UNIVERSIDADE DO EXTREMO SUL CATARINENSE – UNESC

CURSO DE DIREITO

GUSTAVO SCARDUELLI DA ROCHA

UMA ANÁLISE DA RESTRIÇÃO DE ACESSO E DE COMPARTILHAMENTO DE DADOS NA INTERNET EM RAZÃO DOS PROJETOS DE LEI EM TRAMITAÇÃO NO CONGRESSO NACIONAL SOB A LUZ DO DIREITO FUNDAMENTAL DE LIBERDADE DE EXPRESSÃO E INFORMAÇÃO

CRICIÚMA

2013

GUSTAVO SCARDUELLI DA ROCHA

UMA ANÁLISE DA RESTRIÇÃO DE ACESSO E DE COMPARTILHAMENTO DE DADOS NA INTERNET EM RAZÃO DOS PROJETOS DE LEI EM TRAMITAÇÃO NO CONGRESSO NACIONAL SOB A LUZ DO DIREITO FUNDAMENTAL DE LIBERDADE DE EXPRESSÃO E INFORMAÇÃO

Trabalho de Conclusão de Curso, apresentado para obtenção do grau de bacharel no curso de Direito da Universidade do Extremo Sul Catarinense - UNESC

Orientador(a): Prof.(a) Alfredo Engelmann Filho

CRICIÚMA

2013

GUSTAVO SCARDUELLI DA ROCHA

UMA ANÁLISE DA RESTRIÇÃO DE ACESSO E DE COMPARTILHAMENTO DE DADOS NA INTERNET EM RAZÃO DOS PROJETOS DE LEI EM TRAMITAÇÃO NO CONGRESSO NACIONAL SOB A LUZ DO DIREITO FUNDAMENTAL DE LIBERDADE DE EXPRESSÃO E INFORMAÇÃO

Trabalho de Conclusão de Curso aprovado pela Banca Examinadora para obtenção do Grau de Bacharel, no Curso de Direito da Universidade do Extremo Sul Catarinense, UNESC, com Linha de Pesquisa em Crimes Digitais.

Criciúma, 10 de dezembro de 2013.

BANCA EXAMINADORA

Prof. Esp. Alfredo Engelmann Filho - (UNESC) - Orientador

Prof. Esp. João Raphael Gomes Marinho - (UNESC)

Profª Msc. Marciele Berger Bernardes - (UNESC)

Este trabalho é dedicado a todos que direta ou indiretamente contribuíram em minha formação acadêmica.

AGRADECIMENTOS

Agradeço a Deus pelo dom da vida e ao privilégio de poder estudar e chegar até este ponto para viver este momento.

Agradeço a meus pais, José Carlos e Cláudia, pelo amor incondicional em todos os momentos de minha vida e também pela sólida educação recebida e que continuo a receber.

Agradeço a todos os meus familiares, em especial meu querido irmão Leandro, por todo o apoio recebido e a compreensão nos momentos de ausência para a elaboração deste trabalho.

Agradeço a Marina pela compreensão nos momentos de ausência e pelo auxílio na construção desta monografia. Agradeço ao meu orientador, Professor Alfredo pela participação no exame de qualificação e pela leitura atenta do projeto, cujas sugestões serviram para a elaboração deste trabalho.

Agradeço a todos os meus amigos e a todos aqueles que, direta e indiretamente, contribuíram para a elaboração deste trabalho.

"O que não for posto em questão, nunca será provado".

Diderot (1713-1784)

RESUMO

A disseminação dos meios de comunicação permitiu o acesso facilitado à internet. Essa disseminação expressiva do uso da rede de computadores proporcionou aos criminosos mais uma ferramenta para a prática de crime. Em virtude do prática delituosa surgiram questionamentos a cerca da tipificação das condutas criminosas no meio virtual para impor sanções coercitivas aos cibernéticos, sem classificar como crimes as práticas habituais, não violando Direito Fundamental de Liberdade de Expressão e Informação. O Código Penal Brasileiro não abrange punição para tais crimes. Contudo, a necessidade de punir as práticas criminosas na rede trouxe consigo a indispensabilidade de uma reformulação do Código Penal. Foram apresentados na Câmara alguns projetos de lei para tentar tipificar as condutas delituosas. O Direito Digital é um novo ramo do direito que se propõe a estudar os aspectos jurídicos do uso de computador das tecnologias da informação e comunicação, visando regulamentar as relações sociais decorrentes no mundo virtual. O presente trabalho tem como princípio discorrer a cerca dos projetos que tramitam na Câmara. Para isto, foi realizado um estudo sobre os mesmos, demonstrando claramente a importância e a necessidade de normas jurídicas para a resolução dos conflitos que dizem respeito ao Direito Digital.

Palavras-chave: Direito Digital. Conflitos. Normas Jurídicas. Crimes. Internet. Liberdade de Expressão

SUMÁRIO

1. INTRODUÇÃO

O homem, ser racional dotado de inteligência vem desenvolvendo mecanismo para facilitar o seu trabalho. Muitos foram os esforços para conseguir máquinas capazes de realizar alto poder de processamento. A evolução das tecnologias da informação e comunicação está atrelada aos períodos de guerra e revoluções. Durante a guerra fria, na década de 60, o governo americano desenvolveu o projeto ARPANET (*Advanced Research Projetcts Agency*), com o intuito de interligar computadores militares e industriais. A ARPANET evoluiu rapidamente, alcançando dezenas de universidades e empresas, recebendo diversas contribuições para o seu aperfeiçoamento. (GOUVÊA, 1997).

A invenção que tornou possível a popularização da internet em todo o mundo foi a *World Wide Web* também conhecida de WWW, desenvolvida por Tim Berners-Lee em 1990. A Web, como ficou conhecida, nada mais é de que um espaço onde as informações, armazenadas nos milhões de computadores da rede, podem ser acessadas através de qualquer meio computacional. A internet está presente em todos os ambientes podendo ser acessada de diversos dispositivos eletrônicos como o celular, tablet, notebook.

Com o surgimento da internet e a disseminação dos meios de comunicação, surgiram também os crimes cometidos com o uso desta ferramenta. Esse tipo de crime recebeu o nome de ***cibercrimes***, nome criado no final da década de 90, à medida que a Internet se disseminava pelos países da América do Norte. A internet se tornou um recurso indispensável para as empresas e pessoas, devido a sistemas online, pesquisas e atualizações.

Atualmente, no Brasil, existe somente uma lei apelidada de Lei Carolina Dieckmann, a Lei dos Crimes Cibernéticos (12.737/2012), para regular crime de violação indevida de sistemas de computadores ou dispositivos, conectados a rede de computadores, com o intuito de obter, adulterar ou aniquilar dados ou informações sem o consentimento do usuário ou, ainda, para instalar vulnerabilidades.

Dentre os crimes digitais comumente empregados está o furto de dados bancários e senhas através do envio de e-mails com pedidos falsos de atualização. Outro meio de obtenção de dados alheios são os vírus de computador, que resultam em fraudes bancárias e financeiras, por acesso indevido à sites e e-mails.

Não obstante, os crimes mais cometidos na rede são a pirataria, o racismo, o cyberbulling, a apologia ao consumo e a comercialização de drogas, a pedofilia e o tráfico de pessoas. Tem sido constantes as ocorrências de crimes contra a honra, tais como a calúnia, a

injúria e a difamação, principalmente nas redes sociais.

Em decorrência destes fatos e da disseminação dos meios de comunicação que vêm proporcionando o aumento do número de indivíduos conectados à rede mundial de computadores, surgiu o Direito Digital visando criar normas jurídicas para orientar e salvaguardar os internautas diante dos crimes digitais nos mais diferentes meios e locais de acessos.

No Congresso Nacional tramitam alguns Projetos de Lei, com o objetivo de criar uma regulamentação específica para tipificar e punir os crimes praticados na rede.

Quanto à metodologia, este trabalho foi realizado através do método dedutivo, levantamento teórico em livros, artigos, revistas especializadas, bem como pesquisa jurisprudencial.

O objetivo geral deste trabalho é analisar a discussão dos Projetos de Lei de Cibercrimes em trâmite no Congresso Nacional, em face do Direito Fundamental de Liberdade de Expressão e Informação garantidos por Lei.

Os objetivos específicos deste trabalho são: Analisar o histórico da evolução dos cibercrimes e a liberdade de expressão e informação nos meios eletrônicos; Estudar os projetos de lei em trâmite no Congresso Nacional e suas restrições; Verificar os projetos e os limites impostos ao direito fundamental de liberdade de expressão e informação.

2. DOS CIBERCRIMES

O homem sempre desenvolveu a ideia da busca e obtenção de riqueza e bens. A riqueza sempre vem acompanhada de conflitos e, consequentemente, onde há conflito há também a atuação do Direito. Todas as regras sociais ordenam uma conduta, tanto as morais quanto as jurídicas e as convencionais. A maneira como estas regras são ordenadas difere umas das outras. É próprio do Direito ordenar a conduta de maneira bilateral e atributiva, ou seja, estabelecendo uma relação de exigibilidade segundo a proporção objetiva. O Direito não visa ordenar as relações dos indivíduos entre si para satisfação dos mesmos, mas realizar a convivência ordenada que se traduz no bem comum (REALE, 1999).

Com a tradução do bem comum surgiu à ideia de desenvolver-se uma máquina capaz de realizar o processamento de dados. Deve-se salientar que os passos que impulsionaram o desenvolvimento de uma máquina capaz de realizar o processamento de dados nos remete a antiguidade. Segundo Kowaltowski (1996) e Fonseca (2007), foi nesse período que foram dados os primeiros passos a fim de conseguirem-se formas de realizar cálculos de maneira automatizada, utilizando assim pedras e outros dispositivos, sendo esses cálculos realizados através dos *ábacos*. Desde então, muitos são os esforços humanos para conseguirem-se máquinas capazes de processar amplos volumes de dados. Leonardo Da Vinci foi o responsável por ideias de uma somadora mecânica. Em meados de 1600 surge então a *pascalina*, primeira somadora mecânica, desenvolvida por Blaise Pascal. Em 1801, Joseph Marie Jacquard inventa um tear mecânico, com uma leitora automática de cartões (KOWALTOWSKI, 1996).

O breve contexto histórico sobre a evolução dos computadores, foi embasada nos estudo de Kowaltowski (1996) e Fonseca (2007). O século XVIII é responsável por grandes avanços, representados, por exemplo, por Charles Babbage que desenvolveu a máquina de diferenças e a máquina analítica e por Hollerit responsável por uma perfuradora e tabuladora de cartões. No século XIX, tem-se avanços com o surgimento da máquina universal capaz de executar qualquer algoritmo e formando a base da computação, por Alan Turing. Em 1943, em um projeto coordenado pelo mesmo surgiu o Colossus um computador inglês utilizado na segunda guerra mundial. Em 1944, contribuiu de forma direta no projeto de fabricação de computadores, assessorando a Eckert e John Machly, criadores posteriormente do ENIAC e que construiriam mais tarde o UNIVAC em 1950. Durante 1936 e 1939, o engenheiro alemão

Konrad Zuse construiu o primeiro computador eletromecânico binário programável, o qual fazia uso de relés elétricos para automatizar os processos. John V. Atanasoff tem o crédito da patente do primeiro computador digital (1939). Em 1946 foi desenvolvido o computador conhecido por Eniac pelos cientistas norte-americanos John Presper Eckert e John W. Mauchly, da *Electronic Control Company*. Esses dois pesquisadores da Universidade da Pensilvânia, tinham o propósito de construir uma máquina com a finalidade de acompanhar as trajetórias de foguetes. O ENIAC pesava em torno de 30 toneladas e ocupava uma área de 140 metros quadrados. Para funcionar precisava de 18.000 válvulas eletrônicas. (GOUVÊA, 1997 p. 31-32).

Após o desenvolvimento do ENIAC começaram a surgir os computadores eletrônicos os quais se dividiam em dois grupos: os analógicos e os digitais. Os computadores analógicos, do grego *análogos*, isto é, proporcionado, não trabalhavam diretamente com números mas, sim, com expressões físicas como a voltagem e a tensão. Nos computadores digitais do latim *digitus*, ou seja, dedo, as informações numéricas são transformadas em códigos binários, pois o mesmo trabalha com os sinais elétricos binários 1 e 0 (GOUVÊA, 1997, p.32).

As grandes inovações sempre almejaram amenizar os trabalhos repetitivos e bitoladores, assim surgiu o computador:

> Foi na tentativa de livrar-se de trabalhos repetitivos e bitoladores que o homem, há muito tempo, criou as operações de cálculo. A palavra cálculo teve sua origem na expressão latina *calculus*, que a milhares de anos servia para denominar pequenas pedras que eram usadas para contar, deslizando-se por sulcos cavados no chão. Este meio de efetuar operações matemáticas, descoberto recentemente em escavações arqueológicas, recebe o nome de ábaco cujo aperfeiçoamento resultou no primeiro dispositivo manual de cálculo conhecido e sua versão mais antiga data do ano do 3500 (três mil e quinhentos) anos A.C. Numa variante mais moderna, concebida na China 2600 (dois mil e seiscentos) anos A.C., o ábaco era usado com sucesso para representar números no sistema decimal e realizar operações matemáticas (PIMENTA, 2000, p. 5- 6).

A matemática fundamentou os pilares da computação, na medida em que o homem inventava o sistema decimal e o método de multiplicação, descobria que o produto de uma operação multiplicadora conduzia sempre a um resultado (PIMENTEL, 2000, p.5).

Com o advento do computador, cálculos complexos deixaram de ser um enorme problema. O conceito de computador deve ser estendido além das máquinas eletrônicas modernas, experimentos, instrumentos e máquinas menos sofisticadas mais que, ao seu

tempo, desempenharam com real eficácia os propósitos aritméticos colimados (PIMENTEL, 2000, p.5).

Gouvêa em seu texto conceitua o termo computador:

> O termo computador vem do latim *computadore* e significa "aquele que faz cômputos, que calcula". Os homens primitivos fizeram os primeiros cálculos com o uso dos dedos, posteriormente, passaram a utilizar pedras ou seixos. A palavra cálculo vem do latim *calculus*, que significa pequena pedra. Os Ábacos, primeiras máquinas de calcular não mecanizadas (pedras que deslizavam presas em fios), são usados até hoje em alguns países orientais e por deficientes visuais (GOUVÊA, 1997, p.31).

