciais ao réu, como bem explica Capez,

> A aplicação da analogia em norma penal incriminadora fere o principio da reserva legal, uma vez que um fato definido em lei como crime, estaria sendo considerado como tal. Imagine considerar típico o furto de uso (subtração de coisa alheia móvel para o uso), por força da aplicação da analogia do artigo 155 do Código Penal (subtrair coisa alheia móvel com animo de assenhoramento definitivo). Neste caso, um fato não considerado criminoso pela lei passaria a sê-lo, em evidente afronta ao principio constitucional do art. 5º, XXXIX (reserva legal). A analogia in malan partem, em principio, seria impossível, pois jamais seria benéfica ao acusado a incriminação de um fato atípico. (CAPEZ, 2010).

2 DESENHO TEÓRICO E METODOLÓGICO DA PESQUISA

2.1 PROBLEMAS DA PESQUISA

Crimes virtuais são tidos como um grande problema para os juízes brasileiros, devido ao seu difícil enquadramento nas leis existentes, porém mesmo com essa dificuldade, o que os tribunais devem fazer para que as pessoas que cometam tais crimes sejam punidas?

Diante da falta de uma lei específica, quais as dificuldades que os nossos magistrados estão enfrentando para que a população brasileira não seja vítima da impunidade?

Vários projetos de lei já foram propostos, por que ainda assim não existe uma lei específica que tipifica crimes virtuais no Brasil?

A Lei nº 12.737, de 30 de novembro de 2012. Conhecida como Lei Carolina Dieckman consegue dar as respostas esperadas pela Sociedade para desestimular aqueles que abusam das facilidades tecnológicas?

A Lei nº 12.737, de 30 de novembro de 2012, entrou em pleno vigor no último dia 3 de abril de 2013, alterando o Código Penal para tipificar os crimes cibernéticos propriamente ditos (invasão de dispositivo telemático e ataque de denegação de serviço telemático ou de informação), ou seja, aqueles voltados contra dispositivos ou sistemas de informação e não os crimes comuns praticados por meio do computador.

Colateralmente equiparou o cartão de crédito ou débito como documento particular passível de falsificação, embora represente certo avanço ao tipificar crimes cibernéticos propriamente ditos, contém inúmeras deficiências e confrontos com o sistema penal e processual penal vigente, o que deve merecer a atenção dos aplicadores.

2.2 QUESTÕES A SEREM RESPONDIDAS PELA PESQUISA

O que os delegados, promotores e juízes estão fazendo para que os criminosos virtuais não fiquem impunes?

Até que ponto a falta de uma lei específica limita o poder de punição dos tribunais brasileiros?

Quais as leis e projetos existentes no ordenamento jurídico brasileiro?

O direito penal tem acompanhado a evolução criminal cibernética no país?

2.3 OBJETIVO GERAL DA PESQUISA

Analisar a difusão da internet no país e a consequente evolução de crimes virtuais. Expor quais são os motivos da impunidade típica dos crimes cibernéticos, mostrando a importância de lei tipificadora e as dificuldades enfrentadas pelos magistrados brasileiros.

2.4 OBJETIVOS ESPECÍFICOS DA PESQUISA

Identificar e relatar as características dos Crimes Virtuais que implicam na sua difícil tipificação e a na sua consequente impunidade.

Estudar a legislação existente no Brasil sobre o assunto, incluindo projetos de lei em tramitação, para poder verificar a existência ou não desses princípios.

Avaliar a viabilidade ou não de haver uma adaptação dos dispositivos existentes para a regulamentação dos crimes cometidos pela Internet.

Conceituar “crimes virtuais” e suas diferentes classificações.

Discutir conceitos como: proteção da privacidade do indivíduo, responsabilidade dos provedores, proteção à liberdade de expressão, proteção à propriedade intelectual, ciberjurisdição e mostrar sua relevância para a compreensão dos crimes virtuais.

Buscar uma maneira de conciliar o caráter democrático e de livre expressão da Internet com a necessidade de se responsabilizar os criminosos pelo cometimento de atos ilícitos.

Mostrar a importância de uma regulamentação satisfatória das atividades cometidas pela Internet para o Brasil, como meio de se manter competitivo no mercado econômico Internacional.

Mostrar que as dificuldades não são apenas legais, discorrendo sobre as limitações técnicas de investigação por parte das autoridades.

Deixar claro que a maioria dos crimes virtuais não é cometida por gênios criminosos, hackers com um conhecimento avançado de computadores, mas sim fruto de uma falta de preocupação dos indivíduos com a segurança de seus sistemas, de legislação insuficiente, e de falta de recursos por parte da policia para proceder às investigações, fatos que criam no criminoso em potencial a quase certeza da impunidade.

2.5 TIPOS DE PESQUISA

A pesquisa utilizada no projeto será a pesquisa explicativa, pois a mesma tem o objetivo de identificar os fatores que contribuem para a ocorrência de um fenômeno.

Segundo Vergara (2005) a investigação explicativa tem como principal objetivo tornar algo inteligível justificar lhe os motivos. Visa, portanto, esclarecer quais fatores contribui de alguma forma, para a ocorrência de determinado fenômeno. A pesquisa também terá características descritivas, pois visa descrever as características dos Crimes Cibernéticos.

2.5.1 Quanto aos Meios

Para a realização deste trabalho será efetuada uma pesquisa teórica, buscando-se a análise do código penal brasileiro, a doutrina, revistas jurídicas, artigos, e principalmente materiais publicados em sítios eletrônicos, tendo em vista a dificuldade de se encontrar livros sobre o assunto, pareceres ao tema proposto, com o escopo de determinar quais são esses princípios fundamentais, para uma eficaz regulamentação dos cibercrimes.

Ainda nesta pesquisa será utilizado o método dedutivo, através do estudo das legislações que tratem do tema. Também será analisado o avanço legislativo brasileiro em relação aos crimes virtuais.

2.6 TRATAMENTO DOS DADOS

Após a coleta os dados serão tratados qualitativamente, sendo feita a análise e depois a síntese dos referenciais teóricas encontradas.

2.7 RESULTADOS ESPERADOS

O trabalho tem a expectativa de analisar as mudanças e evolução legislativa e social por consequência da difusão da internet.

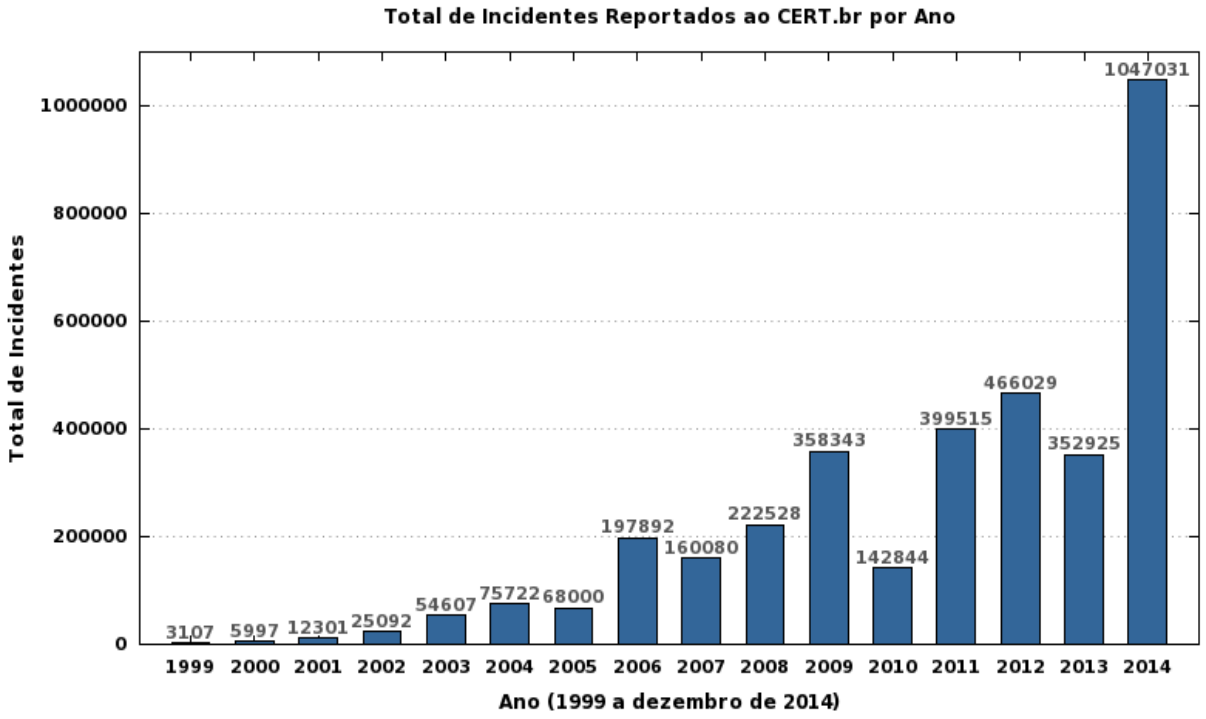
3 CRIMES VIRTUAIS

3.1 CLASSIFICAÇÃO E TIPO DE CRIMES VIRTUAIS

Há várias definições para crimes virtuais, mas a divisão de Araújo (2003) se mostra mais adequada considerando a dinâmica da internet. Para Araújo (2003), os crimescibernéticos são divididos em próprio e impróprio: “os primeiros são aqueles que somente podem ser efetivados por intermédio de computadores ou sistemas de informática, sendo impraticável a realização da conduta por outros meios. [...] impróprios admitem a prática por diversos meios, inclusive os meios informáticos”.

O gráfico 01 demonstra o número de denúncias de Crimes Cibernéticos, feitas através do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança (CERT) no período compreendido entre os anos de 1999 e 2014.

Gráfico 1: Evolução das denúncias de Crimes Virtuais



Fonte: CERT

A seguir serão abordados os crimes mais praticados.

3.2 CRIMES TIPIFICADOS PELA LEGISLAÇÃO BRASILEIRA

Dano

O Código Penal brasileiro define crime de dano como sendo a “destruição, inutilização ou deterioração da coisa alheia”. Em relação aos crimes cibernéticos o dano está relacionado com a destruição e a inutilização de arquivos de dados, seja através de vírus ou fisicamente.