O computador é a parte nuclear do direito cibernético, que interliga com a informática e a cibernética. Cibernética de acordo com WIENR, apud VIENNA, 2001, é uma palavra empregada para nomear informática ou computação. A palavra cibernética tem origem Grega *Kubernetes* (timoneiro). O objetivo da cibernética é a sistematização de uma teoria geral de controles, com isso ela estuda as diversas formas de controles e as leis. Essa interligação ficou bastante aclamada por Limongi França, quando este observou que "a informática é a parte da cibernética que estuda os sistemas determinísticos". Com vistas à sua execução em um computador eletrônico e estudando também o modo pelo qual o computador irá processá-lo, concluiu que era necessário estar familiarizado com os princípios da cibernética e com as noções relativas ao processamento eletrônico de dados (PIMENTEL, 2000, p.23).

2.1 HISTÓRICOS DO DESENVOLVIMENTO DA INTERNET

A interligação de um computador a outro é feita pela internet, considerada a mãe de todas as redes ou redes das redes. A internet pode ser vista como:

> [...] um sistema global de rede de computadores que possibilita a comunicação e a transferência de arquivos de uma máquina a qualquer outra máquina conectada na rede, possibilitando, assim, um intercâmbio de informações sem precedentes na história, de maneira rápida, eficiente e sem a limitação de fronteiras, culminando na criação de novos mecanismos de relacionamento (CORRÊA, 2000, p. 8).

A origem dessa grande rede foi na década de 60 na Guerra Fria. O governo americano desenvolveu o projeto ARPANET (*Advanced Research Projetcts Agency*), com o intuito de interligar computadores militares e industriais. A primeira ligação, feita entre quatro computadores da Califórnia e de Utah, usava uma tecnologia especialmente desenvolvida para

esse fim, através de pacotes enviados pela rede telefônica. A preocupação dos militares era manter a rede funcionando no caso de um ataque nuclear. Era, portanto, imprescindível que houvesse um centro de controle que não pudesse ser destruído. A imensa rede telefônica, que se estendia por todo país, tornou possível a implementação do projeto. A ARPANET se expandiu rapidamente, alcançando dezenas de universidades e empresas, contribuindo para o seu aperfeiçoamento. (GOUVÊA, 1997, p.37).

A invenção que tornou possível a popularização da internet em todo o mundo foi a *World Wide Web* também conhecida de WWW, ou teia de alcance mundial, que foi criada pelo físico Inglês Tim Berners-Lee em 1990, na Suíça, no laboratório de partículas físicas. A Web, como ficou conhecida, nada mais é de que um espaço onde as informações, armazenadas nos milhões de computadores que formam a internet, podiam ser acessadas com um simples clique do *mouse*. Isso era possível através da tecnologia do hipertexto, que permitia a ligação de diversos textos e arquivos, que são os links, tornando-o disponível para qualquer computador conectado à internet (VIEIRA, 2003, p.8).

No início, a maneira como a informação era vista não era muito agradável. *Mosaic* foi o primeiro programa de navegação da história. Esse software fez com que a internet abandonasse o mundo das letrinhas verdes e ganhasse uma interface gráfica. Com isso, as pessoas puderam não apenas compartilhar textos e arquivos, como ocorria mas, também, imagens, som e gráficos em locais de atualização dinâmica, que denominou-se *sites*. Esses sites são semelhantes às páginas das revistas mas em tela de computador (VIEIRA, 2003).

Em 1994, o governo Federal manifestou a intenção de investir e promover o desenvolvimento da internet no país, numa ação com o Ministério da Ciência e Tecnologia e das Comunicações. A responsabilidade de monitorar o serviço de comunicação no Brasil caberia exclusivamente a Embratel. Ocorreu que, com a eleição presidencial de 1994, que trouxe consigo uma agenda política que previa um amplo programa de privatizações, incluindo a descentralização do setor de telecomunicações. Após a eleição foi eleito como presidente da República Fernando Henrique Cardoso, bastou ele assumir o Palácio do Planalto, em 1° de janeiro de 1995, para que planos da Embratel assumir sozinha o mercado de Internet, serem freados bruscamente (VIEIRA, 2003, p.10).

No Brasil, o primeiro contato com a internet ocorreu em 1988 quando a Fundação de Amparo à Pesquisa do Estado de São Paulo (Fapesp), ligada a Secretaria Estadual de Ciência e Tecnologia, realizou a primeira conexão a rede através de uma parceria com o *Fermilab*, que era um dos mais importantes centros de pesquisas científicas dos Estados Unidos. Essa

tarefa coube aos professores Oscar Sala e Flávio Fava de Moraes, da Universidade de São Paulo (USP), que tocaram o projeto em conjunto e inauguraram a conexão oficialmente no ano seguinte. Na época, a Universidade Federal do Rio de Janeiro (UFRJ) e o Laboratório Nacional de Computação Científica (LNCC), em Petrópolis Rio de Janeiro, também se conectaram a internet através de links com universidades americanas (VIERA, 2003, p.8-9).

A internet proporcionou um avanço no mundo do desenvolvimento tecnológico e digital. Conforme os pensamentos de Takahashi (2000), a primeira forma de convergência da base tecnológica, decorre do fato de poder-se representar e processar qualquer tipo de informação de uma única forma, a digital. Através da digitalização, a computação, as comunicações (transmissão e recepção de dados, voz, imagens etc.) e os conteúdos de (livros, filmes, pinturas, fotografias, música etc.) sendo inseridos no computador, fazendo com que o mesmo torne-se um aparelho de TV, a foto favorita sai do álbum para um disquete e, pelo telefone entra-se na Internet. Um extenso leque de aplicações abre-se com isso, função apenas da criatividade, curiosidade e capacidade de absorção do novo pelas pessoas.

Num período de 8 anos a internet se disseminou por todo o mundo, proporcionando conectividade a países até então fora da rede, substituindo outras tecnologias mais antigas. Mesmo com a expansão da internet, muitos países tem esse serviço restrito a poucos, comparando a velocidade de disseminação da internet com outros serviços. Isso reflete que ela se tornou um padrão de fato, e está diante de um fenômeno a ser considerado como fator estratégico fundamental para o crescimento e desenvolvimento das nações (TAKAHASHI, 2000, p.4).

A internet está presente em todos os ambientes: no trabalho, no lar, no ambiente escolar, enfim o mundo não consegue mais viver desconectado. Podemos acessá-la das mais diferentes formas, seja através dos mais variados dispositivos móveis como o celular, o tablet, o notebook, enfim até em nos passeios familiares de domingo pode-se estar conectado, basta ter uma rede de acesso disponível para acessar e começar a trocar milhares de informações via internet. Uma recente reportagem publicada na revista Abril em dezembro de 2011 relata que segundo a F/Nazca S&S que está em sua 10ª edição da F/Radar, relacionada com pesquisa sobre tendências e comportamento na internet realizada semestralmente, em parceria com o Datafolha e trás os seguintes dados:

- 29,5 milhões de brasileiros com mais de 12 anos costumam se conectar a rede por meio de dispositivos móveis, sendo que a maior parte deles, 74%, utiliza o celular para tal fim. Desde a última medição, o índice aumentou 7%.
- A pesquisa identificou ainda que 79% dos que se conectam em movimento o fazem por meio de planos pré-pagos de telefonia e que 16% deles, cerca de cinco milhões de pessoas, já fizeram compras usando o recurso (IBOPE, 2012).

Esta pesquisa relata a atual situação da rede mundial de computadores e trás, também, que tanto crianças como adultos vivem conectados das mais variadas formas.

Segundo o escritor do Livro Verde, Takahashi (2000), no Brasil urge um acelerado processo de articulação efetiva de um programa nacional para a sociedade da informação. Em meados da década de noventa, registrou-se o sucesso na implantação de tal programa. A internet no Brasil teve um grande avanço, referente a comunidade científica, e se destacou como plataforma de expansão do setor privado, estando presente também nos serviços de natureza comercial desde 1995. Na área de telecomunicações, ocorreu o processo de privatização do sistema brasileiro, e a criação da Agência Nacional de Telecomunicações (ANATEL), permitindo a maior e a mais rápida disponibilidade de acesso aos meios de comunicação. Com a Internet, as atividades comerciais no Brasil estão se destacando com enorme expressão, ganhando metade do mercado latino-americano, em número de usuários e em volume de transações e negócios. Com essa expansão da Internet no âmbito comercial e algumas aplicações do governo, tem-se uma grande melhoria tanto da eficiência interna de funcionamento como na prestação de serviço aos cidadãos. Fazendo uma comparação com a América Latina, no país existe uma sofisticada base tecnológica instalada com considerável plantel de recursos humanos qualificados, evolvendo desde pesquisa até fomento e empreendimento (TAKAHASHI, 2000, p. 7).

Quanto ao provimento da internet, do ponto de vista técnico, não pode haver um embaraço para que as empresas de telecomunicações (prestadoras de serviços de telefonia fixa ou televisão a cabo) realizem o provimento de acesso à internet, essa dificuldade resultou de uma opção legislativa, estabelecida pela lei geral das telecomunicações, a Lei nº 9.472, de 16 de julho de 1997, que define serviços de telecomunicações em seu art. 60 e serviços de valor adicionado, no qual se incluem os provedores de acesso à internet, em seu art. 61 (PINHEIRO, 2007, p. 43).

Conforme a Lei nº 9.472/97, o serviço de telecomunicações é o conjunto de atividades, que possibilita a oferta de telecomunicação. Desta forma a telecomunicação e a transmissão, emissão ou recepção, por fio, radioeletricidade, meios ópticos ou qualquer outro processo eletromagnético, de símbolos, caracteres, sinais, escritos, imagens, sons ou informações de qualquer natureza (PINHEIRO, 2007, p. 60).

A Lei nº 9.472/97 prevê expressamente, em seu artigo 61, § 1°, que os serviços de valor adicionado não constituem serviços de telecomunicações. Os provedores de acesso à internet são, de acordo com a lei, usuários do serviço de telecomunicações que lhes dão suporte (PINHEIRO, 2007, p.62).

O serviço de conexão à internet e a regulamentação do uso de meios da rede pública de telecomunicações para o acesso à internet estão previstos na Norma 004/97 da Agência Nacional de Telecomunicações (ANATEL), em seu art. 41 (TOURINHO, 2003, p. 68).

A implantação dessa infra-estrutura é hoje estratégia para muitos países e blocos econômicos, para poderem melhorar a sua competitividade e a qualidade de vida de seus cidadãos. Os países que não acompanharem esse tipo de tendência correm o risco de ficar à margem do desenvolvimento da nova economia. Por tratar-se de países em desenvolvimento como o Brasil, o desnível tecnológico em relação aos países avançados pode acentuar-se e as desigualdades sociais e econômicas aprofundarem-se ainda mais. Para países em desenvolvimento, é prioritária a implantação da Internet na nova geração do país. A viabilização desse projeto requer comunicação avançada e segura, a partir da utilização de circuitos de alta velocidade, com elevada capacidade de tráfego. Sobre essa infra-estrutura, é preciso atribuir ênfase especial ao desenvolvimento de serviços e aplicações em áreas sociais, comerciais e estratégicas, pois o "que fazer" torna-se muito mais importante do que a rede em si (TAKAHASHI, 2000, p.9).

Passada a primeira parte de implantação e a par de uma segunda parte da implantação da internet no Brasil, começou a haver foco crescente em aspectos legais e temas correlatos, tais como padrões e autor regulamentação, classificação de conteúdos e crimes no mundo eletrônico (TAKAHASHI, 2000, p.108).

A Internet nos dias de hoje é um dos veículos mais eloquentes de comunicação, através de um simples clique podemos estar interligados com todo o mundo, acessando todos os sites disponíveis na rede. A Internet expandiu e acompanhando esse avanço surgiram também as novas modalidades de crimes ou novas práticas de crimes já existentes em nosso

ordenamento jurídico, mas agora através da rede. Com esse avanço um dos assuntos mais discutidos na atualidade é quanto à tipificação e imputação penal aos praticantes de tais atos delitivos (INELLAS, 2009, p. 73).

Segundo os pensamentos de Ferreira (2005), a internet não tem um proprietário, não tem nacionalidade e não está em território algum. Os cibercrimes podem atingir mais de uma pessoa, em território diverso, com leis distintas. Portanto, é conhecida como jurisdicional. Assim uma mensagem pode viajar por vários países: localização física e territorial, sendo considerado um espaço amplo, onde as pessoas consideram um paradigma de liberdade.

2.2 DOS CRIMES RELACIONADOS COM A INTERNET

Rosenoer (1996) em sua obra, analisa vários aspectos em relação à regulação da internet nos Estados Unidos. O autor apresenta uma série de julgamentos e os resultados a que se chegou. Um dos casos expostos, é o de um estudante que foi preso por publicar uma mensagem de ficção violenta de matéria sexual em seu grupo de internet e nomeou a personagem principal com o mesmo nome de sua colega de sala, ficando evidente um crime contra a honra. Ao acompanhar a troca de e-mails do estudante com outro, verificou-se conteúdo persistente de violência contra mulheres em geral. As histórias influenciavam a tortura, o estupro e o assassinato de mulheres, inclusive de uma colega. O juiz, ao analisar o caso, constatou que o estudante era um perigo para a comunidade. Entrementes, após recursos, as demais instâncias concluíram que o caso citado era fraco do ponto de vista jurídico, sendo um caso de necessidade de uma ação disciplinar.

Para explicar melhor o que seria honra, Cavalieri conceitua:

> [...] honra é o conjunto de predicados ou condições de uma pessoa, física ou jurídica, que lhe conferem consideração e credibilidade social; é o valor moral e social da pessoa que a lei protege ameaçando de sanção penal e civil a quem a ofende por palavras ou atos. Fala-se, modernamente, em honra profissional como uma variante da honra objetiva, entendida como valor social da pessoa perante o meio onde exerce sua atividade (CAVALIERI, 1997, p. 80).

Conforme o artigo 5º inciso X da Constituição da República Federativa do Brasil de 1988, referente à honra:

> 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;

Vladimir Aras expõe o problema ao trabalhar com a jurisdição e territorialidade da internet, pois se trata de um mundo onde não existem fronteiras. Tudo que é publicado na rede torna-se visível a todo o mundo, enfatizando a disseminação da informação, como pode ser relatado:

> "O grande problema ao se trabalhar com o conceito de jurisdição e territorialidade na Internet reside no caráter internacional da rede. Na Internet não existem fronteiras e, portanto, algo que nela esteja publicado estará em todo o mundo". (ARAS, 2001, p.19)

Em contrapartida, Rosenoer (1996), ressalta que os abusos cometidos por pessoas que utilizam do esquecimento para praticar crimes como difamação, violação aos direitos autorais, lavagem de dinheiro, pornografia, racismo, entre outros tantos crimes através da internet, utilizando-a como ferramenta de práticas criminosas, implica na necessidade de oferecer aos provedores de internet vantagens em denunciar tais práticas a fim de evitar que o poder do computador seja uma ameaça aos direitos de privacidade individuais.

Segundo Sieber (1993 apud Gouvêa 1997), divide-se os crimes por computador em três grupos:

1- Crimes Econômicos;

> 1.1 Fraude por manipulação de dados em sistemas de processamento de dados, que pode de ser feita através de inserção ou posterior modificação dos dados, visando à obtenção de vantagens sobre os bens, sejam estes corpóreos ou incorpóreos. Exemplo destes bens são depósitos monetários, horas extras de trabalho, resultados de cálculos de balanços etc. Dentre os corpóreos, pode-se citar dinheiro em espécie e mercadoria.
> 1.2 Espionagem de dados e pirataria e programas. O principal alvo são os programas de computadores que contêm preciosas informações, como contabilidade, balanço e lista de endereço.
> 1.3 Sabotagem. A forma mais comum, porém, se dá através da colocação de vírus, isto é, um programa capaz de apagar ou modificar em pouco tempo grande quantidade de informação. Este tipo de conduta também pode ser realizado através de redes de telecomunicação. Os agentes da sabotagem são, em geral empregados de empresas ou terroristas que agem por ideologia.
> 1.4 Furto de serviço, também denominado furto de tempo. O objeto da conduta é o processamento de dados ou programas uso próprio dos empregados da empresa. Em alguns caso, esta conduta não causa dano considerável, mas pode ferir os interesses da empresa, em especial se usadas em computadores alugados. Ou então, se há perda de clientes em razão de sistema bloqueado ou congestionado.
> 1.5 Acesso não autorizado a sistemas de processamento de dados, via remota ou *hacking*, independente de interesse econômico, fraude ou sabotagem, podendo ser caracterizado como uma forma especial de furto de serviço. É frequentemente

> cometido por jovens, que destroem dados com o objetivo de bloquear sistemas de computador ou de descobrir deficiências em sistemas de segurança alheio que permitam, posteriormente, fraudes financeiras.
> 1.6 Uso do computador para crimes empresariais. Ocorre quando as empresas sofrem prejuízo em razão da manipulação de seus computadores, principalmente por empregados da própria empresa. Estes casos envolvem a manipulação de rendas administradas por computadores, contas, balanços e etc. (SIEBER apud GOUVÊA, 1997, p. 62-64).

2- As Ofensas contra Direitos Individuais:

> 2.1 Uso incorreto de informação, subdividido nas seguintes formas de abusos: (a) manipulação e rasura de dados por pessoas não autorizadas, (b) obtenção, arquivo, processamento ou revelação de informação incorreta pelo seu legitimo proprietário.
> 2.2 Obtenção ilegal de dados e posteriores arquivo das informação, já que o uso indevido desses dados, mesmos corretos, pode causar enormes prejuízos. A obtenção destas informações pode ocorrer de diversas formas, como o acesso indevido a arquivos. Outro aspecto é o arquivamento de informação cujo o conteúdo não deveria ser mantido. Uma das grandes indagações é a de se saber quem pode manter em arquivo determinadas informações; esta é uma das maiores questões no que concerne à proteção da privacidade.
> 2.3 Revelação ilegal e mau uso de informação. A princípio, cabe a distinção entre informações pessoais sigilosas e não sigilosas. As primeiras podem ser obtidas por meios legais (especialmente nos campos médicos e bancários), mas usadas para outros fins. Em relação às informações não confidenciais, é difícil delimitar quando a informação foi usada de forma abusiva, ilegal ou criminosa.
> 2.4 A dificuldade de se distinguir entre obtenção, arquivamento ou revelação de informação de forma legal ou ilegal fez com que alguns países, como a França, regule a forma de registro ou licença de processamento ou transmissão de dados pessoais. A infração a estas normas pode acarretar sansões penais. (SIEBER apud GOUVÊA, 1997, p. 64).

3- As ofensas contra Direitos Supra-Individuais:

> 3.1 Ofensas contra interesses estaduais e políticos: são os crimes cuja matéria é de interesse do Estado, no campo político, administrativo e judicial. A manipulação de contagem de votos em eleições ou a mudança de resultado de laudo pericial de questões jurídicas são alguns dos exemplos desta categoria.
> 3.2 A extensão desta categoria para crimes contra a integridade humana pode ser exemplificada pelo acidente ocorrido em janeiro de 1979 no Aeroporto JFK, em Nova Iorque. A bordo de um avião encontrava-se um embaixador russo. Os computadores foram manipulados, intencionalmente, por um controlador de tráfego aéreo, causando o desastre (SIEBER apud GOUVÊA, p. 65).

Conforme Temer, as disposições quanto à certificação das assinaturas eletrônicas existentes no Poder Legislativo estão medindo esforços para regulamentação do comércio eletrônico e para os contratos eletrônicos. Angela Bittencourt Brasil (2000) conceitua a palavra assinatura eletrônica, onde relata que é um emaranhado de números que somente poderá ser codificado para quem tem acesso, para quem possui uma chave privada e a sua descodificação deverá ser feita por meio de uma chave pública. Na Câmara dos Deputados estão em tramite algumas proposições legislativas à Internet objetivando principalmente, coibir crimes, proteger a privacidade das pessoas, disciplinar a assinatura eletrônica e

promover a inclusão digital. As questões referentes a assinatura eletrônica caracterizam a identificação do usuário e são de suma importância para que somente quem tenha acesso as informações sejam os usuários responsáveis pela mesma, e não pessoas com intenções duvidosas (TEMER, 2001, p. 108).

Segundo Ferreira, ao mencionar a identificação dos delinquentes da Internet, ressalta que os operadores da rede deverão se modificar, oferecendo aos provedores mecanismos para que se possam rastrear as operações na internet em tempo real, identificado os delinquentes da rede:

> [...] no que se refere a internet, os provedores deverão modificar as suas infraestruturas para poderem oferecer um interfaz (mecanismo) a partir do qual as comunicações interceptadas poderão ser transmitidas a instalações de vigilância, permanentemente e em tempo real; também deverão estar em condições de proporcionar o número da conta, senha, endereço de e-mail e etc. Dessa forma, se aprovada a incidência da resolução, incidirá nos próprios operadores de redes e provedores de serviços, sem os quais será impossível rastrear os passos do delinquente informático e proceder a sua identificação (FERREIRA, 2004, p. 35-36).

Rosenoer (1996), enfatiza que, por falta de leis referentes aos crimes praticados com o uso da Internet, o meio para que se possa ter uma base legal para o julgamento, é se baseando na jurisprudência dos Tribunais. Isso mostra a necessidade de ter uma lei específica para esses tipos de crimes. Essa questão de jurisdição para os crimes de Internet tem gerado alguns desafios, necessitando-se de uma legislação que puna o autor responsável pela mensagem criminosa. Grandes questões são levantadas: quais medidas a serem tomadas para promover a liberdade de expressão, a liberdade de atuação de provedores ao perceber esse tipo de delito na internet e a necessidade de regulação para evitar os atos de má-fé que rondam a rede, esses são tipos de medidas a serem tomadas para coibir crimes.

Ao falar da regulação da Internet Rosenoer (1996), analisa-se a regulamentação sobre dois preceitos, onde visam: a) a regulação da Internet onde cabe ser estudada especificamente nos casos dos contratos eletrônicos, as assinaturas eletrônicas, a certificação do que está sendo entendido como regulação e, em grau menor, as garantias dos direitos autorais, que são os certificados e outros documentos a serem produzidos, bem como a proteção legislativa dos softwares e ainda, em grau mais inferior, a regulação de mensagens no caso de crimes contra a honra pessoal; b) ao tratar-se dos crimes contra a honra, a regulamentação é estendida aos casos retroativos, ou seja, sobrevindo a responsabilidades aos provedores de guardar consigo os dados violados, para que depois a vítima ao apresentar a queixa, os mesmos tomem providência, descobrindo as identidades dos autores. As questões a serem colocadas referem-se, principalmente, à extensão em que os provedores são ou não são vistos como meros

transmissores ou como editores e produtores de textos. Eventualmente os provedores censuram ou atuaram as mensagens no sentido de coibir, ou até mesmo alterá-las, em razão do que percebem a mensagem como difamatória. Esses provedores passam, a ser percebidos como editores e produtores, assim eles correm o rico de sofrerem punições em casos que não coíbem tais mensagens.

Castro, realiza uma abordagem de crimes na internet e suas regulações aos crimes contra a honra previstos no Código Penal que são: calúnia, difamação e injúria, disciplinados nos artigos 138, 139 e 140. Ao analisar tais crimes no contexto da internet, Castro afirma que, tanto a calúnia quanto a difamação, ferem a honra objetiva e, para a sua consumação, deve ficar provado que uma terceira pessoa toma conhecimento do fato. É o caso de homepage ou salas de bate-papo, onde várias pessoas terão acesso a essas ofensas (CASTRO, 2003, p. 64).

Em sua obra, Damásio E. de Jesus, explana que a honra é subdivida em subjetiva e objetiva:

> "Honra subjetiva é o sentimento de cada um a respeito de seus atributos físicos, intelectuais, morais e demais dotes da pessoa humana. É aquilo que cada um pensa a respeito de si mesmo em relação a tais atributos. Honra objetiva é a reputação, aquilo que os outros pensam a respeito do cidadão no tocante a seus atributos físicos, intelectuais, morais etc. enquanto a honra subjetiva é o sentimento que temos a respeito de nós mesmos, a honra objetiva é o sentimento alheio incidido sobre nossos atributos". (JESUS, 2005, p. 201)

De acordo com o entendimento de Sofia de Vasconcelos Casimiro, a Internet proporciona, várias formas de acesso e navegação sem que a identidade de seus usuários seja revelada:

> "[...] a possibilidade dos seus utilizadores atuarem sem que seja revelada a respectiva identidade, facilitando as situações de anonimato do autor da lesão. Por anonimato do autor da lesão entendemos a não identificabilidade ou a indeterminabilidade concreta desse autor. Como bem refere Graham Smith, reportando-se à responsabilização por atuações ilícitas praticadas na Rede, o primeiro desafio é identificar o infrator. A identificação do autor da lesão pode, de fato, revelar uma árdua tarefa e nem sempre será efetuada com êxito. Mesmo nos casos em que consigam superar-se os primeiros entraves a essa identificação, eventualmente afetos aos deveres de acesso, vários outros entraves podem erguer-se ao longo dessa investigação. Assim, o autor pode esconder-se por detrás de um operador que ofereça o serviço de retirar a identidade das mensagens enviadas por correio eletrônico e de reenviá-las sem essa identidade (*remailer*). Para além dessa hipótese, o autor pode utilizar uma falsa identidade (atuação esta que se encontra muito facilitada pelo fato dos próprios fornecedores de acesso não exigirem, por regra, a comprovação dessa identidade no momento da celebração do respectivo contrato)(CASIMORO, 200, p.77-78)".

No Brasil, já existem alternativas para combater crimes praticados na internet. O site SaferNet Brasil apresenta algumas formas de combate ao *ciberbullying*, tanto preventivas

quanto reativas, definido-as como “cibercrimes” que são: práticas criminosas, como roubo, chantagem, difamação, calúnia e violações aos direitos humanos fundamentais, utilizando meios eletrônicos como a Internet. Cita os artigos do Código Penal (art. 147, relativo a ameaças; art. 138, relativo a calúnias; art. 139, relativo à difamação; art. 140, relativo à injúria, art. 307, relativo à falsa identidade) apresenta e ensina os procedimentos para que a vítima possa apelar para a justiça, ensinando-a imprimir e salvar o conteúdo das páginas ou o diálogo dos suspeitos em salas de bate-papo, bem como as mensagens de correio eletrônico “e-mails” ofensivos, juntamente com os cabeçalhos das mensagens e preservar as provas em algum tipo de mídia protegida contra alteração, como CD-R ou DVD-R.

2.3 TIPIFICAÇÃO DOS CRIMES NO BRASIL

O direito, como ciência social, deve estar sempre acompanhando a evolução da sociedade e, consequentemente, seus costumes, adequando-se aos fatos atuais em questão. Diante dessa tipificação alguns crimes podem ficar impunes, já que a nossa Constituição prega em seu artigo 5º, inciso XXXIX, “*não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal*”. Portanto, se não houver uma lei específica punindo os praticantes de crimes praticados pela Internet, pode haver punição? Nestes tipos de caso, os tribunais brasileiros utilizam-se da analogia para o ajustamento da conduta atípica à nossa norma penal vigente. A Constituição Federal prega, em seu artigo 5º, inciso II, o Principio da Legalidade que diz que “*ninguém será obrigado a fazer ou deixar de fazer alguma coisa senão em virtude da lei*”. Assim, é proibido o emprego da analogia em matéria penal, ou seja, os nossos magistrados acabam encontrando dificuldades para incriminar esse tipo de conduta (INELLAS, 2009).

Segundo o pensamento do escritor Miguel Reale, a analogia atende ao principio que o direito é um sistema de fins:

> Pelo processo analógico, 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 ratio, ibi eadem juris dispositio* (onde há a mesma razão deve haverá mesma disposição de direito). (REALLE, 2002, p. 296).

Se olharmos por outro prisma, podemos perceber que esses tipos de crimes já são existentes em nosso ordenamento jurídico, mas a questão é a forma como esses crimes são praticados, diferentes dos convencionais, com o auxilio da Internet, mas que almejam o mesmo resultado (INELLAS, 2009, p. 113).

A questão que surge é como punir os praticantes desses crimes, se não sabemos o caminho para conseguir localizá-los? Essa é a dificuldade encontrada pela polícia para tentar localizar esses criminosos que se utilizam de seus conhecimentos de informática para realizar diversos atos ilícitos, como crimes contra o sistema financeiro, contra a ordem tributária, estelionato, e outros que estão sendo comuns no país (INELLAS, 2009, p. 117).