Para que seja configurado o crime de dano é necessária à ocorrência de pelo menos uma das situações descrita no código penal, quer sejam: destruição, inutilização ou deterioração.

Pedofilia

Segundo artigo 241 da Lei nº. 8.069/90, também conhecida como Estatuto da Criança e do Adolescente, pedofilia é “Apresentar, produzir, vender, fornecer, divulgar ou publicar, por qualquer meio de comunicação, inclusive rede mundial de computadores ou internet, fotografias ou imagens com pornografia ou cenas de sexo explícito envolvendo criança ou adolescente”. A pedofilia torna-se um crime de informática quando os pedófilos trocam entre si materiais pornográficos através de e-mails, redes sociais e outras ferramentas da internet.

Em 2007, ao julgar um recurso especial do Ministério Público contra decisão da Justiça fluminense que entendera ser crime apenas a publicação e não apenas a mera divulgação de imagens de sexo explícito de menores, o Superior Tribunal de Justiça definiu que envio de fotos pornográficas de menores pela internet (e-mail) é crime.

O Estatuto da Criança e do Adolescente (ECA) sofreu no ano de 2008 uma atualização dada pela Lei nº. 11.829, com objetivo de “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", adequando o ECA à 13 dinâmica da internet.

Crimes contra a honra

Os crimes contra a honra aumentaram assustadoramente com a expansão da internet e o advento das novas tecnologias. Um simples recado numa rede social, como por exemplo, chamando uma pessoa de bandida, pode-se tornar uma prova irrefutável de calunia, onde milhares de pessoas são testemunhas.

Há três espécies de crimes contra a honra, sendo que os três estão previstos no Código Penal: Calúnia - Art. 138 "Caluniar alguém, imputando-lhe falsamente fato definido como crime"; Difamação - Art. 139 "Difamar alguém, imputando-lhe fato ofensivo à sua reputação"; Injúria - Art. 140 "Injuriar alguém, ofendendo lhe a dignidade ou o decoro".

Jesus difere calúnia da injúria:

> [...] enquanto a calúnia existe imputação de fato definido como crime, na difamação o fato é meramente ofensivo à reputação do ofendido. Além disso, o tipo de calúnia exige elemento normativo da falsidade da imputação, o que é irrelevante no delito da difamação. Enquanto na injúria o fato versa sobre qualidade negativa da vitima, ofendendo lhe a honra subjetiva, na difamação há ofensa à reputação do ofendido, versando sobre fato a ela ofensivo. (JESUS, 2007).

Atualmente os crimes contra a honra praticados através da internet são um grande problema para a polícia e para os juízes, devido ao fato da difícil remoção do material ofensivo e da distinção entre uma simples brincadeira e um verdadeiro crime. As diversas ferramentas como redes sociais, e-mails, blogs e chats possibilitam inúmeras formas de se praticar um crime contra a honra.

Racismo

Existem diferentes formas de discriminação racial e a internet com certeza é uma das ferramentas mais eficazes para se praticar um crime de racismo, graças às redes sociais, emails, chat entre outros.

Para Bulos,

> Racismo é todo e qualquer tratamento discriminador da condição humana em que o agente dilacera a autoestima e o patrimônio moral de uma pessoa ou de um grupo de pessoas, tomando como critérios raça ou cor da pele, sexo, condição econômica, origem, etc. (BULOS, 2003)

A Constituição da República Federativa do Brasil no seu artigo XLII prevê que a “prática do racismo constitui crime inafiançável e imprescritível, sujeito à pena de reclusão, nos termos da lei”.

Apesar de todas as previsões legais os crimes de discriminação racial ainda são comuns na nossa sociedade e a difícil identificação do autor de um crime praticado através da internet faz com que alguns criminosos saiam impunes.

Violação dos Direitos Autorais

Copiar, reproduzir ou utilizar indevidamente obras sem a expressa autorização do(s) autor(es) configura violação dos direitos autorais, também conhecido como pirataria.

Vários sites como os de gerenciamento de arquivos e de downloads violam indiscriminadamente os direitos autorais.

A pirataria virtual é crime previsto em lei, porém ainda divide opiniões em relação a sua configuração, para alguns autores o fato de simplesmente disponibilizar arquivos sem a expressa autorização do autor confira um crime de pirataria, mas para outros autores é necessário que haja a intenção de se obter lucro com a disponibilização dos arquivos.

Independentemente da configuração de um ato como pirataria virtual, a punição para quem pratica tal crime é difícil de ser aplicada, pois milhares de pessoas disponibilizam arquivos para download e milhões baixam esses arquivos, sendo muito difícil identificar quem disponibilizou o arquivo e praticamente impossível identificar todas as pessoas que baixaram.

Roubo de Identidade

Também conhecido como phishing o roubo de identidade refere-se ao roubo de informações pessoais como senhas, números de cartão de crédito e informações bancárias. As técnicas mais conhecidas de roubo de identidade são: a engenharia social, onde o criminoso consegue a confiança da vítima e rouba as informações

através da internet; furto de correspondências de caixas de correio e até mesmo inspeção de lixo.

Acesso não autorizado a rede de computadores, dispositivo de comunicação ou sistema informatizado

Uma das condutas mais praticadas pelos criminosos é o acesso não autorizado às redes privadas e a dispositivos de comunicação. Em alguns casos essas invasões são feitas apenas pelo prazer que o indivíduo tem em transpor as barreiras de segurança encontradas. Porém na maioria dos casos os acessos não autorizados ocorrem com a intenção de obter informações pessoais das vítimas.

Ao obter informações pessoais o invasor está ferindo diretamente a intimidade da vítima, o que pode trazer vários transtornos para a mesma. Entretanto, caso o agente acesse outros dispositivos com a intenção de apenas de bisbilhotar, ele não poderá ser punido, pois não existe tipificação penal

Invasão de sites e pichação virtual

Atualmente milhões de pessoas têm sites pessoais e a maioria não se preocupa com a segurança desses sites, o que facilita a ação de crakers que invadem esses sites e alteram as informações veiculadas, inclusive fotos, vídeo e imagens.

A invasão de sites pessoais é a mais comum, por não terem uma segurança adequada, entretanto, atualmente ocorreu uma onda de ataques a sites do governo, inclusive sites de polícia, o que mostra a capacidade dos crakers que normalmente invadem esses sites pelo simples prazer em transpor as barreiras de segurança.

Figura 01: O SITE DO IBGE (índice brasileiro de geografia e estatísticas) Foi alvo de crackers,foi invadido na madrugada de sexta-feira dia 24/06/2011 .Os invasores são chamados de fire h4ck3r e fail shell ,os hackers dizem não ter ligações com anymous e Lulzsec que seriam grupos que não tem muitos propósitos. infelizmente.quis dizer felizmente o ataque não atingiu seu banco de dados apenas sua home page.Os hacker que se intitula nacionalistas ainda divulgaram seus ataques no zone-h.

Fonte: site info. abril.com.br

Normalmente as invasões e a consequente pichação ocorrem através de disparo de inúmeros acessos simultâneos originados de vários computadores, denominados zumbis, situados em localidades diversas, para sobrecarregar o sistema até derrubá-lo. Tais procedimentos são também conhecido por ataques de negação de serviços do tipo (DdoS) Distributed Denial of Service ou (DoS) Denial of Service.

Figura 02: O site oficial do pastor e deputado federal Marco Feliciano (PSC-SP) foi invadido por hackers na tarde desse domingo (06/2015). O ataque ocorreu na mesma data da Parada Gay em São Paulo. O grupo entitulado ProtoWave utilizou uma imagem de um Jesus Cristo negro, que segura em cada mão uma imagem da cabeça do pastor e um perfume da empresa O Boticário, recentemente criticada por conservadores ao inserir referências a casais gays em sua campanha publicitária. O grupo também inseriu uma sátira da canção I will survive, da cantora Glória Gaynor, que toca quando o internauta acessa o site.
Fonte: site Correio Braziliense.

Em 2012 sites de governos do Brasil e do mundo, assim como os de grandes corporações sofreram com um grande número de invasões e pichações, que ocorreram como uma resposta ao fechamento de sites de compartilhamento de arquivos.

Com o surgimento da internet, novos meios de espionagem foram aparecendo. Keyloggers, trojans, malware e spyware são utilizados na espionagem industrial, permitindo o acesso remoto à informação muitas vezes confidencial.

Ciberterrorismo

Consiste na prática de ataques terroristas através da internet, com o objetivo de causar danos a sistemas computacionais. Em agosto de 2011 uma companhia holandesa DigiNotar admitiu que hackers tinham gerado vários certificados SSL de forma ilegal. Mais tarde, descobriu-se que o certificado foi utilizado para espionar cerca de 300 iranianos por meio de suas contas de Gmail.

Vários especialistas em segurança da informação alertam para o perigo de que as organizações terroristas possam usar a internet para a prática de terrorismo. Segundo eles essas organizações possuem conhecimentos técnicos suficientes para invadir sistemas de informação.

Interceptação de Informação

Segundo a Lei 9.296/96, artigo 10 “constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei”.

Apesar de ilegal é muito comum à interceptação de informações principalmente através da internet, como por exemplo, a interceptação de e-mails, com a intenção de obter informações confidenciais de indivíduos e organizações.

Disseminação de Vírus e Similares

Não é crime o simples ato de disseminar ou contaminar um computador com um vírus, contudo caso ocorra dano patrimonial a terceiro, poderá ser aplicado o artigo 163 do Código Penal Brasileiro que prevê pena de detenção, de um a seis meses, ou multa para quem “destruir, inutilizar ou deteriorar coisa alheia”.

Um estudo realizado entre 16 e 30 de julho 2012 pela empresa de segurança da informação Symantec revelou o Brasil tem um prejuízo anual de aproximadamente 8 bilhões de doláres, com os crimes de fraude e roubo de informações, realizados através da disseminação de vírus.

Gráfico 02: Gráfico do relatório "Norton Cybersecurity Report 2012" que mostra o custo anual, em dólares, do cibercrime realizados através de vírus.

Fonte: Symantec

De acordo com o relatório Norton Cybersecurity Report 2012 apresentado no Gráfico 03 o país é o terceiro mais afetado por atividade ilegal na rede, atrás de China ($ 46 bilhões) e Estados Unidos (R$ 21 bilhões) e empatado com a Índia.

Como a disseminação de vírus não é tipificada por nenhuma lei brasileira, essa prática criminosa só poderá ser punida se o agente que disseminar o vírus cometer em decorrência da disseminação outra atividade ilícita prevista no nosso ordenamento jurídico.

3.3 SUJEITOS DO CRIME VIRTUAL

Sujeito Ativo

Ao contrário do que muita gente pensa os criminosos da informática não são os hackers. Os profissionais de informática e os doutrinadores preferem chamar esses criminososde crackers.

Assim como os crakers, os hackers também detêm um amplo conhecimento de informática, porém diferentemente dos crakers, eles não usam esse conhecimento paradanificar sistemas e nem para prejudicar as pessoas. Normalmente os hakers são contratadospor empresas que pretendem encontrar alguma falha de segurança nos seus sistemas.

Também conhecidos como “White Hat”, os hakers não praticam nenhum crime, assim como afirma Assunção:

> Hacker White-Hat: Seria o “hacker do bem”, chamado de “hacker chapéu branco”. É aquela pessoa que se destaca nas empresas e instituições por ter um conhecimento mais elevado que seus colegas, devido ao autodidatismo e à paixão pelo que faz. Não chega a invadir sistemas e causar estragos, exceto ao realizar teste de intrusão. Resumindo: tem um vasto conhecimento, mas não o usa de forma banal e irresponsável. (ASSUNÇÃO, 2008)

Os crakers são os criminosos que usam seu vasto conhecimento para invadir sistemas, para roubar dados ou causar danos a terceiros. Ao contrário dos hakers que são conhecidos como “White Hat”, os crakers são conhecidos como “Black Hat”, conforme Assunção,

> Hacker Black-Hat: “hacker do Mal” ou “chapéu negro”. Esse, sim usa seus conhecimentos para roubar senhas, documentos, causar danos ou mesmo realizar espionagem industrial. Geralmente tem seus alvos bem definidos e podem passar semanas antes de conseguir acesso onde deseja, se o sistemafor bem protegido. (ASSUNÇÃO, 2008)

É comum as pessoas trocarem os termos, associando o criminoso ao termo hacker, entretanto o termo mais adequado é craker, sendo hacker aquela pessoa que detém um vasto conhecimento de informática, mas não prejudica ninguém.

Sujeito Passivo

Qualquer pessoa que tenha ou não acesso à internet pode ser vítima de um crime cibernético. Os sujeitos passivos são as pessoas que utilizam qualquer tecnologia informática (computadores, smartphones, tablets, etc.).

4 LEGISLAÇÃO BRASILEIRA E ESTRANGEIRA

4.1 CRITÉRIOS DE JULGAMENTO

Mesmo com a ausência de uma lei específica e as lacunas encontradas nas leis existentes, os magistrados contam com algumas opções para condenar um réu. Essasalternativas estão elencadas no artigo 4º do Decreto-Lei nº. 4.657/1942 “Quando a lei for omissa, o juiz decidirá o caso de acordo com a analogia”.

A fundamentação é essencial na sentença, pois é nela que o juiz menciona seus motivos, e essas alternativas permitem aos juízes fundamentarem as suas decisões mesmo quando a lei for omissa ou lacunosa. O juiz pode ser afastado da carreira de magistrado se não utilizar os costumes, analogia, caso a lei seja omissa.

Analogia

A analogia consiste em aplicar uma lei que regule um caso semelhante a casos não previstos por lei. Portanto quando um magistrado recorre à analogia ele está estendendo a umcaso semelhante à resposta dada a um caso particular.

Segundo Reale a analogia é um processo pelo qual:

> Estendemos a um caso não previsto aquilo que o legislador previu para outro semelhante, em igualdade de razões. Se o sistema do Direito é um todo que obedece a certas finalidades fundamentais, é de se pressupor que, havendo identidade de razão jurídica, haja identidade de disposição nos casos análogos, segundo um antigo e sempre novo ensinamento: ubi eadem, ibi eadem juris dispositivo (onde há a mesma razão deve haver a mesma disposição de direito). (REALE, 2004).

Mesmo a analogia sendo permita no Direito Civil, o seu uso deve ser feito com muita cautela, pois existem casos que aparentam ser completamente iguais, mas pode existir um detalhe em um deles que altere totalmente a sua essência jurídica, tornando-o diferente e assim inadequado compará-lo ao outro.

Há alguns requisitos necessários para o uso da analogia, que são os seguintes: a ausência de norma que regule um caso concreto, a similaridade entre o caso não regulado por lei e aquele amparado expressamente por uma norma e a existência de uma razão jurídica que permita a extensão normativa expressa ao caso não contemplado na lei, - no caso do Direito Civil o Decreto-Lei nº. 4.657/1942 no seu artigo 4º permite o uso de analogia nos casos em que a lei for omissa.

Costumes

A palavra costume deriva do latim consuetudo, e significa tudo que se estabelece por força do uso e do hábito. O costume ocupa um plano secundário em relação à lei e só pode ser usado depois que o juiz esgotar todas as possibilidades de uso da analogia para suprir as lacunas da lei. Há três tipos de costumes, quando comparados à lei, secudum legem, praeter legem e contra legem.

O costume amparado por lei é o secudum legem, que pode ser observado no art. 1.297, § 1º, do Código Civil e no artigo 100, inciso III, do Código Tributário Nacional.

Praeter legem é o costume não amparado por lei, mas que completa o sistema legislativo e por fim contra legem que é o costume contrário à lei, onde as normas costumeiras contrariam a lei e implicitamente revogam-nas, por resultar na não aplicação da lei em virtude de desuso.

4.2 PROJETO DE LEI, N 89 DE 2003

Vários projetos de lei que visam à tipificação de alguns dos crimes cibernéticos foram propostos, mas todos foram arquivados, dentre eles o mais completo e o mais polêmico foi o Projeto de Lei nº. 89 de 2003 de autoria do senador Eduardo Azeredo (PSDB/MG). O projeto visa à tipificação de alguns crimes virtuais e sofreu duras críticas por supostamente colocar em risco a liberdade de expressão na internet brasileira.

O projeto 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), a Lei nº. 7.716, de 5 de janeiro de 1989, a Lei nº. 8.069, de 13 de julho de 1990, e a Lei nº. 10.446, de 8 de maio de 2002, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, de rede de computadores, ou que sejam praticadas contra dispositivos de comunicação ou sistemas informatizados e similares, e dá outras providências.

Este projeto definia como crime:

1) O acesso indevido a meio eletrônico, ou seja, acessar, indevidamente ou sem autorização, meio eletrônico ou sistema informatizado ou ainda fornecer a terceiro

meio indevido ou não autorizado de acesso a meio eletrônico ou sistema informatizado. Para esses casos o projeto, previa detenção de três meses a um ano, e multa;

2) Manipulação indevida de informação eletrônica – “manter ou fornecer, indevidamente ou sem autorização, dado ou informação obtida em meio eletrônico ou sistema informatizado”. Pena de detenção de seis meses a umano, e multa;

3) Dano eletrônico, ou seja, destruir, inutilizar ou deteriorar coisa alheia ou dado eletrônico alheio;

4) Difusão de vírus eletrônico, ou seja, criar, inserir ou difundir dado ou informação em meio eletrônico ou sistema informatizado, indevidamente ou sem autorização, com a finalidade de destruí-lo, inutilizá-lo, modifica-lo ou dificultar-lhe o funcionamento;

5) Pornografia infantil – pena de reclusão de um a quatro anos para quem fotografar, publicar ou divulgar, por qualquer meio, cena de sexo explícito ou pornográfica envolvendo criança ou adolescente;

6) O atentado contra a segurança de serviço de utilidade pública, ou seja, atentar contra a segurança ou o funcionamento de serviço de água, luz, força, calor, informação ou telecomunicação, ou qualquer outro de utilidade pública;

7) A interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático, dispositivo de comunicação, rede de computadores ou sistema informatizado, ou seja, interromper ou perturbar serviço telegráfico, radiotelegráfico, telefônico, telemático, informático, de dispositivo de comunicação, de rede de computadores, de sistema informatizado ou de telecomunicação, assim como impedir ou dificultar-lhe o restabelecimento;

8) A falsificação de dado eletrônico ou documento público, ou seja, falsificar, no todo ou em parte, dado eletrônico ou documento público, ou alterar documento publico verdadeiro;

9) Falsificação de telefone celular ou meio de acesso a sistema eletrônico – o indivíduo que “criar ou copiar, indevidamente ou sem autorização, ou falsificar código, seqüência alfanumérica, cartão inteligente, transmissor ou receptor de radiofrequência ou de telefonia celular ou qualquer instrumento que permita o acesso a meio eletrônico ou sistema informatizado”. Para esses casos o projeto determina pena de reclusão, de um a cinco anos, e multa.

Como pode ser observado à cima o projeto tipifica vários crimes cibernéticos, e seria muito importante para o combate desses crimes, porém devido à superficialidade de alguns artigos o projeto vem sofrendo duras críticas de usuários e de especialistas em direito da informática.

Um exemplo da superficialidade do projeto pode ser observado no artigo 285 que prevê pena de uma a três anos de prisão para quem “inserir ou difundir dado ou informação em meio eletrônico ou sistema informatizado, indevidamente ou sem autorização”, a questão que fica é o que é um dado? Se uma pessoa difundir um vírus - que é um dado - através de um pendrive do qual não sabia estar contaminado, ela será punida?

Essa questão entre outras acabou gerando vários protestos na internet e o projeto acabou por ser arquivado.

Figura 03: Banner contra o Projeto de Lei nº 89/03

Fonte: bc10.com.br

4.3 LEI, Nº 12.737, DE 30 DE NOVEMBRO DE 2012.

Em 30 de novembro de 2012 o Brasil deu um passo importante no combate aos crimes cibernéticos com o advento da Lei, nº 12.737/2012. também conhecida

como Lei Carolina Dieckmann, uma alusão à atriz que recentemente teve fotos íntima divulgadas na internet.