Segundo Inellas, a verdade é que a polícia não está preparada, tampouco os magistrados, para lidar com esse tipo de crime. Mais precisamente a forma como são tratados essas infrações pela ausência de lei específica sobre o caso. Desse modo, tem-se um tratamento amador, tendo muito a evoluir nesse sentido. A criação de uma norma penal específica para sancionar os crimes praticados através da Internet, seria o primeiro passo a ser dado para sanar o problema que afronta a sociedade mundial.

Alguns países já começaram a introduzir no código penal questões referentes aos crimes praticados através da rede. Segundo Castro, o Código Penal Português de 1995, Decreto-Lei nº 48/95, descreve dois crimes relacionados à informática, que seria os crimes contra a reserva da vida privada por meio de inquirição através da informática, o outro tipo penal dispõe sobre a burla informática nas comunicações. Burla informática nas comunicações, de acordo com o entendimento do Superior Tribunal Federal Brasileiro, no acórdão nº 78/07.6JAFAR.E2.S1, "é a manipulação de um sistema informático, com o objetivo de uma interferência no resultado ou na estruturação incorreta de um programa, utilização incorreta ou incompleta de dados, utilização de dados sem autorização ou qualquer intervenção não autorizada de processamento". Em ambos os casos o legislador prevê tipos penais e punições cabíveis. As penalidades para os crimes na internet estão tendo um avanço perceptível em Portugal, ainda que ausente a regulamentação dos crimes relativos à proteção da honra individual no âmbito da internet. Já, na Itália, a legislação vigente sobre a informática dá maior ênfase às questões referentes aos direitos autorais, principalmente aos relacionados com os termos de programas de computadores, sendo que a legislação foca em seis figuras essenciais: sabotagem, acesso ilegal, violação de segredo informático e do sigilo, falsificações, fraude informática e violação dos direitos do autor, em especial ao software (CASTRO, 2003, p. 207).

Assim, no texto escrito por Castro, a Lei Francesa de nº 78/16, de 06 de janeiro de 1978, dá ênfase às caricaturas ou montagens que impliquem em condutas ofensivas e devem ser justificadas e vir a ser objeto de análise, de modo a verificar se não afronta tal princípio. Ao analisar outras áreas importantes, como o respeito às relações sentimentais, o autor apresenta casos em que as decisões foram tomadas a partir de jurisprudência, levando como base os princípios fundamentais consagrados na legislação francesa. Nesse sentido, pode-se notar que as parcerias entre o setor público e o privado, no que concerne à regulação da internet, a adulteração da personalidade, por intermédio de fabricação de falsos perfis em sites hospedados na internet, bem como fotomontagens ofensivas onde configurem difamação ou outros crimes contra a personalidade, devem sofrer sanção penal, garantindo o princípio do respeito à personalidade (CASTRO, 2003, p. 215).

Segundo Robert apud Canen (2009), menciona o principio da Liberdade de Expressão, da proteção à vida privada e do segredo das mensagens enviadas por meio de endereços eletrônicos, ele mostra o que existe na comissão nacional francesa de controle de interceptações de segurança. Uma autoridade administrativa independente, da Corte Européia dos Direitos dos Homens ao analisar as leis, como a alemã, afirma que a participação do Estado é justificada, no mundo da internet, como uma ideia de salvaguarda e democracia. Tendo como ideia principal a de se trazer para a internet uma legislação especifica, objetivando trazer uma regulação que faça com que os princípios constitucionais, devidamente ponderados, sejam observados, de forma consensual respeitando, assim, a personalidade e as regras que regem a sociedade.

No contexto brasileiro, se espera a elaboração de lei que trate sobre a informática e a internet nos campos do Direito Penal, Direito Civil, Direito Comercial, Direito Tributário e outros. Enquanto essa legislação específica não chega, impõe-se a aplicação da legislação existente referente à matéria discutida, ou seja, Constituição Federal, Código Penal, Código Civil entre outras legislações.

No Brasil já existe uma lei específica para a proteção do software, a Lei nº 9.609/98. Pereira (2011), em sua obra, explana que essa lei se preocupa com o respeito à propriedade intelectual dos programas de computador, que recebeu o nome de Lei do Software, que afirma que o regime de propriedade do software é concedido pelas normas de direitos autorais e conexos em vigor.

Referente as legislação já existentes no Brasil, Castro (2003), nos traz a legislação já existente em nosso ordenamento jurídico, uma lei específica, a Lei do Software (Lei n.º 9.609/98), que dispõe sobre a proteção da propriedade intelectual de programas de

computador, sua comercialização no País, e dá outras providências, e nada menciona sobre a matéria a respeito da internet. Diferente das leis americanas, a lei brasileira é omissa quanto à regulamentação da internet em nosso país.

2.4 OS PROJETOS DE LEI EM TRÂMITE NO CONGRESSO NACIONAL E SUAS RESTRIÇÕES

Os direitos e deveres de um cidadão perante a sociedade são instituídos por lei, com a finalidade de manter a ordem e o equilíbrio das relações humanas. Segundo França (1997), a palavra lei é usada como princípio que determina não só o modo como os seres humanos agem como, também, os acontecimentos naturais. O conceito de lei origina-se da palavra ordem, ou seja, a disposição do homem viver em sociedade. A Lei é o direito elaborado por uma pessoa conhecedora do assunto, mediante um ato de vontade, o qual se denomina legislação, ou seja, o ato de elaborar leis. Por vezes, o legislador, no ato da elaboração da lei, leva em consideração suas paixões e preconceitos. Algumas vezes passam através deles e por eles são denegridas outras, ficam entre eles e a eles se incorporam (MONTESQUIEU, 1973, p.479).

Em sua obra "Cartas Persas", Montesquieu adverte que as leis sejam redigidas de forma simples, compreensível por todos, em especial para aqueles as qual será aplicada, diferenciando-se dos demais textos da literatura, de maneira difusa, onde o significado está na essência da redação:

> [...] O estilo das leis deve ser simples; a expressão direta é sempre melhor compreendida do que a expressão meditada. Não há majestade nas leis do baixo império; nelas os princípios falam como vetores. Quando o estilo das leis é empolado, olhamo-las apenas como obra de ostentação. É essencial que as palavras das leis despertem em todos os homens as mesmas ideias (...). As leis não devem ser sutis; elas são feitas para pessoas de entendimento medíocre: não são uma obra de lógica, mas a razão simples de um pai de família (MONTESQUIEU, 1973,p.475-476).

Cabe ao Poder Legislativo a função de elaborar as leis e sua fiscalização. No Brasil, adota-se a divisão dos poderes: o Legislativo, o Judiciário e o Executivo. Segundo Mendes (2008), na divisão dos poderes, o poder Legislativo de modo atípico tem a função de julgar e administrar. Isso acontece quando promove cargos de estrutura ou atua no poder de polícia, por exemplo.

O Poder Legislativo Brasileiro opera no Congresso Nacional de forma bicameral, ou seja, duas Câmaras: dos Deputados e a do Senado. A Câmara dos Deputados é representada por deputados eleitos pelo povo de forma direta num sistema proporcional em cada Estado membro da União e do Distrito Federal, cujo mandato é de quatro anos. O Senado Federal é composto por três representantes de cada Estado membro da União e do Distrito Federal, e são eleitos pelo sistema majoritário, ou seja, o candidato com a maioria dos votos no distrito eleitoral é o único a ser eleito, com mandato de oito anos. (MENDES, 2008, p.853).

O Brasil adota o sistema bicameral por força da adoção do sistema federalista, e não como ocorre nos demais países, onde o sistema bicameral existente não advêm do sistema federalista, mas sim de outras circunstâncias, como é o caso da divisão histórica da Câmara de Londres e da Câmara dos Comuns, na Inglaterra. Vale ressaltar que os Senadores, no Brasil, em tese não são representantes do povo, mas sim dos Estados da Federação Brasileira, participando, por esse motivo, na formação da vontade nacional. Essa participação no processo legislativo por parte dos entes federados é uma exigência da teoria federalista (TAVARES, 2008, p. 1100).

O Poder Legislativo como o próprio nome diz, tem como função legislar, editar leis, atos normativos primários, que instituem direitos e criam obrigações, função essa típica do poder Legislativo. Em seu artigo 59, a Constituição Federal do Brasil lista os instrumentos normativos compreendidos:

> Art. 59. O processo legislativo compreende a elaboração de:
> I - emendas à Constituição;
> II - leis complementares;
> III - leis ordinárias;
> IV - leis delegadas;
> V - medidas provisórias;
> VI - decretos legislativos;
> VII - resoluções.
> Parágrafo único. Lei complementar disporá sobre a elaboração, redação, alteração e consolidação das leis (BRASIL, 1988).

O processo legislativo, para Sampaio (1996), é definido como uma espécie do gênero amplo do direito processual, que também é chamado adjetivo ou formal, para distinguir do direito substantivo ou material. É o direito processual que revela o caráter dinâmico do ordenamento jurídico. Através dele, o direito regula a sua própria criação, estabelecendo as normas que presidem à produção de outras normas, sejam normas gerais ou individualizadas. Quando se trata de normas que regulam a produção, criação, modificação ou revogação de normas gerais, aí se encontra o processo legislativo.

Silva (2005), define o processo legislativo como um conjunto de atos (iniciativa, emenda, votação, sanção e veto), visando à formação das leis constitucionais, complementares e ordinárias, resoluções e decretos legislativos.

Ainda em relação aos pensamentos de Silva (2005), a maneira pela qual os atos do processo legislativo se realizam são denominados procedimentos. Diz respeito ao andamento da matéria nas Casas Legislativas. Essas regras também aplicam-se para os Estados e Municípios na formação de leis orgânicas internas.

O processo legislativo, no âmbito sociológico, refere-se ao conjunto de fatores legítimos ou fáticos que fornecem movimento aos legisladores e, principalmente, ao modo como eles procedem, rotineiramente, ao realizar as tarefas legislativas. Indo além, caberia ressaltar que trata-se de uma sociologia do processo legislativo que se preocupa em identificar e analisar as diversas ocorrências presentes no decorrer da concepção das leis, como a pressão popular, a mídia, os grupos de pressão, os ajustes políticos partidários, as trocas de favores do Governo com os parlamentares e tantos outros fatores que estão ligados à elaboração de uma lei (TAVARES, 2008, p. 1134).

A Constituição Federal Brasileira, na Sessão VIII, do Capítulo I, do Título IV, designa as normas destinadas a regular o processo para a formação das leis. Trata-se da sequência definida de atos e etapas que exercem no intuito de estabelecer novas normas jurídicas (TAVARES, 2008, p. 1134).

Para que um projeto de lei passa a vigorar, é necessário que o processo passe por uma série de etapas, quais sejam: a iniciativa que divide-se em comum, reservada, privada de órgãos do Judiciário, privada do Ministério Público, privada da Câmara dos Deputados, do Senado e do Tribunal de Contas da União e privada do Presidente da República. Após a iniciativa, para ser aprovado, passa pelas etapas de Discussão, Votação, Sanção ou Veto e, por fim, para tornar-se uma lei deve haver a Promulgação e Publicação (MENDES, 2008, p. 873). Nas seções a seguir serão explanadas as etapas do procedimento citado:

a. Iniciativa

O processo de criação de um novo direito, perante o poder legislativo, tem início por iniciativa de cidadãos ou entidades. Na obra de Mendes (2008), destacam-se seis tipos de iniciativas para dar-se início a um projeto de lei:

- Iniciativa Comum: pode ser apresentado por qualquer membro do Congresso Nacional, por comissão de suas Casas, pelo Presidente da República ou pelos cidadãos, que é o caso da iniciativa popular;

- Iniciativa Reservada: a Constituição reserva a possibilidade a apenas algumas autoridades ou órgãos para que se possa ter um debate em torno do assunto;
- Iniciativa Privada de Órgãos do Judiciário: tem sua iniciativa pelo Supremo Tribunal Federal;
- Iniciativa Privada do Ministério Público: tem legitimidade para propor ao Poder Legislativo a criação e extinção de seus cargos e serviços auxiliares, e a política remuneratória e os planos de carreira;
- Iniciativa Privada da Câmara dos Deputados, do Senado e do Tribunal de Contas da União: no âmbito das Câmaras seja dos Deputados ou do Senado, sugerem-se leis no que tange à remuneração dos servidores incluídos na sua organização. Perante o Tribunal de Contas da União cabe a este apresentar o projeto de lei visando dispor sobre a organização administrativa, criação de cargos e remuneração de servidores e a fixação de subsídios dos membros da Corte;
- Iniciativa Privada do Presidente da República: por iniciativa do presidente da República no que tange às esferas das Forças Armadas, servidores públicos, civis e militares.

b. Análise

Segundo Lenza, o projeto em primeiro lugar é analisado por uma comissão temática, que avaliará o projeto proposto e, em seguida, será analisado pela Comissão de Constituição e Justiça, que ponderará, entre outros aspectos, a constitucionalidade, podendo aprovar os projetos, desde que estes estejam de acordo com as normas da Casa. O parecer das Comissões Temáticas é opinativo, já que a matéria será discutida e passará por um processo de votação (LENZA, 2011, p-515).

c. Votação

A votação poderá ocorrer via sistema automatizado ou via cédulas sendo suas formas: simbólica, nominal ou escrutínio secreto. O processo simbólico será aplicado na votação das proposições pelos Parlamentares sendo que, caso haja consenso por parte dos deputados, estes permanecem sentados, caso haja discordância, se levantam (LENZA, 2011, p. 516).