Lei que dispõe sobre a tipificação criminal de delitos informáticos; e altera o Decreto-Lei no 2.848, de 07 de dezembro de 1940 - Código Penal; e dá outras providências. Com o seguinte disposto:

> "Invasão de dispositivo informático"
>
> 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 vulnerabilidades para obter vantagem ilícita:
>
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.
>
> § 1o Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.
>
> § 2o Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
>
> § 3o Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
>
> Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.
>
> § 4o Na hipótese do § 3o, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.
>
> § 5o Aumenta-se a pena de um terço à metade se o crime for praticado contra:
>
> I - Presidente da República, governadores e prefeitos;
>
> II - Presidente do Supremo Tribunal Federal;
>
> III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou
>
> IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal."
>
> "Ação penal
>
> Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos."

> Art. 3o Os arts. 266 e 298 do Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal, passam a vigorar com a seguinte redação:
>
> “Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública
>
> Art. 266. .....
>
> § 1º Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento.
>
> § 2o Aplicam-se as penas em dobro se o crime é cometido por ocasião de calamidade pública.” (NR)
>
> “Falsificação de documento particular
>
> Art. 298. .....
>
> Falsificação de cartão
>
> Parágrafo único. Para fins do disposto no caput, equipara-se a documento particular o cartão de crédito ou débito.” (NR)
>
> Art. 4o Esta Lei entra em vigor após decorridos 120 (cento e vinte) dias de sua publicação oficial.

Apelidada de “Lei Carolina Dieckmann”, a Lei nº 12.737, de 30 de novembro de 2012, entrou em pleno vigor no dia 3 de abril de 2013, alterando o Código Penal para tipificar os crimes cibernéticos propriamente ditos (invasão de dispositivo telemático e ataque de denegação de serviço telemático ou de informação), ou seja, aqueles voltados contra dispositivos ou sistemas de informação e não os crimes comuns praticados por meio do computador. Colateralmente equiparou o cartão de crédito ou débito como documento particular passível de falsificação.

A lei é fruto de projeto apresentado pelo Deputado Federal Paulo Teixeira (PT-SP), cujo trâmite foi acelerado depois da invasão, subtração e exposição na internet de fotografias íntimas da referida atriz.

Cuidando-se de nova lei incriminadora, a Lei nº 12.737/2012 que, em seu art. 4º estabelece uma vacatio legis de 120 (cento e vinte) dias, não poderá retroagir para alcançar condutas pretéritas.

Assim, a nova lei incrimina as condutas de: Invasão de dispositivo informático

- Invadir dispositivo informático alheio de qualquer espécie, conectados ou não em rede, desde que violado mecanismo de segurança (senha, firewall etc.), desde que a finalidade do criminoso seja obter, adulterar ou destruir dados ou informações.

- Instalar no dispositivo informático qualquer vulnerabilidade com o fim de obter uma vantagem ilícita (patrimonial ou não). Produzir, oferecer, distribuir, vender ou difundir dispositivo ou programa de computador com o intuito de permitir a invasão de dispositivo informático ou a instalação de vulnerabilidades.
- O objeto jurídico tutelado pela norma é a liberdade individual do usuário do dispositivo informático.

- As penas para esses delitos são de reclusão de 3 (três) meses a 1 (um) ano de detenção, e multa.

- As penas aumentam de 1/6 a 1/3 se a invasão resulta prejuízo econômico.

- O crime é qualificado, com penas que vão de 6 (seis) meses a 2 (dois) anos de reclusão e multa, caso a conduta não configure outro crime mais grave, quando a invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações definidas em lei como sigilosas. Se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos, a pena do crime qualificado será também aumentada de 1/3 a 2/3.

- As penas, conforme o caso (tipo simples ou qualificado) serão aumentadas de 1/3 até a metade, se o crime for praticado contra Presidente da República, Governadores e Prefeitos, Presidente do Supremo Tribunal Federal, da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal, ou dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.

- Importante: se a conduta for mais grave que a simples invasão com a finalidade de obtenção, adulteração ou destruição dos dados ou informações, ou a instalação de vulnerabilidades, como por exemplo, fraudes em netbanking (furto qualificado), estelionato ou extorsão, interceptação de comunicação telemática, o crime de

invasão de dispositivo informático será desconsiderado, porque constituirá somente um meio para o cometimento daquelas condutas.

- Para que o criminoso possa ser investigado pela Polícia e processado pelo Ministério Público, é preciso que a vítima autorize, oferecendo a representação. O Ministério Público pode processar diretamente o criminoso somente quando o crime é praticado contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos. Interrupção de Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação ou utilidade pública (ataque de denegação de serviço – DOS/DDOS).

- O artigo 266 do Código Penal pune a conduta de interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento, estabelecendo penas que variam de 1 (um) a 3 (três) anos de reclusão e multa, que são aplicadas em dobro em caso de calamidade pública.

- A Lei nº 12.327 alterou a denominação do crime do art. 266 do Código Penal, acrescentando que a interrupção de serviço telemático ou de informação de utilidade pública, bem como impedir ou dificultar-lhe o restabelecimento também é crime.
- Essa interrupção ou impedimento pode ser realizada de várias formas (crime de forma livre), por exemplo, a destruição física de uma determinada rede. Mas também pode ser feita mediante um ataque virtual, o qual também está contemplado pela alteração legislativa.

- Portanto, hoje, no Brasil, é crime a conduta denominada ataque de denegação de serviço (DOS/DDOS). O DOS (denial of service) não constitui geralmente uma invasão de sistema alvo, mas uma sobrecarga de acessos que fazem com que o fluxo de dados da rede seja interrompido. É chamado de ataque de denegação de serviço difundido ou DDOS (distributed denial of service) quando o criminoso infunde por meio de seu computador (mestre) vulnerabilidades ou programas maliciosos em vários computadores (zumbis), fazendo com que contra a vontade ou mesmo sem que os usuários afetados percebam, acessem simultaneamente ou sequencialmente

o serviço que pretende ser travado. Equiparação do cartão de crédito e débito com documento particular.

- A nova Lei também equiparou o cartão de crédito ou débito com o documento particular, transformando-os em objetos materiais do crime de falsidade documental.

- Para a configuração do crime basta que exista a inserção de dados impregnados na tarja magnética (parte juridicamente relevante do documento), que permite o acesso a sistemas bancários ou de crédito pertencentes a determinado correntista, não emitidos pela instituição correspondente.

- Todavia, somente a conduta de falsificar no todo ou em parte o cartão será considerada crime, o que não ocorre com a simples posse de um cartão clonado por quem não foi responsável pela falsificação. - Se utilizado o cartão e alcançado o dano patrimonial, em regra, tratar-se-á de crime de furto qualificado pela fraude e a falsidade será absorvida.

Como visto, a Lei nº 12.737/2012, embora represente certo avanço ao tipificar crimes cibernéticos propriamente ditos, contém inúmeras deficiências e confrontos com o sistema penal e processual penal vigente, o que deve merecer a atenção dos aplicadores.

Os crimes cibernéticos propriamente ditos são a porta de entrada para outras condutas criminosas, facilitando a utilização do computador como instrumento para cometer delitos.

O legislador não contemplou a invasão de sistemas, como os de clouding computing, optando por restringir o objeto material àquilo que denominou dispositivo informático, sem, contudo, defini-lo. Atividades de comercialização de cracking codes e de engenharia reversa de software também não foram objeto da norma.

Além das imperfeições na redação dos tipos, as penas cominadas na nova lei são ínfimas se considerada a potencial gravidade das condutas incriminadas, bastando dizer que um ataque de denegação de serviço pode colocar em risco vidas de uma população inteira. Implicam, por outro lado, a competência do Juizado Especial Criminal, cujo procedimento sumaríssimo é incompatível com a

complexidade da investigação e da produção da prova de crimes de alta tecnologia (perícia no dispositivo informático afetado, por exemplo). Numa síntese, os tipos e penas da Lei nº 12.737/2012 não conseguem dar as respostas esperadas pela Sociedade para desestimular aqueles que abusam das facilidades tecnológicas.

4.4 LEI Nº 12.965, DE 23 DE ABRIL DE 2014.

Devido o rápido desenvolvimento da internet no Brasil nas últimas décadas, surgiu a necessidade de se regulamentar o uso de tal rede no país, a fim de se estabelecer princípios, direitos e deveres a serem observados e obedecidos por todos os usuários da web.

E com a demanda, surgiu a Lei popularmente conhecida como Marco Civil da Internet. Criado pelo Poder Executivo, teve inicio em 2011 como uma Proposta de Lei nº 2.126, onde, em primeira instância, passou pelo Plenário da Câmara e por diversas outras comissões como: as Comissões de Defesa do Consumidor, Ciência e Tecnologia, Comunicação e Informática, Constituição e Justiça e de Cidadania, Proposição Sujeita à Apreciação do Plenário, diversas vezes nos decorrer dos anos até 2013, o projeto foi colocado em apreciação pela Câmara dos Deputados, entretanto, cancelado. No inicio do ano de 2014 o projeto foi novamente trazido a pauta, em discussão no Plenário da Câmara dos Deputados, onde o projeto foi emendado. Foram apresentadas as Emendas de Plenário que a comissão especial conclui pela constitucionalidade, juridicidade e boa técnica legislativa.

No dia 25 de Março de 2014 foi aprovada a redação final e encaminhada para a apreciação do Senado, sendo aprovado pelo mesmo no dia 22 de Abril de 2014. Por fim, a lei foi sancionada simbolicamente pela Presidente Dilma Rousseff no dia 23 de Abril de 2014 em uma Conferência Internacional, conhecida como NETMundial, realizada em São Paulo e que reuniu representantes de mais de 90 países. Lei esta, publicada no Diário Oficial da União no dia 24 de Abril de 2014, com vigência prevista para o dia 23 de Junho de 2014.

O Marco Civil da Internet traz em seus dispositivos a garantia à defesa dos consumidores que usam a Internet para adquirirem produtos e serviços; regula a comercialização das empresas que utilizam a rede mundial de computadores como meio de comércio, assegurando a regime de livre iniciativa, bem como a livre concorrência; Além de reger os serviços prestados pelos provedores de Internet,

estipulando o fornecimento com segurança e a garantia da funcionalidade, sob responsabilidade dos agentes prestadores.

Dessa forma, essa Lei busca garantir um acesso de qualidade e privacidade à todos os usuários sem distinção de classe social ou econômica.

Assim como retratados nos incisos do Art. 5º da Constituição Federal vigente, a Lei12.965/14 possui como fundamento a liberdade de expressão, respeitando as diferenças sociais e pessoais, com o intuito de proteção aos direitos e garantias individuais. Portanto, os principais objetivos da Lei são princípios que andam juntos com os demais princípios do ordenamento jurídico brasileiro, conforme transcrito na Lei:

> Art. 6oNa interpretação desta Lei serão levados em conta, além dos fundamentos, princípios e objetivos previstos, a natureza da Internet, seus usos e costumes particulares e sua importância para a promoção do desenvolvimento humano, econômico, social e cultural.

Aos usuários, ficam assegurados direitos e garantias que caracterizam a promoção da cultura e o exercício da cidadania pelo acesso à Internet, como escrito no Art. 7º. A Lei assegura o princípio da inviolabilidade da vida privada e da intimidade, princípio este que, apesar de já ser exercido no Brasil para os acontecimentos fora da rede, mostrou-se deficiente quando relacionada ao mundo virtual ultimamente.

Aos clientes dos provedores ficam reservados os direitos de receberem os serviços contratados de qualidade, podendo ficar o uso da rede suspenso se, e somente se, houver débitos decorrentes de sua utilização. Além disso, o Marco Civil garante o sigilo de informações, comunicações, dados e registros armazenados, exceto quando o usuário expressar e informar o consentimento da utilização de seus dados, ou por determinação judicial, ou hipóteses previstas em lei. E o Código de Defesa do Consumidor fica responsável pela defesa das relações de consumo realizadas na rede.

Ainda, o Art. 7º dispõe que é Direito do usuário a clareza e a publicidade das políticas de serviços oferecidos pelas empresas ao consumidor. O texto normativo reforça que é garantido o direito à privacidade e à liberdade de expressão, estipulando que qualquer cláusula contratual que se mostre contra este direito é nula. Estipula também que o não oferecimento de um foro brasileiro para a solução de possíveis problemas que aconteceram decorrentes de serviços prestados no território nacional torna nula a respectiva cláusula contratual.

A Neutralidade da rede é um dos pontos polêmicos do Marco Civil e divide opiniões dos especialistas no assunto, favoráveis ou não, de diferentes pessoas na sociedade desde o Projeto de Lei ser apresentado.

O Art. 9º, § 1º da Lei 12.965/14 dispõe sobre a Neutralidade na rede afirmando que as empresas responsáveis pelo roteamento, transmissão ou comutação da Internet deve tratar com isonomia qualquer pacote de dados, independentemente do conteúdo, da origem e destino ou da aplicação.

Ainda, concede ao Presidente da República o poder de regulamentar, por meio de decretos, a discriminação ou degradação do tráfego de dados, decorrendo sobre priorização de serviços de emergência ou requisitos técnicos que sejam indispensáveis à prestação dos serviços e aplicações. Porém, não o deve fazer sem antes consultar o Comitê da Internet e a Agência Nacional de Telecomunicações (ANATEL).

Para tanto, a Lei estabelece que caso ocorra uma violação do § 1º o responsável pelo fornecimento da rede deve obedecer o seguinte artigo do Código Civil:

> Art. 927. Aquele que, por ato ilícito, causar dano a outrem, fica obrigado a repará-lo.
> Parágrafo único. Haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem.

Além disso, deve agir com com total transparência e clareza, e informar, da mesma maneira, aos seus usuários, sobre todos os detalhes do gerenciamento de tráfego adotados, inclusive no que se trata à segurança da rede, oferecendo serviços com condições que não haja discriminações. Fica vedado à empresa que fornece, comuta ou transmite a conexão da Internet, seja ela gratuita ou onerosa, o bloqueio, a monitoração ou a análise do conteúdo do pacote de dados oferecido.

Um exemplo utilizado corriqueiramente para demonstrar um caso em que não há neutralidade é a comparação das empresas de Internet, com as empresas de televisão por assinatura, onde o cliente assina pacotes por diferentes serviços. Dessa forma, uma empresa que fornece acesso à rede pode cobrar R$ 15,00 para o acesso a e-mails, mas vetar o acesso à redes sociais como o YouTube, Facebook ou Twitter.

Para as empresas, a neutralidade total acaba com a possibilidade de oferecer pacotes mais acessíveis. Já os defensores da Lei afirmam que ela assegura o acesso aos serviços mais caros para uma faixa da população com menor poder aquisitivo.

Além da neutralidade da rede, às empresas que fornecem o acesso à conexão fica o dever da proteção de todos os registros e dados pessoais; do armazenamento dos registros de conexão e dos acessos às aplicações; e da responsabilidade por danos que decorram de conteúdo gerado por terceiros.

O Marco Civil da Internet estabelece que a empresa deve armazenar registros de conexão e de acesso à aplicativos sempre preservando a honra, a vida privada, e a imagem dos usuários. Informações, estas, com acesso somente perante uma ordem judicial que não entre em conflito com o Art. 7º da mesma Lei. Não impedindo, entretanto, o acesso à dados cadastrais que informem qualificação pessoal, endereço e filiação, por parte de empresas competentes para a aquisição desses dados.

Vale ressaltar que as condições acima aplicam-se com validade para os dados obtidos pelas empresas no território Nacional desde que pelo menos um terminal do provedor esteja aqui localizado.

Até mesmo quando tratar-se de pessoa jurídica sediada no exterior que oferte serviço público brasileiro ou possua algum integrante do mesmo grupo econômico com estabelecimento no Brasil. Ou seja, qualquer empresa que opere no Brasil deve respeitar a legislação aqui vigente e entregar as informações requeridas pela Justiça.

Portanto, sem interferência em sanções cíveis, administrativas ou criminais, os dispostos tratados acima referentes aos Art. 10 e 11 da Lei 12.965/14, ficam sujeitas à sanções que variam dependendo do caso, podendo serem aplicadas isolada ou cumulativamente:

> (...)
> I - advertência, com indicação de prazo para adoção de medidas corretivas;
> II - multa de até 10% (dez por cento) do faturamento do grupo econômico no Brasil no seu último exercício, excluídos os tributos, considerados a condição econômica do infrator e o princípio da proporcionalidade entre a gravidade da falta e a intensidade da sanção;
> III - suspensão temporária das atividades que envolvam os atos previstos no art. 11; ou
> IV - proibição de exercício das atividades que envolvam os atos previstos no art. 11.

> Parágrafo único. Tratando-se de empresa estrangeira, responde solidariamente pelo pagamento da multa de que trata o caputsua filial, sucursal, escritório ou estabelecimento situado no País.

É responsabilidade do provedor da conexão de guardar sigilosamente os registros de conexões em ambiente controlado e seguro pelo prazo de 1 ano, não podendo transferir a responsabilidade para terceiro. Havendo a possibilidade, ainda, de que a autoridade policial ou o Ministério Público requerer a guarda dos registros de conexão por prazo superior a 1 ano, tendo, o requerido, a partir do requerimento, prazo de 60 dias para ingressar com pedido de autorização judicial para o acesso aos registros de conexões.

Salientando que o provedor deve sempre manter sigilo sobre o requerente das informações. Na hipótese da violabilidade de qualquer parágrafo do Art. 13º da respectiva Lei, considerar-se-ão a natureza e a gravidade da infração, os danos resultantes, os agravantes, os antecedentes do infrator e a reincidência.

Tratando-se de acesso à aplicações, o respectivo registro deverá ser armazenado pelo prazo de 6 meses sob sigilo e em local seguro, por provedor de aplicações de Internet constituído como Pessoa Jurídica, exercendo atividade de forma profissional e com fins econômicos. Entretanto, uma ordem judicial poderá determinar que algum provedor que não se enquadre nas características acima guarde os registros de acesso por determinado período.

A autoridade policial ou o Ministério Público poderão requerer neste caso também à qualquer provedor para que os registos de acesso aos aplicativos sejam armazenados por prazo superior ao estipulado no Art. 15º. É importante citar que registro de acesso algum poderá ser armazenado sem o prévio consentimento do titular, respeitando o Art. 7º da mesma Lei.

Tratando-se da responsabilidade por danos decorrentes de conteúdo gerado por terceiros o provedor de Internet não pode ser responsabilizado, exceto se, após receber ordem judicial para tornar indisponível o conteúdo infringente, não o fizer.

A ordem judicial para remover conteúdo infringente deverá conter identificação específica do conteúdo permitindo a possível localização sem erros do material. As causas que tratam sobre o ressarcimento de danos decorrentes de conteúdos relacionados à honra, à reputação, ou a direitos de personalidade poderão ser apresentadas perante o Juizado Especial.

O juiz poderá antecipar, total ou parcialmente, a tutela requerida no pedido inicial existindo prova inequívoca dos fatos, e presentes também os requisitos de verossimilhança dos fatos alegados e o receio de dano de difícil reparação.

Entretanto, a lei, embora cheia de falhas deve ser elogiada, pois até através dela que se chegará à uma regulamentação mais próxima da realidade social, fazendo com os usuários que crescem a cada ano, se sintam um pouco mais seguros em usar a rede mundial de computadores.

4.5 PROJETO DE LEI Nº. 215/15

Conhecida popularmente como Lei do Esquecimento, o anteprojeto de Lei de Proteção de Dados Pessoais passou a ser discutido. O objetivo do anteprojeto consiste em fornecer ao cidadão o controle sobre as suas informações pessoais.

Tramita na Câmara dos Deputados o Projeto de Lei 215/15, do deputado Hildo Rocha (PMDB-MA), que aumenta em 1/3 a pena para os chamados crimes contra a honra, quando cometidos em redes sociais.

A proposta altera o Código Penal Brasileiro (Decreto-Lei 2848/40), que já prevê casos em que a pena para os crimes de calúnia, difamação e injúria é aumentada em um 1/3. São aqueles cometidos contra: o presidente da República ou chefe de governo estrangeiro; funcionário público; a honra de alguém na presença de várias pessoas ou por meio que facilite a divulgação; idosos e pessoas com deficiência (neste caso, exceto para o crime de injúria).