Caso seja requerida a verificação da votação, será ela repetida pelo processo nominal, conforme o art. 186 do Regimento Interno da Câmara dos Deputados:

> Art. 186. O processo nominal será utilizado:
> I - nos casos em que seja exigido quórum especial de votação;
> II - por deliberação do Plenário, a requerimento de qualquer Deputado;
> III - quando houver pedido de verificação de votação, respeitado o que prescreve o§ 4º do artigo anterior (Fonte: http://www.camara.gov.br acesso em: 07/07/2013);

Ainda, sobre Regimento Interno da Câmara dos Deputados, o seu art. 188, estabelece que a votação por escrutínio secreto far-se-á pelo sistema eletrônico, nos seguintes casos:

> Art. 188. A votação por escrutínio secreto far-se-á pelo sistema eletrônico, nos termos do artigo precedente, apurando-se apenas os nomes dos votantes e o resultado final, nos seguintes casos:
> I - deliberação, durante o estado de sítio, sobre a suspensão de imunidades de Deputado, nas condições previstas no § 8o 67 do art. 53da Constituição Federal;
> II - por decisão do Plenário, a requerimento de um décimo dos membros da Casa ou de Líderes que representem esse número, formulado antes de iniciada a Ordem do Dia.
> § 1o A votação por escrutínio secreto far-se-á mediante cédula, impressa ou datilografada, recolhida em urna à vista do Plenário:
> I - quando o sistema eletrônico de votação não estiver funcionando;
> II - no caso de pronunciamento sobre a perda do mandato de Deputado ou de suspensão das imunidades constitucionais dos membros da Casa durante o estado de sítio;
> III - para eleição do Presidente e demais membros da Mesa do Presidente e Vice-Presidentes de Comissão Permanente, dos membros da Câmara que irão compor a Comissão Representativa do Congresso Nacional, dos dois cidadãos que irão integrar o Conselho da República, e nas demais eleições.
> § 2o Não serão objetos de deliberação por meio de escrutínio secreto:
> I - recursos sobre questão de ordem;
> II - projeto de lei periódica;
> III - proposição que vise à alteração de legislação codificada ou disponha sobre leis tributárias em geral, concessão de favores, privilégios ou isenções e qualquer das matérias compreendidas nos incisos I, II, IV, VI, VII, XI, XII e XVII do art. 21 e incisos IV, VII, X, XII e XV do art. 22 da Constituição Federal;
> IV - autorização para instauração de processo, nas infrações penais comuns ou nos crimes de responsabilidade, contra o Presidente e o Vice-Presidente da República e os Ministros de Estado (Fonte: http://www.camara.gov.br acesso em: 07/07/2013).

A votação secreta realizar-se-á pelo sistema eletrônico, exceto nas eleições que implantará o sistema de cédula (LENZA, 2011, p. 517).

De acordo com os entendimentos de Lenza, caso o projeto de lei sofra rejeição na Casa Iniciadora, este será arquivado. No entanto, caso o mesmo seja aprovado, ele seguirá para a Casa Revisora, passando também pelas Comissões e, ao final, a Casa Revisora poderá aprová-lo, rejeitá-lo ou emendá-lo. Ainda, segundo o autor, quando o Projeto de Lei é aprovado, em um só turno de discussão e votação, este será enviado para a sanção ou veto do Chefe do Executivo. Já no momento em que o Projeto de Lei for rejeitado pela Casa Revisora, este será arquivado, e só será apresentado na mesma sessão legislativa mediante proposta da maioria absoluta dos membros de qualquer uma das Casas do Congresso Nacional. Por fim, tem-se a emenda do projeto, na hipótese do projeto inicial sofrer algum tipo de emenda, e somente o que foi modificado deverá ser apreciado pela Casa Iniciadora, sendo vedada a apresentação de emendas no que quer dizer a subemenda (LENZA, 2011, p. 517).

Caso a Casa Iniciadora aceite o projeto introduzido pela Casa Revisora, este seguirá para a deliberação executiva. Caso contrário, houver rejeição do projeto proposto pela casa

iniciadora, em sua redação original, este seguirá para a apreciação executiva (LENZA, 2011, p. 518).

No processo legislativo de elaboração das leis, no sistema brasileiro, haverá predominância da Casa Iniciadora sobre a Casa Revisora. Assim, como salienta Carvalho (1996), "*o poder de veto equilibra na sistemática presidencial a falta de prerrogativa do Presidente para dissolver a Câmara, existente no sistema parlamentarista*".

d. Sanção

A sanção é de responsabilidade exclusiva do Presidente da República. O projeto de lei só vai para a análise do presidente depois de ser devidamente aprovado pelo Congresso Nacional. A sanção pode ser expressa, nos casos em que o Presidente se manifesta a favor, no prazo de 15 dias úteis, ou tácita, quando permanece sem se manifestar no mesmo prazo (MORAES, 2011, p. 684).

e. Veto

O veto, assim como a sanção, é de responsabilidade exclusiva do Presidente da República. É a manifestação em discordância do Presidente com o projeto de lei aprovado pelo Poder Legislativo, no prazo de 15 dias. O prazo inicia sua contagem com o recebimento do projeto de lei por parte do chefe do Poder Executivo. O dia inicial não é contado, porém, o dia final integra a contagem (MORAES, 2011, p. 684).

De acordo com os ensinamentos do autor, o Presidente da República poderá discordar do projeto de lei, ou poderá entender que o projeto de lei é inconstitucional (aspecto formal) ou contrário ao interesse público (aspecto material). Ou seja, em primeiro caso, teremos o chamado veto jurídico e, em segundo caso, teremos o veto político (MORAES, 2011, p. 685).

f. Promulgação e publicação

Para Mendes (2008), a promulgação de uma lei passa a existir com sanção do chefe do poder executivo no caso o Presidente de República. Cabe ao Presidente da República o encargo de promulgar a lei mas, se houver sanção tácita ou rejeição de veto, caso ele não o fizer em quarenta e oito horas, cabe ao Presidente do Senado a incumbência. O ato da publicação de uma nova lei é um ato relevante para fixar o momento da vigência da lei.

2.4.1 O PROJETO DE LEI Nº 84/99

Segundo Reinaldo Filho (2004), o Projeto de Lei nº 84/99, trata de uma maneira mais ampla e organizada dos crimes cometidos através dos meios eletrônicos. Esse projeto tem o

propósito de criar novos tipos penais, estendendo ao campo de incidência de algumas figuras já existente no Código Penal, impossíveis de terem sido previstos pelo legislador de 1940, ano em que se editou o atual Código Penal. Determinadas condutas surgidas nesses ambientes são inteiramente novas e não guardam relação ou similitude com tipos já descritos no atual Código Penal Vigente, havendo uma necessidade de sua reformulação na "Era Digital". Por isso, o projeto de lei cria novos tipos penais, não se limitando a reformular conceitos legais já existentes.

A seguir o Projeto de Lei de nº 84/99, de autoria do Deputado Luiz Piauhylino, dispõe sobre os crimes cometidos na área de informática:

> **DOS CRIMES DE INFORMÁTICA**
> **Seção I**
> **Dano a dado ou programa de computador**
> Art. 8º - Apagar, destruir, modificar ou de qualquer forma inutilizar, total ou parcialmente, dado ou programa de computador, de forma indevida ou não autorizada.
> Pena: detenção, de um a três anos e multa.
> Parágrafo único. Se o crime é cometido:
> I - contra o interesse da União, Estado, Distrito Federal, Município, órgão ou entidade da administração direta ou indireta ou de empresa concessionária de serviços públicos;
> II - com considerável prejuízo para a vítima;
> III - com intuito de lucro ou vantagem de qualquer espécie, própria ou de terceiro;
> IV - com abuso de confiança;
> V - por motivo fútil;
> VI - com o uso indevido de senha ou processo de identificação de terceiro; ou
> VII - com a utilização de qualquer outro meio fraudulento.
> Pena: detenção, de dois a quatro anos e multa
> **Seção II**
> Acesso indevido ou não autorizado
> Art. 9º - Obter acesso, indevido ou não autorizado, a computador ou rede de computadores.
> Pena: detenção, de seis meses a um ano e multa.
> § 1º - Na mesma pena incorre quem, sem autorização ou indevidamente, obtém, mantém ou fornece a terceiro qualquer meio de identificação ou acesso a computador ou rede de computadores.
> § 2º - Se o crime é cometido:
> I - com acesso a computador ou rede de computadores da União, Estado, Distrito Federal, Município, órgão ou entidade da administração direta ou indireta ou de empresa concessionária de serviços públicos;
> II - com considerável prejuízo para a vítima;
> III - com intuito de lucro ou vantagem de qualquer espécie, própria ou de terceiro;
> IV - com abuso de confiança;
> V - por motivo fútil;
> VI - com o uso indevido de senha ou processo de identificação de terceiro; ou
> VII - com a utilização de qualquer outro meio fraudulento.
> Pena: detenção, de um a dois anos e multa.
> Seção III
> Alteração de senha ou mecanismo de acesso a programa de computador ou dados
> Art. 10 - Apagar, destruir, alterar, ou de qualquer forma inutilizar, senha ou qualquer outro mecanismo de acesso a computador, programa de computador ou dados, de forma indevida ou não autorizada.
> Pena: detenção, de um a dois anos e multa.
> Seção IV

> Obtenção indevida ou não autorizada de dado ou instrução de computador
> Art. 11. Obter, manter ou fornecer, sem autorização ou indevidamente, dado ou instrução de computador.
> Pena: detenção, de três meses a um ano e multa.
> (www.mpba.mp.br Acesso em 06/8/2013)

Conforme o site da Câmara, segue o tramite do Projeto de Lei nº 84/1999 apresentado pelo deputado Luiz Piauhylino na Câmara dos Deputados, mostrando apenas as três primeiras movimentações do projeto e as três últimas:

> Autor: Luiz Piauhylino - PSDB/PE
> Apresentação: 24/02/1999
> **Ementa:** Dispõe sobre os crimes cometidos na área de informática, suas penalidades e dá outras providências.
> **NOVA EMENTA**: Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal e a Lei nº 9.296, de 24 de julho de 1996, e dá outras providências.
> **Explicação da Ementa:** Caracteriza como crime informático ou virtual os ataques praticados por "hackers" e "crackers", em especial as alterações de "home pages" e a utilização indevida de senhas.
> **24/02/1999 PLENÁRIO (PLEN)**•APRESENTAÇÃO DO PROJETO PELO DEP LUIZ PIAUHYLINO.
> **24/02/1999 Mesa Diretora da Câmara dos Deputados (MESA)**•DESPACHO INICIAL A CCTCI E CCJR (ARTIGO 54 DO RI).
> **11/05/1999PLENÁRIO (PLEN)**•LEITURA E PUBLICAÇÃO DA MATERIA. DCD 11 05 99 PAG 19975 COL 01.
>
> **[...]**
>
> **09/11/2012 Mesa Diretora da Câmara dos Deputados (MESA)**•Remessa à sanção por meio da Mensagem nº 40/12.•Ofício nº 705/12/PS-GSE comunicando envio à sanção.
> **30/11/2012 Mesa Diretora da Câmara dos Deputados (MESA)**•Transformado na Lei Ordinária 12735/2012. DOU 03/12/12 PÁG 01 COL 01. Vetado parcialmente. Razões do veto: MSC 525/12-PE. DOU 03/12/12 PÁG 09 COL 03.
> **07/12/2012 Mesa Diretora da Câmara dos Deputados (MESA)**•Recebimento do Ofício nº 528/12(CN) comunicando veto parcial e solicitando indicação de membros para integrar a Comissão Mista incumbida de relatar o(s) veto(s). (Fonte: http://www.camara.gov.br acesso em 09/08/2013)

O Projeto de Lei tem como explicação de ementa "*Caracterizar como crime informático ou virtual os ataques praticados por "hackers" e "crackers", em especial as alterações de "home pages" e a utilização indevida de senhas*". Esse projeto foi apresentado na Câmara dos Deputados no dia 24/02/1999. Desta data em diante, o projeto foi estudado pelos membros da Câmara, passou por votação e algumas reformulações, emendas e pareceres da Comissão de Ciência e Tecnologia, Comunicação e Informática (CCTCI), Comissão de Segurança Pública e Combate ao Crime Organizado (CSPCCO) e Comissão de Constituição e Justiça e de Cidadania (CCJC) (Fonte: http://www.camara.gov.br acesso em 06/08/2013).

No dia 30/11/2012 a mesa da Câmara dos Deputados transformou em Lei Ordinária de nº 12735/2012 e vetando parcialmente o Projeto de Lei apresentado pelo Deputado do estado

de Pernambuco. Sua última movimentação foi no dia 07 de dezembro de 2012, onde a mesa da Câmara dos deputados está estudando o veto parcial do Projeto de Lei nº84/99 e solicitando indicação de membros para compor a Comissão Mista encarregada de relatar o(s) veto(s) (Fonte: http://www.camara.gov.br acesso em 06/08/2013).

O projeto de lei de nº 84/99 que foi transformado em Lei Ordinária sob nº 12735/2012, até o presente momento encontra-se estacionado. Ele está à espera de um relator que irá apresentar o veto do restante projeto de lei nº 84/99 que não foi utilizado.

2.4.2 O PROJETO DE LEI Nº 1713/95

Segundo Gouvêa (1997), o projeto de lei nº 1713/95, discorre sobre o acesso, a responsabilidade e os crimes cometidos nas redes de computadores. Ela menciona que são 35 artigos do projeto tratando da tipificação dos crimes. Em seguida segue alguns comentários sobre os tipos penais propostos.

No capítulo V, do Projeto de Lei, estão tipificados os crimes e suas sanções, tendo como título do capítulo, a seguinte expressão: "*Dos crimes de informática cometidos em decorrência da utilização de computador ou equipamento de informática em redes integradas*", e retrata no artigo 18 até ao artigo 29 as seguintes propostas:

> Art. 18 – obter acesso, indevidamente, a um sistema de computador ou uma rede integrada de computadores:
> Pena – detenção, de 3 (três) meses a 6 (seis) meses, ou multa.
> § 1º - Se o acesso se faz por uso indevido de senha ou de processo de identificação magnética de terceiro:
> Pena – detenção, de 1 (um) a 2 (dois) anos, e multa.
> § 2º - Se, além disso, resultar prejuízo econômico para o titular:
> Pena – detenção, de 1 (um) a três, e multa.
> § 3º - Se o acesso tem por escopo causar dano a outrem ou obter vantagem indevida.
> Pena – detenção, de 2 (dois) a 4 (quatro) anos, e multa.
> § 4º - Se o sistema ou a rede integrada de computadores pertence a pessoa jurídica de direito público interno, autarquias, empresas públicas, sociedades de economia mista, fundações instituídas ou mantidas pelo Poder Público e serviços sociais autônomos, a pena é agravada em um terço.
> Art.19 – Apropriar-se indevidamente de informações, de que tem posse ou a detenção em rede integrada de computadores:
> Pena – reclusão, de 1 (um) a três anos, e multa.
> Art. 20 – Obter segredos empresariais ou informações de caráter confidencial em rede integrada de computadores, com o intuito de causar danos financeiros ou obter vantagem econômica para si ou para outrem:
> Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa.
> Art. 21 – Apropriar-se indevidamente de valores, de que tem posse ou a detenção através da manipulação de qualquer sistema de processamento de dados, obtendo assim vantagem econômica para si ou para outrem:
> Pena – reclusão, de 1 (um) a 5 (cinco) anos, e multa.
> Art. 22 – Obstruir o funcionamento de rede integrada de computadores ou provocar-lhe distúrbios:
> Pena – detenção, de 1 (um) a 2 (dois) anos, e multa.

> Art. 23 – Obter acesso a sistema ou a rede integrada de computadores, com o intuito de disseminar informações fraudulentas:
> Pena – reclusão, de 1 (um) a 5 (cinco) anos, e multa.
> Art. 24 – Falsificar, alterar ou apagar documentos através de sistema ou rede integrada de computadores e seus periféricos:
> Pena – reclusão, de 1 (um) a 5 (cinco) anos, e multa.
> § 1º. Nas mesmas penas incorre quem sabendo ser falso, utiliza-se de documentos obtidos através de sistema ou de rede integrada de computadores;
> § 2º. Considera-se documento o dado constante no sistema de computador e suporte físico como disquete, disco compacto, CD-ROM ou qualquer outro aparelho usado para o armazenamento de informação, por meio mecânico, ótico ou eletrônico.
> Art. 25 – interceptar indevidamente a comunicação entre computadores durante a transmissão de dados:
> Pena – detenção, de 6 (seis) meses a 1 (um) ano, e multa.
> Parágrafo único. A pena é agravada em um terço se a interceptação invade a privacidade do usuário.
> Art. 26 – Obter, de forma não autorizada, informações confidenciais ou pessoais do indivíduo em sistema ou rede integrada de computadores:
> Pena – detenção, de 6 (seis) meses a 1 (um) ano, e multa.
> Art. 27 – Deixar de informar ou de retificar dados pessoais contidos em rede integrada de computadores, quando requeridos pelo interessado:
> Pena – detenção de 3 (três) a 9 (nove) meses, e multa.
> Parágrafo único. Na mesma pena incorre quem:
> I – transfere dados pessoais contidos em um sistema de computador, sem a permissão do interessado, a pessoa não autorizada com finalidade diversa daquela à qual a informação foi obtida:
> II – transfere, sem a permissão do interessado, dados pessoais para fora do país.
> Art. 28 – Obter acesso a sistema de dados ou rede integrada de computadores de instituição financeiras com o objetivo de transferir, para si ou para outrem, dinheiro, fundos, créditos e aplicações de terceiros:
> Pena – reclusão, de 2 (dois) a 6 (seis) anos, e multa.
> Art. 29 – Obter acesso ilícito a sistema de computador ou a rede integrada de computadores, com o intuito de apropriar-se de informação confidenciais ligadas à segurança nacional:
> Pena – reclusão, de 2 (dois) a 6 (seis) anos, e multa.
> Parágrafo único. Se, além do acesso, as informações são copiadas, vendidas ou transferidas para outrem, a pena é agravada em um terço. (Fonte: http://www.camara.gov.br acesso em 27 de maio de 2013).

De acordo com os comentários do deputado Cássio Cunha Lima do PMDB/PB, autor do Projeto de Lei apresentado na Câmara, relata que:

> A proposta apresentada tem a finalidade de contribuir para a correção dessa lacuna da legislação brasileira. Busca, à luz da natureza e do funcionamento das redes de computadores, definir as responsabilidades dos vários agentes (administrador de rede, provedor de serviços e usuários, entre outros) em relação à operação e ao uso da rede e tipificar, além disso, os crimes relacionados com tais atividades, estabelecendo as respectivas penalidades (GOUVÊA, 1997, p. 123).

De acordo com os comentários da Comissão de Ciência e Tecnologia que foram retirados do site da Câmara, Cássio Cunha Lima é abrangente e tecnicamente bem fundamentado, tratando amplamente do acesso à redes de computadores, da segurança dos serviços de rede e do uso de dados disponíveis em bancos de dados, emitir material obsceno pela Internet ou deixá-lo disponível à consulta (Fonte: http://www.camara.gov.br acesso em 05/8/2013).

Conforme o site da Câmara a seguir está exposta às três primeiras movimentações do projeto de Lei 1713/95 e as três últimas:

> **PL 1713/1996**
>
> **Projeto de Lei**
> **Situação:** Apensado ao PL 1070/1995
> Identificação da Proposição
> **Autor -** CASSIO CUNHA LIMA - PMDB/PB
> **Apresentação -** 27/03/1996
> **Ementa -** Dispõe sobre o acesso, a responsabilidade e os crimes cometidos nas redes integradas de computadores e dá outras providências.
> **Explicação da Ementa -** Estabelece que somente por ordem judicial poderá haver cruzamento de informações automatizadas com vistas a obtenção de dados sigilosos.
>
> 27/03/1996 Apresentação do Projeto de Lei pelo Dep. CASSIO CUNHA LIMA
> 19/04/1996 Mesa Diretora da Câmara dos Deputados (MESA)
> A CCTCI E CCJR.(DESPACHO INICIAL)
> 19/04/1996 PLENÁRIO (PLEN)
> PUBLICAÇÃO DA MATERIA.
> DCD 18 04 96 PAG 10032 COL 02.
> 27/05/1996 Comissão de Ciência e Tecnologia, Comunicação e Informática (CCTCI)
> RELATOR DEP LUIZ PIAUHYLINO.
> DCD 28 05 96 PAG 15192 COL 02.
>
> [...]
>
> 13/03/2007 Mesa Diretora da Câmara dos Deputados (MESA)
> Devido a desarquivamento desta proposição em requerimento anterior, foi declarada prejudicada a solicitação de desarquivamento constante do REQ-74/2007. DCD 16 03 07 PÁG 10273 COL 01.
> 29/03/2007 Mesa Diretora da Câmara dos Deputados (MESA)
> Devido a desarquivamento desta proposição em requerimento anterior, foi declarada prejudicada a solicitação de desarquivamento constante do REQ-181/2007. DCD 31 03 07 PAG 13812 COL 01.
> 31/01/2011 Mesa Diretora da Câmara dos Deputados (MESA)
> Arquivado nos termos do Artigo 105 do Regimento Interno da Câmara dos Deputados. Publicação no DCD do dia 01/02/2011 - Suplemento ao nº 14.
> 16/02/2011 Mesa Diretora da Câmara dos Deputados (MESA)
> Desarquivado nos termos do Artigo 105 do RICD, em conformidade com o despacho exarado no REQ-132/2011. (Fonte: http://www.camara.gov.br acesso em 05/8/2013)

O Projeto de Lei tem como explicação de ementa: "*Estabelecer que somente por ordem judicial poderá haver cruzamento de informações automatizadas com vistas a obtenção de dados sigilosos*". Esse projeto foi apresentado na Câmara dos Deputados no dia 10/10/1995. Dessa data em diante o mesmo foi debatido pelos membros da Câmara, passou por votação e algumas adequações de emendas e pareceres da Comissão de Ciência e Tecnologia, Comunicação e Informática (CCTCI), Comissão de Desenvolvimento Econômico, Indústria e Comércio (CDEIC) (www.camara.gov.br acesso em 05/8/2013).

No dia 02/02/1999 o projeto de lei sofreu o seu primeiro arquivamento de acordo com os termos do art.105 do Regime Interno da Câmara dos Deputados (RICD), sendo em seguida desarquivado no dia 09/03/1999 nos termos do artigo 105, parágrafo único, do RICD:

> Art. 105. Finda a legislatura, arquivar-se-ão todas as proposições que no seu decurso tenham sido submetidas à deliberação da Câmara e ainda se encontrem em tramitação, bem como as que abram crédito suplementar, com pareceres ou sem eles, salvo as:
> I – com pareceres favoráveis de todas as comissões;
> II – já aprovadas em turno único, em primeiro ou segundo turno;
> III – que tenham tramitado pelo Senado, ou dele originárias;
> IV – de iniciativa popular;
> V – de iniciativa de outro Poder ou do Procurador-Geral da República.
> Parágrafo único. A proposição poderá ser desarquivada mediante requerimento do Autor, ou Autores, dentro dos primeiros 180 (cento e oitenta) dias da primeira sessão legislativa ordinária da legislatura subsequente, retomando a tramitação desde o estágio em que se encontrava.

Desde sua apresentação, o Projeto de Lei sofreu quatro arquivamentos, todos em face do art. 105 do Regime Interno, bem como quatro desarquivamentos, conforme o artigo 105, parágrafo único, do RICD (Fonte: www.camara.gov.br acesso em 05/8/2013).

O projeto teve sua última movimentação pelos membros da Câmara no dia 16 de dezembro de 2011, desarquivado nos termos do Artigo 105 do RICD, em conformidade com o despacho exarado no REQ-132/2011, sendo que permanece desarquivado e sem nenhuma movimentação até a presente data (Fonte: www.camara.gov.br acesso em 05/8/2013).

Esse projeto, quer penalizar de uma forma ou de outra quem invade o sistema operacional do outrem. O legislador pretende, punir aquele que indevidamente acessa os sistemas de computador ou as redes integradas. O tipo penal protege os sistemas de computador e as redes agregadas.

2.4.3 O PROJETO DE LEI Nº 4.102 DO SENADO FEDERAL (PLS Nº 152/91)

O Projeto de Lei nº 4.102, do Senado Federal (PLS nº 152/91), de autoria do Senador Mauricio Corrêa, define crimes praticados por meio de computador, que dispõe:

> **Art.1º** - Constituem crimes contra a inviolabilidade de dados e sua comunicação:
> I – violar dados por meio de acesso clandestino ou oculto a programa ou sistema de computação.
> Pena: detenção de seis meses a um ano, e multa;
> II – violar o sigilo de dados, acessando informação contida em sistema ou suporte físico de terceiro.
> Pena: detenção de um a seis meses, e multa;
> III – inserir em suporte físico de dados, ou em comunicação de dados, programa destinados a funcionar clandestinamente em sistemas de terceiros, que cause prejuízo ao titular ou ao usuário do sistema, ou conscientemente fazê-lo circular.
> Pena: detenção de um a seis meses, e multa.

§ 1º Na hipótese do inciso II deste artigo:
a) se o acesso se faz com o uso indevido de senha ou de processo de identificação magnética de terceiro.
Pena: detenção de três meses a um ano, e multa;
b) se do acesso resultar vantagem econômica indevida, em detrimento de titular do sistema, pune-se o fato como estelionato qualificado nos termos do art. 2º desta Lei.
§ 2º Na hipótese do inciso III deste artigo:
a) se resultar perda definitiva de informação contida no sistema;
Pena: detenção de seis meses a dois anos, e multa;
b) se, além da perda de informação resultar prejuízo econômico para o titular do sistema;
Pena: detenção de um a três anos e multa.
Art. 2º - A prática de conduta descrita nesta Lei como meio para a realização de qualquer outro crime qualifica-o, agravando a pena de um sexto até a metade.
Art. 3º - A informação ou dado constante de sistema eletrônico que, por qualquer razão, tenha relevância nas relações entre pessoas considera-se "documento", punindo-se sua adulteração material oi ideológica nos termos do Código Penal, com a qualificação prevista no art. 2º desta Lei.
Parágrafo único – Para fins deste artigo considera-se "documento público" a informação ou dado constante de sistema:
a) pertencente ou a serviço de órgão público da administração direta ou indireta, instituição financeira, Bolsa de Valores ou estabelecimento de ensino oficial ou reconhecido;
b) em condições de autorizar pagamento, quitação, movimentação de conta corrente ou qualquer transferência de valores;
c) destinado ao acesso público, pago ou gratuito, a informações comerciais, econômicas ou financeiras.
Art. 4º - O Título VII da Lei nº. 7.646 de 18 de dezembro de 1987, passa a vigorar com a seguinte epígrafe, acrescido de um novo art. 38 e parágrafo, renumerando-se o atual e subsequentes:
TÍTULO VII
Dos Crimes e Penalidades
Art. 38 – Inserir ou suprimir dado ou programa em sistema de computação, com a intenção de:
a) impedir ou dificultar acesso a qualquer dado ou programa;
b) prejudicar o funcionamento do sistema de computação ou comprometer a confiabilidade de qualquer dado ou programa.
Pena: detenção de a dois anos.
§ 1º Quando o crime previsto neste artigo for praticado contra a administração pública direta ou indireta e empresa concessionária de serviços públicos, a pena cominada será aumentada para detenção, de um ano e seis meses a três anos, e multa.
§ 2º Se o crime previsto neste artigo for praticado com a intenção de cometer ou facilitar outros delitos, a pena será aumentada de um terço.
Art. 5º - Esta Lei entra em vigor na data de sua publicação.
Art. 6º - Revogam-se as disposições em contrário. (Fonte: http://www.camara.gov.br acesso em 05/8/2013)

Segue o tramite do Projeto de Lei nº 152/1991, que define os crimes de uso indevido de computadores e dá outras providências, sendo declaradas apenas as três primeiras movimentações do projeto e as três últimas:

PROJETO DE LEI DO SENADO Nº 152, DE 1991
Autor: SENADOR - Maurício Corrêa
Ementa: DEFINE OS CRIMES DE USO INDEVIDO DE COMPUTADOR E DA OUTRAS PROVIDENCIAS.
Data de apresentação: 21/05/1991
Situação atual: Local: 12/02/2007 - Secretaria de Arquivo

> Situação: 08/01/2007 - AGUARDANDO DECISÃO DA CÂMARA DOS DEPUTADOS
> Outros números: Origem no Legislativo: CD PL. 04102 / 1993
> Indexação da matéria: Indexação: DEFINIÇÃO, CRIME, UTILIZAÇÃO, COMPUTADOR. IMPUTAÇÃO, PENA, ACESSO, PROGRAMA, SISTEMA DE COMPUTADOR, INSERÇÃO, ALTERAÇÃO, SUPRESSÃO, DADOS, PROGRAMA.
> 21/05/1991 ATA-PLEN - SUBSECRETARIA DE ATA - PLENÁRIO
> Ação: LEITURA.
> 21/05/1991 MESA - MESA DIRETORA
> Ação: DESPACHO A CCJ (DECISÃO TERMINATIVA), ONDE PODERA RECEBER EMENDAS, PELO PRAZO DE 05 (CINCO) DIAS UTEIS.
> DCN2 22 05 PAG 2433.
> 29/05/1991 CCJ - Comissão de Constituição, Justiça e Cidadania
> Ação: ENCERRAMENTO PRAZO, TENDO SIDO APRESENTADA 01 (UMA) EMENDA DO SEN GERSON CAMATA.
>
> [...]
>
> 01/12/2005 SSEXP - SUBSECRETARIA DE EXPEDIENTE
> Situação: REMETIDA À CÂMARA DOS DEPUTADOS
> Ação: Anexado ao processo cópia do Of. PS-GSE nº 235/05, do Sr. Primeiro-Secretário da Câmara dos Deputados acerca da tramitação da matéria.
> 08/01/2007 SSEXP - SUBSECRETARIA DE EXPEDIENTE
> Situação: AGUARDANDO DECISÃO DA CÂMARA DOS DEPUTADOS
> Ação: AO PLEG, com destino ao Arquivo.
> 12/02/2007 SARQ - Secretaria de Arquivo
> Ação: ARQUIVADO
> (Fonte: http://www.senado.gov.br acesso em 05/08/2013)

O Projeto de Lei tem como explicação de ementa: "*Definir os crimes de uso indevido de computador e da outras providências*". Esse projeto foi apresentado no Senado Federal no dia 21/05/1991. Desde a apresentação do projeto o mesmo passou por votação e algumas adequações de emendas e pareceres da CCJ (Comissão de Constituição, Justiça e Cidadania) e da Mesa Diretora (Fonte: www.senado.gov.br acesso em 13/08/2013).