Ainda segundo o Código Penal, a aplicação da pena, em todos os casos, será em dobro quando o crime contra a honra for mercenário, ou seja, motivado pelo pagamento de recompensa ou pela simples promessa dela.

Rocha ressalta que, quando o Código Penal foi elaborado, a tecnologia não estava no atual estágio de desenvolvimento. "Os crimes contra a honra praticados pelas redes sociais têm um efeito devastador na vida das vítimas, causando enormes prejuízos na vida profissional, familiar, além de sofrimentos morais, emocionais e mentais irreparáveis", afirma.

A proposta será analisada pela Comissão de Constituição e Justiça e de Cidadania (inclusive quanto ao mérito). Depois, será votada pelo Plenário.

Apesar de toda mobilização da sociedade civil e esforço dos deputados que tentaram retirar do PL 215/15 o artigo que versava sobre o direito ao esquecimento e

a remoção de conteúdos da internet, o texto do substitutivo de autoria do deputado Juscelino Filho (PRP-MA) foi aprovado na tarde desta terça-feira, 6/10, sem mudanças. O PL agora segue para apreciação em plenário, antes de ser enviado para o Senado.

O texto aprovado modifica o artigo 19º do Marco Civil da Internet, incluindo um parágrafo, o 3º-A, que permite requerer judicialmente, a qualquer momento, a indisponibilização (leia-se remoção) de conteúdo que associe o seu nome ou imagem a crime de que tenha sido absolvido, com trânsito em julgado, ou a fato calunioso, difamatório ou injurioso.

Um dos críticos do dispositivo, o deputado Alessandro Molon (Rede-RJ), que foi relator do Marco Civil da Internet na Câmara, explicou que, em outros países onde há a discussão sobre o assunto, as pessoas públicas são proibidas de fazer uso do direito ao esquecimento, o que não ocorre no projeto aprovado pela CCJ e provoca críticas de que foi feito para defender políticos. "Na Europa, não existe isso de retirar conteúdos, trata-se de desindexar, ou seja, dissociar as buscas na internet pelo nome daquela pessoa e as matérias que são difamatórias", acrescentou Molon.

Outras alterações propostas pelo PL ao Marco Civil foram abrandadas, incluindo a manutenção da necessidade de ordem judicial para a requisição de dados dos usuários. O relator acatou a opinião majoritária na comissão de que continua a ser necessária autorização judicial para o acesso a dados de conexão e conteúdos privados de aplicativos.

Com relação à identificação obrigatória, o texto aprovado prevê no entanto, a ampliação dos dados cadastrais a serem coletados pelos provedores de internet, impondo a obrigação de reterem dados como endereço completo, telefone e CPF, que poderão ser repassados, sem ordem judicial, para autoridades que tenham atribuição legal para fazer esse pedido, quando estiverem fazendo uma investigação. Pelo Marco Civil, já é possível pedir sem autorização da Justiça a identificação, filiação e endereço do autor de páginas ou comentários.

Em audiência pública na CPI dos Crimes Cibernéticos na Câmara dos Deputados. realizada também nesta terça-feira, 6/10, o professor da Faculdade de Direito da Universidade do Estado do Rio de Janeiro (UERJ), Ronaldo Lemos, afirmou que a sistemática de retenção de dados pessoais na rede mundial de computadores, prevista no Marco Civil da Internet, “coloca o país na contramão da

história". A guarda dessas informações pelos provedores é considerada fundamental para a investigação de crimes cibernéticos.

Apesar de reconhecer que o Marco Civil é um dos dispositivos legais mais modernos em todo o mundo, Ronaldo Lemos ressaltou que a sistemática de retenção de dados adotada pelo Brasil foi a mesma usada em vários países da Europa. No entanto, vários deles começaram a abandoná-la após a Corte Europeia de Justiça decretar a sua inconstitucionalidade, sob o argumento de que interfere em direitos fundamentais, deixando o cidadão sob constante vigilância.

Segundo Ronaldo Lemos, Áustria, República Tcheca, Finlândia e Alemanha são alguns dos países que já reviram a retenção de dados pessoais de usuários da internet, e a Noruega jamais adotou essa sistemática. "A opção do Brasil em adotá-la no Marco Civil foi legítima, e hoje há pressões por guardar mais dados ou ampliar a lista de dados guardados. Mas, se isso acontecer, o país estará na contramão da história e se distanciando do cenário global", afirmou.

Pois o PL 215/15 torna ainda mais abrangente a retenção de dados.
Na mesma audiência pública da CPI dos Crimes Cibernéticos, outros palestrantes pediram cautela em eventuais mudanças no Marco Civil da internet.

No tocante aos crimes contra a honra o substitutivo aprovado modifica ainda procedimentos de apuração de crimes contra a honra (calúnia, difamação e injúria) praticados por meio da internet. Pelo texto, a autoridade policial deverá imprimir o conteúdo ofensivo publicado que servirá como prova para dar início à ocorrência. Atualmente, a legislação não é clara sobre como deve ser feita a coleta de subsídios para esse tipo de ação.

A proposta também altera o Código Penal para duplicar a pena para crimes contra honra cometidos na internet caso a infração provoque a morte de alguém. O relatório anterior de Juscelino Filho duplicava a sanção pelo simples fato de o crime ser praticado por meio da web, mas o texto foi alterado. O deputado lembrou que a legislação em vigor já pune com um 1/3 a mais de detenção quem comete esses delitos "por meio que facilite sua divulgação", no qual se enquadraria a internet.

Algumas críticas referente à PL 215/15 é está sendo acusado por ativistas digitais de ser um mecanismo para defender políticos de críticas em blogs e perfis das redes sociais.

Entre a sociedade civil organizada, o PL 215/15 ganhou o apelido de PL Espião, por facilitar a espionagem e retirada de conteúdos na rede que possam ser

considerados ofensivos à honra de alguém – inclusive dos políticos e autoridades públicas. Há uma petição online no ar pedindo a rejeição do PL, que ainda será votado no Plenário da Câmara.

"Não se constrói uma nação sem memória e sem história. Este projeto de lei representa uma grave ameaça à liberdade de expressão na internet e ao direito à informação de toda a sociedade brasileira. No fundo o que se quer é permitir que pessoas públicas incomodadas com determinados conteúdos na internet possam pedir para apagá-los", lamentou Alessandro Molon.

O deputado usou como exemplo o caso do ex-presidente Fernando Collor de Mello, afastado pelo Congresso Nacional, mas absolvido no Supremo Tribunal Federal. “A informação de que ele foi processado no Supremo, mesmo que tenha sido absolvido, é uma informação relevante do ponto de vista histórico e você não pode apagar e fingir que isso não existiu”, ponderou Molon.

O Conselho de Comunicação do Congresso Nacional se posicionou contra o projeto, assim como o Comitê Gestor da Internet no Brasil que, na semana passada editou uma resolução que diz que o projeto subverte o seu Decálogo ao propor o estabelecimento de “práticas que podem ameaçar a liberdade de expressão, a privacidade dos cidadãos e os direitos humanos em nome da vigilância, bem como desequilibrar o papel de todos os atores da sociedade envolvidos no debate”.

4.6 CONVENÇÃO DE BUDAPESTE

Alguns países já estão bem avançados em relação a regulamentação da internet, principalmente os que aderiram a Convenção sobre o Cibercrime, ou Convenção de Budapeste. O Brasil até que tentou participar da Convenção através do senador Eduardo Azeredo (PSDB-MG), mas o país só poderia se tornar signatário do tratado se fosse convidado pelo Comitê de Ministros do Conselho Europeu, o que não aconteceu.

A Convenção sobre Cibercrime do Conselho da Europa é o primeiro trabalho internacional de fundo sobre crime no ciberespaço. Foi elaborado por um comitê de peritos nacionais, congregados no Conselho da Europa e consiste num documento de direito internacional público. Embora tenham na sua origem, sobretudo, países membros do Conselho da Europa, tem vocação universal. Na sua elaboração participaram vários outros países (Estados Unidos da América, Canadá, Japão e

África do Sul) e pretende-se que venha a ser aceite pela generalidade dos países do globo.

A Convenção prioriza “uma política criminal comum, com o objetivo de proteger a sociedade contra a criminalidade no ciberespaço, designadamente, através da adoção de legislação adequada e da melhoria da cooperação internacional” e reconhece “a necessidade de uma cooperação entre os Estados e a indústria privada”.

O tratado traz quatro capítulos (Terminologia, Medidas a Tomar a Nível Nacional, Cooperação Internacional e Disposições Finais) e define os cibercrimes, tipificando os como: infrações contra sistemas e dados informáticos; infrações relacionadas com computadores; infrações relacionadas com o conteúdo, pornografia infantil e infrações relacionadas com a violação de direitos autorais.

O capítulo 1 da convenção traz as terminologias necessárias para a compreensão do tratado, as definições são as seguintes:

a) Sistemas informáticos “significa qualquer dispositivo isolado ou grupo de dispositivos relacionados ou interligados, em que um ou mais entre eles, desenvolve, em execução de um programa, o tratamento automatizado dos dados”;

b) Dados informáticos são “qualquer representação de fato, de informações ou de conceitos sob uma forma suscetível de processamento num sistema de computadores, incluindo um programa, apto a fazer um sistema informático executar uma função”;

c) Fornecedor de serviço é:

- ✓ “Qualquer entidade pública ou privada que faculte aos utilizadores dos seus serviços a possibilidade de comunicar por meio de um sistema informático;

- ✓ “Qualquer outra entidade que processe ou armazene dados informáticos em nome do referido serviço de comunicação ou dos utilizadores desse serviço”.

d) Dados de tráfego são “todos os dados informáticos relacionados com uma comunicação efetuada por meio de um sistema informático, gerados por este sistema como elemento de uma cadeia de comunicação, indicando a origem da

comunicação, o destino, o trajeto, hora, a data, o tamanho, a duração ou o tipo do serviço subjacente".

Já o capítulo 2 tece sobre as medidas que cada país membro deverá adotar em relação aos seguintes assuntos:

- Acesso ilegítimo - "cada país adotará as medidas legislativas e outras que se sejam necessárias para estabelecer como infração penal, no seu direito interno, o acesso intencional e ilegítimo à totalidade ou a parte de um sistema informático".

- Interceptação ilegítima -"cada parte adotará as medidas legislativas e outras que se revelarem necessárias para estabelecer como infração penal, no seu direito interno a interceptação intencional e ilegítima de dados informáticos, efetuadas por meios técnicos, em transmissões não públicas, para dentro de um sistema informático, incluindo emissões eletromagnéticas provenientes de um sistema informático que veicule esses dados".

- Interferência em dados - "cada país adotará as medidas legislativas e outrasque se revelarem necessárias para estabelecer como infração penal, no seudireito interno, o ato de intencionalmente e ilegitimamente danificar, apagar, deteriora, alterar ou eliminar dados".

- Interferência em sistemas - cada parte adotará as medidas legislativas e outras que se revelarem necessárias para estabelecer como infração penal, no seu direito interno, a obstrução grave, intencional e ilegítima, ao funcionamento de um sistema informático, através de introdução, transmissão, danificação, eliminação, deterioração ou supressão de dados informáticos".

- Uso abusivo de dispositivos - "cada país adotará as medidas legislativas e outras que se revelarem necessárias para estabelecer

como infração penal a produção, a venda, a obtenção para utilização, a importação, a distribuição, ououtras formas de disponibilização de:

I) Dispositivos, inclusive programas informáticos, concebido ou adaptado para permitir a prática de um crime.

II) Um código de acesso que permitam acessar em todo, ou em parte um sistema informático.

- Falsidade informática “cada país adotará as medidas legislativas necessária para estabelecer como infração e introdução, a alteração, a eliminação ou a supressão intencional e ilegítima de dados informáticos, produzindo dados não autênticos, com a intenção de que estes sejam ou não diretamente legíveis”.

- Burla informática “cada parte adotará as medidas legislativas que se revelem necessárias para estabelecer com infração penal, o ato intencional e ilegítimo, que origine a perda de bens a terceiros através da introdução, da alteração, da eliminação ou da supressão de dados informáticos”.

- Pedofilia: “Cada país tomará medidas legislativas para estabelecer como crime as seguintes condutas, quando cometidas de forma intencional e ilegítima”.

I) Produzir pornografia infantil com o objetivo da sua difusão através de um sistema informático;

II) Oferecer ou disponibilizar pornografia infantil através de um sistema informático;

III) Oferecer ou transmitir pornografia infantil através de um sistema informático;

IV) Obter pornografia infantil através de um sistema informático para si próprio ou para terceiros;

V) Possuir pornografia infantil num sistema informático ou num meio de armazenamento de dados informáticos;

- Violação dos direitos do autor - Cada parte adotará as medidas necessárias para estabelecer como crime a violação do direito do autor relacionadas com a interpretação, execução, com exceção de qualquer direito moral conferido por essa convenção, quando esses atos forem praticados intencionalmente, a uma escala comercial e por meio de um sistema informático.

O tratado traz ainda em seu texto regras de cooperação internacional onde é fixado o limite mínimo de um ano de prisão, para que seja admissível a extradição, sendo necessária a dupla incriminação. Porém, o texto prevê a possibilidade de haver extradição para crimes de pena inferior em caso de existir um tratado bilateral entre dois estados envolvidos e nesse tratado se prever um limite inferior. Segundo o artigo 24º da convenção um país signatário pode recusar a extradição caso o crime cometido seja considerado de ordem política ou relacionado com a mesma, ou ainda que esteja em causa a soberania, a segurança, a ordem pública ou outros interesses essenciais do Estado.

Em relação à cooperação mútua a Convenção de Budapeste em seu artigo 26º prevê a possibilidade de um país encaminhar informações a outro Estado caso essas informações sejam úteis ou necessárias ao início ou ao desenvolvimento de uma investigação de um crime enquadrado na Convenção. A remessa de informação para outro país signatário deve observar a confidencialidade dos dados.

O ingresso do Brasil no tratado seria de suma importância para o combate aos crimes cibernéticos, pois se o país se tornasse membro da convenção, ele adentraria num regime internacional de combate ao cibercrime, facilitando, assim, uma cooperação maior com outros países que sofrem das mesmas práticas ilícitas, mas que possuem leis diferentes.

De acordo com o mestre em direito da informática, Maria Amália Câmara, “apesar de ser um ramo em ascensão, nossos julgadores mostram que não têm conhecimento das tecnologias, especialmente porque é algo muito recente”.

5 MOTIVOS DA IMPUNIDADE

Os motivos que implicam na impunidade de quem pratica um crime virtual são: Inexistência de lei tipificadora, difícil identificação do autor do crime, falta de conhecimento técnico dos magistrados e advogados e também as facilidades encontradas para praticar tais crimes.

5.1 PRINCÍPIO DA LEGALIDADE E INEXISTÊNCIA DE LEI TIPIFICADORA

O princípio da legalidade traz que caso não haja uma lei que tipifica uma conduta, então ninguém será obrigado praticar ou deixar de praticar tal conduta, é o que diz o artigo 5º, inciso II da Constituição Federal, “ninguém será obrigado a fazer ou deixar de fazer alguma coisa senão em virtude de lei”, em outras palavras, mesmo que a conduta seja imoral ou antiética, ninguém poderá ser punido por praticá-la, caso a mesma não esteja enquadrada em alguma lei.

A Constituição Federal e o Código Penal brasileiro definem em seu artigo 5º, inciso XXXIX e artigo 1º, respectivamente, que “não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal”. Tais artigos são exemplos do princípio constitucional da legalidade e deixam bem claro o grande problema da impunidade dos crimes cibernéticos – como em sua maioria eles não são tipificados por nenhuma lei, então nem crimes eles são, e se não são crimes, não pode haver punição para quem pratica-los.

Nesse contexto Castro afirma que

> O problema surge em relação aos crimes cometidos contra o sistema de informática, atingindo bens não tutelados pelo legislador, como dados, informações, hardware, sites, home pages, e-mail, etc... São condutas novas que se desenvolveram junto com nossa sociedade razão pela qual o legislador de 1940, época do Código Penal, não pôde prever tais tipos penais. (CASTRO, 2003)

Tal princípio se justifica limitar o poder arbitrário do Estado, protegendo os direitos dos cidadões e limitando a atuação do Estado à lei. Porém, acaba por beneficiar o agente do crime cibernético, já que não existe lei para a maioria desses crimes.

Para os magistrados pátrios a maior dificuldade em punir quem pratica um crime virtual está relacionada à dificuldade de enquadrar tais crimes na nossa

legislação comum, opinião compartilhada por Prieto e Gahyva (2012), como não há um regramento legal específico que componha um microssistema que trate do tema, muitas condutas danosas acabam sem punição, pois nem sempre se faz possível à aplicação da legislação penal comum.

Ainda segundo Prieto e Gahyva,

> [...] as infrações penais e abusos que constantemente ocorrem são de toda a ordem: racismo; pornografia infantil; apologia ao crime; difamação; estelionato; pirataria; espionagem clandestina; crimes contra a economia popular; ameaça; violação de correspondência; furto; e, até mesmo prática de terrorismo. (PRIETO; GAHYVA, 2012)

Diante da amplitude dos Crimes Cibernéticos é necessário que se crie uma lei que tipifique os crimes da informática com urgência, é o que defende Silva,

> É extremamente necessário e urgente, buscar a tipificação dos crimes de informática e condutas criminosas que são efetuadas através da Rede Mundial de Computadores, sob o risco da própria sociedade como um todo entrar em uma área ainda por muitos desconhecida, onde não há território delimitado e muito menos um ordenamento jurídico de controle social. (SILVA, 2012)

O problema é que a tecnologia é muito dinâmica e está em constante mudança e o ordenamento jurídico brasileiro não acompanha essa mudança e nem se preocupa em acompanhar, haja vista que Crimes Cibernéticos não é nenhuma novidade e mesmo assim nenhuma lei que enquadra tais crimes foi criada.

A dificuldade em criar tal lei fica mais evidente quando o crime ocorre fora do território brasileiro, pois o Brasil adota o princípio geral da territorialidade, onde as leis ficam limitadas ao seu território.

Em sua obra Roque explana que,

> [...] a questão que sucinta maiores dúvidas é a dos crimes à distância como nos casos dos delitos praticados através da internet quando a ação é executada em um país e seus efeitos ocorrem no Brasil. Como resolver, então, estes problemas: a solução estaria na celebração de tratados internacionais, mas para isso ser possível há necessidade da existência, primeiramente, da dupla incriminação, ou seja, que as condutas constituam crime em ambos os países. (ROQUE, 2007)

Prieto e Gahyva (2012) concluem que não resta outra solução para o direito senão acompanhar essa evolução, buscando ampliar a regulamentação de tais comportamentos, reconhecendo sempre que o combate a tal espécie de

criminalidade representa um enorme e diário desafio para todos os componentes do sistema penal.

5.2 DIFÍCIL IDENTIFICAÇÃO DO AUTOR

Para acessar a internet não é necessário na maioria dos casos nenhum tipo de identificação pessoal, qualquer pessoa pode acessá-la praticamente de qualquer lugar e sem nenhum controle.

A maior falha de segurança da internet é que não é necessária a identificação do usuário através de um documento oficial. Hoje a identificação de um usuário é feita através do IP da máquina.

É através do protocolo tcp/ip que é feito a identificação com exatidão de onde o criminoso praticou o crime, o problema é que o protocolo identifica apenas o computador e não o usuário, o que prejudica a identificação de uma pessoa em específico.

A identificação do autor do crime se torna mais difícil quando o criminoso utiliza uma rede sem fio livre, como as encontradas em faculdades por exemplo. Essas redes são utilizadas por várias pessoas e identificar um usuário em específico é praticamente impossível. As Lan Houses também são utilizadas por criminosos que se aproveitam do fato de que grande parte delas não cobram a apresentação de um documento para liberar o acesso à internet.

Outro fator que prejudica a identificação do autor do crime é que é necessária uma autorização judicial para a identificação do IP, o que demora cerca de dez dias.