De acordo com o Senado Federal, o projeto teve sua última movimentação pelos membros do Senado no dia 08 de janeiro de 2007, onde estavam aguardando a decisão da Câmara dos Deputados com destino ao arquivo. Após ter saído a decisão, o Projeto de Lei nº 152/1991 foi arquivado no dia 12/02/2007, situação em que se encontra atualmente (Fonte: www.senado.gov.br acesso em 13/08/2013).

A proposta legislativa quer punir quem insira altera dado ou programa em sistema de computador. Esse projeto visa punir os *crachers*, criadores de vírus.

2.4.4 PROJETO DE LEI DO SENADO Nº 234/96

Projeto nº 234/96, cuja autoria é do Senador Júlio Campos, dispõe sobre o Crime contra a inviolabilidade de comunicação de dados de computador:

> **Art.1º** - É crime contra a inviolabilidade de comunicação de dados de computador:
> I – manipular, sabotar, espionar, acessar de qualquer maneira, sem a autorização competente, o conteúdo de computador.
> Pena: detenção, de um a dois anos, e multa.
> II - utilizar abusivamente se a devida autorização das instalações de processamento de dados.
> Pena: detenção, de um ano a seis meses, ou multa.
> **Art. 2º** - A pena será aumentada de 1/3 (um terço) se o cometimento do crime definido nesta lei:
> I – prejudicar o funcionamento do programa ou confiabilidade de tais dados;
> II – impedir ou dificultar o acesso de pessoas autorizadas ao sistema se computador;
> III – burlar a integridade ou a fidelidade das informações;
> IV – alterar ou destruir o conteúdo de qualquer computador.
> **Art. 3º**- Se o crime definido nesta Lei for cometido contra a administração pública, direta ou indireta, ou empresa concessionária de serviços públicos, a pena cominada será aumentada de 2/3 (dois terço).
> **Art. 4º** - Se o agente ao violar os dados, ou em seguida a esta pratica outro crime contra o titular do sistema, aplicam-se cumulativamente a pena de violação e a cominada ao outro crime.
> **Art. 5º** - Esta lei entra em vigor na data de sua publicação.
> **Art. 6º** - Revogam-se as disposições em contrário. (Fonte: http://www.senado.gov.br acesso em: 05/08/2013)

A seguir será apresentadas as três primeiras tramitações do Projeto de Lei de nº 234/1996 na Câmara, e as três últimas:

> PROJETO DE LEI DO SENADO Nº 234, DE 1996
> **Autor:** SENADOR - Júlio Campos
> **Ementa:** DEFINE CRIME CONTRA A INVIOLABILIDADE DE COMUNICAÇÃO DE DADOS DE COMPUTADOR.
> **Data de apresentação:** 22/10/1996
> **Situação atual:** Local: 29/01/1999 - SECRETARIA GERAL DA MESA
> **Situação:** 29/01/1999 - ARQUIVADA AO FINAL DA LEGISLATURA
> **Indexação da matéria:** Indexação: FIXAÇÃO, CRITERIOS, DEFINIÇÃO, CRIME, INVIOLABILIDADE,
> COMUNICAÇÃO DE DADOS, COMPUTADOR. IMPUTAÇÃO, PENA, DETENÇÃO, MULTA, HIPOTESE, CRIME, INVIOLABILIDADE, COMUNICAÇÃO DE DADOS, COMPUTADOR. FIXAÇÃO, REQUISITOS, AUMENTO, PERCENTAGEM, PENA, CRIME, HIPOTESE, PREJUDICIALIDADE, FUNCIONAMENTO, PROGRAMA, CONFIANÇA, DADOS, IMPEDIMENTO, ACESSO, AUTORIZAÇÃO, SISTEMA, COMPUTADOR, FRAUDE, INFORMAÇÃO, ALTERAÇÃO, DESTRUIÇÃO, CONTEUDO. HIPOTESE, CRIME CONTRA A ADMINISTRAÇÃO PUBLICA, ADMINISTRAÇÃO PUBLICA DIRETA, ADMINISTRAÇÃO PUBLICA INDIRETA, EMPRESA, CONCESSIONARIA, SERVIÇO PUBLICO, AUMENTO, PERCENTAGEM, PENA, AGENTE, VIOLAÇÃO, DADOS, TITULAR, SISTEMA, CUMULATIVIDADE.
> 22/10/1996 ATA-PLEN - SUBSECRETARIA DE ATA - PLENÁRIO
> Ação: LEITURA.
> 22/10/1996 MESA - MESA DIRETORA
> Ação: DESPACHO A CCJ (DECISÃO TERMINATIVA), ONDE PODERA RECEBER
> EMENDAS, APOS PUBLICAÇÃO E DISTRIBUIÇÃO EM AVULSOS, PELO PRAZO DE 05 (CINCO) DIAS UTEIS.
> DSF 23 10 PAG 17337.
> 22/10/1996 PLEG - PROTOCOLO LEGISLATIVO
> Ação: ESTE PROCESSO CONTEM 04 (QUATRO) FOLHAS NUMERADAS E RUBRICADAS.

> [...]
>
> 12/11/1998 CCJ - COMISSÃO CONSTITUIÇÃO E JUSTIÇA
> Ação: DEVOLVIDA PELO RELATOR, SEN JOSE IGNACIO FERREIRA, PARA REDISTRIBUIÇÃO.
> 03/12/1998 CCJ - COMISSÃO CONSTITUIÇÃO E JUSTIÇA
> Ação: REDISTRIBUIÇÃO AO SEN FRANCELINO PEREIRA.
> 29/01/1999 SGM - SECRETARIA GERAL DA MESA
> Situação: ARQUIVADA AO FINAL DA LEGISLATURA
> Ação: MATERIA ARQUIVADA NOS TERMOS DO ART. 332 DO RISF.
> DSF Nº 22-A DE 24 02 PAG 3276. (PUBLICADO EM SUPLEMENTO).
> (Fonte: http://www.senado.gov.br acesso em 05/8/2013)

O Projeto de Lei possui como ementa: "*Definir crime contra a inviolabilidade de comunicação de dados de computador*". Esse projeto foi apresentado no Senado Federal no dia 22/10/1996. Desde sua apresentação, este passou por votação e algumas adequações de emendas e pareceres da CCJ e da Mesa Diretora, e foi arquivado em virtude do art. 332, do RISF (Regimento Interno do Senado Federal) da Câmara do Senado Federal, que tem as seguintes disposições:

> "Art. 332 Ao final da legislatura serão arquivadas todas as proposições em tramitação no Senado, exceto:
> I – as originárias da Câmara ou por ela revisadas;
> II – as de autoria de Senadores que permaneçam no exercício de mandato ou que tenham sido reeleitos;
> III – as apresentadas por Senadores no último ano de mandato;
> IV – as com parecer favorável das comissões;
> V – as que tratem de matéria de competência exclusiva do Congresso Nacional (Const. art. 49);
> VI – as que tratem de matéria de competência privativa do Senado Federal (Const. art. 52);
> VII - pedido de sustação de processo contra Senador em andamento no Supremo Tribunal Federal (Const., art. 53, §§ 3º e 4º, EC n.º 35/2001).
> § 1º Em qualquer das hipóteses dos incisos do caput, será automaticamente arquivada a proposição que se encontre em tramitação há duas legislaturas, salvo se requerida a continuidade de sua tramitação por 1/3 (um terço) dos Senadores, até 60 (sessenta) dias após o início da primeira sessão legislativa da legislatura seguinte ao arquivamento, e aprovado o seu desarquivamento pelo Plenário do Senado;
> § 2º Na hipótese do § 1º, se a proposição desarquivada não tiver a sua tramitação concluída, nessa legislatura, será, ao final dela, arquivada definitivamente" (Fonte: http://www.senado.gov.br acesso em 05/08/2013)

Conforme o site do Senado Federal, o projeto teve sua última movimentação pelos seus membros no dia 03 de dezembro de 1998, onde a CCJ redistribuiu a ação ao Senador Francelino Pereira. Após isso o Projeto de Lei nº 234, de 1996 foi arquivado no dia 29/01/1999, sendo mantida sua situação até o presente momento (Fonte: www.senado.gov.br acesso em 13/08/2013).

Atualmente o projeto de lei entra-se arquivado, caso ele não tenha uma tramitação concluída, discutida em plenário, será arquivado definitivamente. Umas das discutições é que

o autor desse projeto deixa vago o que seria computador e auxilio de computador, não sendo admitido termos vagos em nosso Código Penal.

2.4.5 PROJETO DE LEI DA CÂMARA (PLC) Nº 35/2012, LEI CAROLINA DIECKMANN

Segundo o jornal do Senado Federal foi aprovado, no dia 31/10/2012, o Projeto de Lei da Câmara nº 35/2012, de autoria do deputado Paulo Teixeira (PT-SP), que altera o Código Penal, para tipificar como crime uma série de delitos cibernéticos (Fonte: http://www12.senado.gov.br acesso em 06/08/2013).

O Projeto aprovado caracteriza como crime a violação indevida de sistemas de computadores ou dispositivos, sendo estes conectados à rede de computadores, com o intuito de obter, adulterar ou aniquilar dados ou informações sem o consentimento do usuário ou, ainda, para instalar vulnerabilidades. Infrações como a invasão de dispositivos informáticos são tipificados como crimes menos graves, podendo o infrator ser preso por um período de três meses a um ano, além de multa. Já a pena para quem invadir conteúdo de comunicações eletrônicas privadas, informações sigilosas e segredos industriais ou comerciais pode ficar de três meses a dois anos de prisão, além de multa. (Fonte: http://www12.senado.gov.br acesso em: 06/08/2013).

A seguir será apresentada uma breve explanação sobre o Projeto de Lei da Câmara de nº 35/2012, apelidado de Lei Carolina Dieckmann, a Lei dos Crimes Cibernéticos nº (12.737/2012), aprovado na Câmara e sancionado pela Presidenta Dilma Rousseff:

> **Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências.**
> O CONGRESSO NACIONAL decreta:
> Art. 1º Esta Lei dispõe sobre a tipificação criminal de delitos informáticos e dá outras providências.
> Art. 2º O Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal, fica acrescido dos seguintes arts. 154-A e 154-B:
> "**Invasão de dispositivo informático**
> Art. 154-A. Devassar 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, instalar vulnerabilidades ou 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 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 e 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.
§ 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, se o fato não constitui crime mais grave.
§ 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 120 (cento e vinte) dias após a data de sua publicação oficial. (Fonte: http://www.senado.gov.br acesso em 06/8/2013)

A seguir, serão apresentadas as três primeiras e as três últimas tramitações do Projeto de Lei nº 35/2012:

PROJETO DE LEI DA CÂMARA Nº 35, DE 2012
Autor: DEPUTADO - Paulo Teixeira
Ementa: Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências.
Explicação da ementa: Dispõe sobre a tipificação criminal de delitos informáticos, para tanto acresce os arts. 154-A e 154-B ao Decreto-Lei nº 2.848/40 (Código Penal), para dispor no art. 154- A que constitui crime a invasão de dispositivo informático, consistindo em devassar 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, instalar vulnerabilidades ou obter vantagem ilícita, sujeitando os infratores a pena de detenção de 3 (três) meses a 1 (um) ano e multa, havendo hipóteses de aumento se houver prejuízo econômico, comercialização ou transmissão a terceiro, ou se o crime for praticado contra autoridades públicas: Presidente da República, governadores, prefeitos, Presidente do Supremo Tribunal Federal, Presidente da Câmara dos Deputados, Presidente do Senado Federal e outras; prevê no art. 154-B que os 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 (arts. 1º e 2º). Altera a redação dos arts. 266 e 298 do Decreto-Lei nº 2.848/40 (Código Penal), para dispor no art. 266, em relação o crime de "Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública", que incorre nas mesma penas (detenção, de um a três anos, e multa) quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta o seu restabelecimento; acresce parágrafo único ao art. 298 para dispor que equiparasse a documento particular o cartão de crédito débito, sujeitando os infratores as mesmas penas do crime de falsificação de documento particular, prevista no caput do mencionado artigo (reclusão, de um a cinco anos, e multa).
Assunto: Jurídico - Direito penal e processual penal
Apelido: (CRIMES CIBERNÉTICOS, CAROLINA DIECKMANN)
Data de apresentação: 17/05/2012
Situação atual: Local: 03/01/2013 - Secretaria de Arquivo
Situação: 03/12/2012 - TRANSFORMADA EM NORMA JURÍDICA
Matérias relacionadas: RQS - REQUERIMENTO 776 de 2012 (Senador Eduardo Braga e outros)
Outros números: Origem no Legislativo: CD PL. 02793 / 2011
Norma jurídica gerada: LEI-012737 de 2012
Indexação da matéria: Indexação: ALTERAÇÃO, CÓDIGO PENAL, TIPICIDADE, CRIME, INFORMÁTICA,INVASÃO, DISPOSITIVO, SEGURANÇA, DESTRUIÇÃO, ADULTERAÇÃO, DADOS,INFORMAÇÕES, INTERRUPÇÃO, SERVIÇO, FALSIFICAÇÃO DE DOCUMENTOPARTICULAR, EQUIPARAÇÃO, CARTÃO DE CRÉDITO, CARTÃO DE DÉBITO.
17/05/2012 PLEG - PROTOCOLO LEGISLATIVO
Situação: AGUARDANDO LEITURA
Ação: Este processo contém 13 (treze) folha(s) numerada(s) e rubricada(s).
À SSCLSF.
17/05/2012 SSCLSF - SUBSEC. COORDENAÇÃO LEGISLATIVA DO SENADO
Situação: AGUARDANDO LEITURA
Ação: Aguardando leitura.
Juntada, à fl. 14, legislação citada.
17/05/2012 ATA-PLEN - SUBSECRETARIA DE ATA - PLENÁRIO
Ação: A Presidência recebeu, da Câmara dos Deputados a presente matéria.
Às Comissões de Ciência, Tecnologia, Inovação, Comunicação e Informática; e de Constituição, Justiça e Cidadania.
Publicação em 18/05/2012 no DSF Página(s): 19594 (Ver Diário)
Publicação em 18/05/2012 no DSF Página(s): 19557 - 19565 (Ver Diário)

[...]