5.3 FALTA DE CONHECIMENTO TÉCNICO DOS MAGISTRADOS

Para a maioria dos autores um dos grandes problemas em se julgar um crime de informática é a falta de conhecimento técnico de juízes e advogados.

Alguns julgamentos como o da apresentadora de TV Daniela Cicarelli e seu namorado, Tato Malzoni, que tiveram um vídeo com cenas íntimas divulgado num site de compartilhamento de vídeos. Na ocasião o desembargador de São Paulo Ênio Santarelli Zuliani determinou o bloqueio da transmissão de dados entre a web brasileira e o site de compartilhamento de vídeo.

A decisão equivocado do desembargador afetou milhões de usuários da internet que ficaram sem acesso ao site durante três dias. Provavelmente por falta de conhecimento da área, o desembargador tomou uma decisão que prejudicou várias pessoas, sendo que apenas uma intimação para que o site retirasse o vídeo do ar bastaria.

5.4 FACILIDADES EM COMETER TAIS CRIMES

Com crescimento das redes sociais as pessoas passaram a expor cada vez mais a sua vida na internet, inclusive as crianças e os adolescentes, o que aumentou o interesse de pedófilos, que criam perfis falsos para atrair as vítimas e assim por em pratica os seus crimes.

Assim como a pedofilia, o crescimento da internet e das redes sociais possibilitou o surgimento de vários crimes cibernéticos próprios e a intensificação de outros crimes já existentes, como a pirataria virtual de músicas, vídeos e livros, que podem ser encontrados facilmente com uma simples pesquisa.

Atualmente não é necessário que uma pessoa detenha grandes conhecimentos em informática para praticar um crime, pois há vários fóruns na internet que ensinam quem quiser a ser um craker, são vários tópicos que contém passo a passo o que deve ser feito para capturar senhas de mensageiros instantâneos.

Além dos fóruns, há vários sites que disponibilizam para download vírus que podem ser facilmente programados e espalhados pela internet. Esses criminosos aproveitam da inocência de grande parte dos usuários da internet, para disseminar vírus e assim obterem informações pessoais.

CONCLUSÃO

Este trabalho não visa esgotar os assuntos então apresentados, porém, apenas dar uma ideia do que está ocorrendo ante as mudanças apresentadas.

De acordo com a Constituição da República Federativa do Brasil de 1988, em seu artigo 5º, podemos encontrar a palavra intimidade em dois incisos:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> (...) X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;
> LX - a lei só poderá restringir a publicidade dos atos processuais quando a defesa da intimidade ou o interesse social o exigirem;

Tais dispositivos não são os únicos que garantem referidos direitos, porém, são os principais encontrados em nossa constituição federal.

Com o advento de leis específicas, em especial as Leis nº 12.737 de 2012, e a Lei do Marco Civil da Internet, nosso país está se inserindo, na lista de países que já apenam crimes relacionados ao mundo virtual.

Não há de se negar que com o advento do Marco Civil da Internet o Brasil deu um grande passo, trazendo um pouco de segurança e proteção aos usuários da rede, porém com muitas lacunas a serem sanadas.

Destaca-se, ainda, o projeto lei nº 225/2015, muito polêmico por tratar sobre assuntos que versam sobre direitos constitucionais como o da intimidade, privacidade, entre outros, e sua inviolabilidade ou não.

Muito há de se discutir, pois a criminalidade virtual cresce numa velocidade avassaladora, e devemos nos preparar para prevenção e punição desses crimes.

O desenvolvimento de qualquer nação soberana, hodiernamente, depende de um plano tecnológico sério e de ponta para suportar a demanda que está por vir. Não podemos mais sermos vítimas de ataques de outras nações, como a que ocorreu no ano passado com os Estados Unidos da América, em um episódio que gerou enorme desconforto entre esses dois Estados, muito menos sermos atacados pelos nossos infratores nacionais.

Não podemos esquecer também que a pedra fundamental para que não se ocorra invasões ou mesmo ataques virtuais variados é a simples e eficaz educação.

Não basta possuirmos as ferramentas mais modernas e avançadas do mundo, sem que as pessoas que acessam tais máquinas continuem na idade da pedra no quesito intelectual e moral.

Sem sombra de dúvidas, o aperfeiçoamento integral de todas as faculdades humanas, é o ponto central do desenvolvimento de uma sociedade livre e justa. O avanço tecnológico é mais um degrau no desenvolvimento humano, não podendo andar apartado da educação e do respeito.

REFERÊNCIAS

ANÔNIMO. **Segurança Máxima: O guia de um hacker para proteger seu site na Internet e sua rede**. Rio de Janeiro : Campus, 2000.

ASSUNÇÂO, Marco Flávio Araújo. **Segredo do Hacker Éticos**. 2. ed. Florianópolis: Visual Books, 2008.

BULOS, Uadi Lammego. **Constituição Federal anotada**. 5 ed. São Paulo: Saraiva, 2003. P.255.

BLUM, Renato M.S. Opice; BRUNO, Marcos Gomes da Silva; ABRUSIO, Juliana Canha. **Manual de Direito Eletrônico e Internet**. São Paulo: Lex Editora, 2006.

BOCCHINI, Lino. Quem é o culpado pelo suicídio da garota em Veranópolis? Disponível em: <http://www.cartacapital.com.br/blogs/blog-do-lino/o-suicidio-daadolescente-de-veranopolis-e-nossa-culpa-6036.htm > Acesso: em 19 nov. 2013.

BREDA, Tadeu. Apenas soluções técnicas não podem conter espionagem na internet.Disponível:<http://www.redebrasilatual.com.br/saude/2013/07/apenassolucoes-tecnicas-nao-podem-conter-espionagem-pela-internet-8210.html> Acesso em: 10/10/2015

Brasil. Contituição (1998). Contituição da República Federativa do Brasil de 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/> Acesso em: 30/09/2015.

Brasil. Decreto-Lei nº 2.848, de 07 de dezembro de 1940. Código Penal. Disponível em:<http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm>. Acesso em: 30/09/2015.

Brasil. Decreto-Lei nº 3.914, de 9 de dezembro de 1941. Disponível: < http://www.planalto.gov.br/ccivil_03/decreto-lei/Del3914.htm>. Acesso em: 18/10/2015.

Brasil. Lei nº 11.829, de 25 de novembro de 2008. Disponível em:<http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/lei/l11829.htm> Acesso em: 20/10/2015.

Brasil. Lei nº 9.296, de 24 de julho de 1996. Disponível em: <http://www.planalto.gov.br/ ccivil_03/Leis/L9296.htm>. Acesso em: 20/04/2015.

Brasil. Lei nº 8.069, de 13 de julho de 1990. Disponível em: <http://www.planalto.gov.br/ ccivil_03/leis/l8069.htm> Acesso em: 21/05/2015.

Brasil. Lei nº 12.737, de 30 de novembro de 2012. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso: 20/10/2015

Brasil. Lei nº 12.965, de 23 de abril de 2014. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso: 22/10/2015

Brasil. Projeto de Lei nº 225/2015. Disponível em: <http://www2.camara.leg.br/proposicoesWeb/>.Acesso:18/11/2015

BRASIL**. Código Penal, Código de Processo Penal, Constituição Federal, Legislação Penal e Processual Penal**. 14ª. ed. São Paulo: Editora Revista dos Tribunais, 2015.

CAPEZ, Fernando. **Curso de direito penal: parte geral**. v. I. 6 ed. São Paulo: Saraiva, 2003.

CAPEZ, Fernando. **Curso de direito penal: parte geral.** v. I. 6 ed. São Paulo: Saraiva, 2009. COMPUTERWORLD.

CASTRO, Carla Rodrigues Araújo de. **Crimes de informática e seus aspectos processuais**. Rio de Janeiro: Lumen Juris, 2003.

COMER, Douglas E. **Internetworking with TCP/IP.** 3 ed. V.2. New Jersey : Prentice Hall, 1995.

COMPUTERWORLD. Ameaça de ciberterrorismo não deve ser subestimada. Disponível em: <http://computerworld.uol.com.br/seguranca/2012/03/04/ameaca-do-ciberterrorismo-naodeve-ser-subestimada/>Acesso em: 21/05/2015.

DAOUN, Alexandre Jean; LIMA, Gisele Truzzi de. Crimes Informáticos: O Direito penal na Era da Informação. Disponível em:<http://www.truzzi.com.br/pdf/artigo-crimesinformativos-gisele-truzzi-alexandre-daoun.pdf >Acesso em 28/03/2012.

FERREIRA, Ivette Senise. **A criminalidade Informática**. In: LUCCS, Newton; SIMÃO FILHO, Adalberto (Coord.) Direito & Internet: Aspectos Jurídicos relevantes. 2. ed. São Paulo: Quartier Latin. 2005.

FRANCO, João Vitor Sias. Princípio da legalidade no âmbito das leis penais. Disponível em: <http://jus.com.br/artigos/14552/principio-da-legalidade-no-ambito-das-leis-penais>. Acesso em: 28/03/2012.

JESUS, Damásio Evangelista, **Direito Penal 2° volume parte especial: dos crimes contra a pessoa e dos crimes contra o patrimônio** / Damásio E. de Jesus – 28 ed. Ver e atual, São Paulo: Saraiva 2007. p.225

JESUS, Damásio Evangelista. **Direito Penal – Parte Geral**. 15a ed. São Paulo: Saraiva, 1991. p.51.

NOGUEIRA, Sandro D"Amato. **Crimes de Informática**. São Paulo: BH Editora, 2008. P.29.

PRIETO, André; GAHYVA, Hercules da Silva. Crimes cibernéticos e a legislação brasileira. Disponível: <http://www.lfg.com.br/public_html/article.php?story=20100608151713149&mode=print>Acesso em: 03/04/2015.

ROQUE, Sérgio Marques. **Criminalidade Informática – Crimes e Criminosos do Computador.** 1 ed. São Paulo: ADPESP Cultural, 2007. SILVA, Jacimar Oliveira da. Tipificação de crimes efetuados pela internet. Disponível em: Acesso em: 02/04/2012.

ROSA, Fabrízio. **Crimes de Informática**. Campinas: Bookseller, 2002.