18/12/2012 SSCLSF - SUBSEC. COORDENAÇÃO LEGISLATIVA DO SENADO
Ação: Encaminhado ao Plenário.
18/12/2012 ATA-PLEN - SUBSECRETARIA DE ATA - PLENÁRIO
Ação: Leitura do Ofício nº 744/2012, de 18 de dezembro de 2012, do Primeiro-Secretário da Câmara dos Deputados, comunicando que o projeto foi sancionado e convertido na Lei nº 12.737, de 30 de novembro de 2012, e que foi encaminhado a esta Casa uma via dos autógrafos do presente projeto, bem como cópia da mensagem e do texto da lei.
Publicação em 19/12/2012 no DSF Página(s): 74576 - 74578 (Volume nº II) (Ver Diário)
03/01/2013 SARQ - Secretaria de Arquivo
Ação: PROCESSO ARQUIVADO. (Fonte: http://www.senado.gov.br acesso em 06/8/2013).

O Projeto de Lei de Autoria do Deputado Paulo Teixeira e outros. O deputado possui como objetivo acrescentar os artigos 154-A, 154-B, 266 §1º, §2º e 298 Parágrafo Único do

Decreto-Lei nº 2.848/40, pois em sua redação, no ano de 1940, não havia previsão de crimes no âmbito cibernético. Sendo assim ocorreu uma atualização na redação original com o intuito de tipificar os delitos cometidos na rede de computadores. Desde a apresentação do projeto na Câmara dos Deputados, no dia 17/05/2012, o mesmo foi analisado pelos membros da Câmara, passou por votações e pareceres da Comissão de Ciência e Tecnologia, Comunicação e Informática (CCTCI), SSCLSF - SUBSEC. Coordenação Legislativa do Senado, TA-PLEN - Subsecretaria de Ata – Plenário, até sua aprovação definitiva (Fonte: http://www.camara.gov.br acesso em 06/8/2013).

No dia 18/12/2012 o Projeto de Lei da Câmara dos Deputados de nº 35/2012 foi sancionado e convertido na Lei de nº 12.737, de 30 de novembro de 2012, e foi apelidada de (Crimes Cibernéticos, Carolina Dieckmann). O Projeto de Lei foi aprovado, em um só turno de discussão e votação, e enviado para a sanção do Chefe do Executivo (Fonte: http://www.camara.gov.br acesso em 06/8/2013).

Essa nova lei insere em nosso Código Penal mais três artigos e também insere o parágrafo único no artigo 298. O artigo 154 "A" dispõe sobre a "invasão de dispositivo informático", o artigo 154 "B" dispõe sobre a ação penal, o artigo 266 dispõe sobre a "Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública" e por ultimo o parágrafo único do artigo 298 que dispões sobre a "falsificação de cartão". Esta lei está em vigor desde o dia 03 de abril de 2013. As penas previstas variam de três meses a dois anos de prisão, a depender da gravidade do caso.

2.4.6 MARCO CIVIL PL 2126/2011

A Secretaria de Assuntos Legislativos do Ministério da Justiça, juntamente com o Centro de Tecnologia e Sociedade da Escola de Direito da Fundação Getúlio Vargas no Rio de Janeiro, propôs no ano de 2009, a criação de uma constituição para a internet, elencando no projeto as condições de uso da Internet em relação aos direitos e deveres de seus usuários, prestadores de serviços e provedores de conexão e, também, o papel do Poder Público com relação à Internet.

Um dos objetivos é tirar a responsabilidade por parte dos provedores de internet acerca das informações publicadas. A decisão, atualmente, ocorre por meio da jurisprudência e, após a notificação do usuário, os provedores têm 48 horas para deletar o conteúdo da rede.

O texto do projeto trata de temas como neutralidade da rede, privacidade, retenção de dados, a função social da rede e responsabilidade civil dos usuários e provedores.

Como anexo, o projeto na íntegra.

3. O PROJETO DE LEI E OS LIMITES IMPOSTOS AO DIREITO FUNDAMENTAL DE LIBERDADE DE EXPRESSÃO E INFORMAÇÃO

3.1 DIREITOS FUNDAMENTAIS DE LIBERDADE DE EXPRESSÃO E INFORMAÇÃO

Os Direitos Fundamentais estão consagrados na Constituição Federal, no Título II, essenciais à vida da natureza humana, necessários para a digna existência da pessoa. Segundo Pinho (2011), os mesmos são necessários para assegurar uma existência digna, livre e igual a todos os seres humanos.

Para Tavares (2010), não existe nenhum direito fundamental humano que possa ser considerado absoluto, nem nas constituições, sendo o alcance absoluto do mesmo restringido. O autor destaca que os direitos humanos consagrados e assegurados não podem:

- Servir como escudo protetivo para a prática de atividades ilícitas;
- Servir para respaldar irresponsabilidade civil;
- Anular os demais direitos igualmente consagrados pela Constituição;
- Anular igual direito das demais pessoas, devendo ser aplicados harmonicamente no âmbito material.

Conforme Farias, a Inglaterra foi um dos primeiros países a travar uma luta em prol da liberdade de expressão do pensamento e da opinião. Após a Inglaterra ter se manifestado, os Estados Unidos e a França também se manifestaram em prol da liberdade de expressão e de opinião. A Declaração de Direito, de 1689, em inglês *Bill of Rights* do Estado de Virgínia, em seu artigo 12, proclamava-se “a liberdade de imprensa é um dos grandes suportes da liberdade e não pode ser restringida jamais, a não ser por governos despóticos”. Já na França, a Declaração dos Direitos do Homem e do Cidadão de 1789, no seu artigo 11, estabelecia que “a livre manifestação do pensamento e das opiniões é um dos direitos mais preciosos do homem: todo cidadão pode, portanto, falar, escrever e imprimir livremente, é exceção o abuso

dessa liberdade pelo qual deverá responder nos casos determinados por lei" (FARIAS, 2000, p. 38).

Mendel (2009), enfatiza que todas as pessoas têm direto à liberdade de expressão e informação, sendo esta informação consagrada na Declaração Universal dos Direito do Homem, de 1948, de cumprimento obrigatório pelos signatários. O autor destaca que este direito inclui *"a liberdade de expressar opiniões sem interferência e de buscar, receber e transmitir informações e ideias por quaisquer meios e sem limitações de fronteiras".*

Em suma, nas palavras de Farias, a liberdade de expressão e informação atinge o nível máximo de sua proteção quando é exercida por profissionais dos meios de comunicação. Ou seja, além do limite interno referido da veracidade da informação, a liberdade de expressão e informação deve ser combinado com os direitos fundamentais dos cidadãos afetados pelas opiniões e informações (FARIAS, 2000, p. 40).

A Constituição Federal, em seus artigos 5º, inciso IV, IX, XIV e 220, §§ 1º e 2º, regula a liberdade de expressão e informação:

> 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:
> IV - é livre a manifestação do pensamento, sendo vedado o anonimato;
> IX - é livre a expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença;
> XIV - é assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício profissional;
> Art. 220. A manifestação do pensamento, a criação, a expressão e a informação, sob qualquer forma, processo ou veículo não sofrerão qualquer restrição, observado o disposto nesta Constituição.
> § 1º - Nenhuma lei conterá dispositivo que possa constituir embaraço à plena liberdade de informação jornalística em qualquer veículo de comunicação social, observado o disposto no art. 5º, IV, V, X, XIII e XIV.
> § 2º - É vedada toda e qualquer censura de natureza política, ideológica e artística. (BRASIL,1988).

Segundo Meyer-Pflug (2009), o direito de manifestação do pensamento e das ideias deve ocorrer livre de qualquer penalidade ou ameaça, pois é a expressão da razão e manifestação do raciocínio humano. Incide na possibilidade de escolher quais ideias, atitudes intelectuais ao qual se deva adotar. A liberdade de expressão é essencial para o desenvolvimento intelectual da pessoa humana (MEYER-PFLUG, 2009, p. 68).

A liberdade de expressão é entendida como um direito subjetivo fundamental assegurado a todos os cidadãos, e crescente na livre manifestação do próprio pensamento,

ideias e opiniões através de palavras escrita, e imagens ou quaisquer outros meios de difusão, além do direito de se comunicar e receber informações, sem impedimento nem discriminação (FARIAS, 2000, p.40).

De acordo com as palavras de Meyer-Pflug (2009), a liberdade de expressão é o direito de cada um expor suas ideias, opiniões e emoções e tem, por desígnio, a realização pessoal na medida em que expõe a sua livre opinião, a livre ideia e persuasão que achar conveniente. Assim, a garantia da liberdade de expressão é saliente, colocando os indivíduos como os responsáveis por suas opiniões.

Ao falar em liberdade de expressão e comunicação, Farias (2004), em primeiro lugar, expõe que a liberdade de expressão substitui a liberdade de manifestação do pensamento, liberdade de manifestar a sua própria opinião, liberdade de manifestar a consciência, tendo a capacidade de empregar a linguagem liberdade de expressão para abranger as expressões de pensamento, de opinião, de consciência, de crença ou de juízo de valor.

Segundo Meyer-Pflug (2009), o livre ato do pensamento atinge uma esfera maior do que um simples direito de escolher seus próprios conceitos, ou seja, o homem necessita expor as suas opiniões, buscar convencer os outros acerca de seus conceitos e debater com os demais integrantes da sociedade. Ele precisa expressar suas ideias e pensamentos, sofrendo influência de pessoas da sociedade, com condições sociais, econômicas e culturais diferentes.

Assim afirmava Norberto Bobbio 1992, ao dizer que os direitos dos homens são direitos históricos, direitos esses, fundamentais, são nascidos por certas situações, caracterizadas por lutas em defesa de novas liberdades, nascidas de forma gradual. Numa época histórica, o que parece fundamental para algumas culturas, não era fundamental na mesma época para outras.

Quando Meyer-Pflug (2009) fala da liberdade expressão e pensamento, menciona que a mesma deriva da liberdade religiosa, da liberdade de informação, da liberdade de imprensa e da própria inviolabilidade de correspondência, sendo que a liberdade de expressão do pensamento pode dar-se por meio do uso da escrita, das imagens e não essencialmente de forma falada. A redação constitucional protege o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, exceto, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal, no art. 5º, XIII, da Constituição Federal de 1988.

Em poucas palavras Jabur, manifesta que a primeira forma pela qual os seres humanos manifestarem a sua razão foi pela liberdade de pensamento, estando ligada ao direito à liberdade. O direito de mostrar o que se pensa é tanto quanto limitado pelo conteúdo e extensão de outras garantias primordiais, consagradas por nosso sistema jurídico (JABUR, 2000, p. 55)

Jabur , critica o ser humano pela forma de expressar os seus pensamentos, e diz que: "*seria ilógico, incalculável e inútil que a qualidade de pensar ficasse confinado, permanecesse oculto no intelecto".* É do ser humano o dever de expressão, onde está ligada à liberdade de pensamento (JABUR, 2000, p. 55-56).

3.2 A LIBERDADE DE EXPRESSÃO E INFORMAÇÃO NA INTERNET

A internet, nas últimas décadas, vem disseminando, e o direito, de certo modo, teve que acompanhar esta evolução, acelerando o seu desenvolvimento e aprimorando-se para solucionar os conflitos que emergem do meio virtual. Meios ilícitos, violência e crimes fazem parte do dia-a-dia da rede mundial de computadores. É fundamental que o direito acompanhe esta evolução, para regular de forma eficiente e eficaz os delitos praticados no ambiente virtual, pois muitos destes são praticados no anonimato (TINOCO, 2012).

A informática, nos dias atuais, confere à liberdade de expressão uma nova roupagem. Segundo Jabur (2000), a liberdade de expressão ganha um novo relevo em virtude do alcance dos meios computacionais e aprimora-se em razão da troca de ideias, sentimentos, sabedoria e conhecimentos, que promove a evolução dos seres humanos. Constitui-se, ainda, em uma virtude dos regimes democráticos (JABUR, 2000).

O Ministro Toffoli, em um dos seus julgamentos no Tribunal Superior Eleitoral, faz uma referencia especificamente à Internet:

> "Em meus julgamentos no TSE, a esse propósito, tenho defendido a ampla liberdade de uso da internet, essa arena do livre pensamento, do tráfego consciente de ideias e de difusão de doutrinas. A internet é o templo da liberdade comunicativa, seja por não ter regulação de conteúdo (na maior parte dos países do mundo ocidental democrático), seja por não ter concessionários que controlem seu conteúdo de modo oligopolizado ou monopolizado, seja pela liberdade que cada usuário detém para receber ou emitir suas produções artísticas, culturais ou educacionais" (Fonte: http://www.stf.jus.br acesso em 28 de setembro de 2013).

A liberdade de expressão e os direitos autorais estão regulamentados na Constituição Federal, ou seja, a proteção aos direitos morais do autor, tais como a eficácia do direito de arrependimento e o direito à conservação da integridade da obra. A produção literária, científica e artística, de criação do espírito do autor, está protegida pelos direitos morais do autor, inclusive as que competem ao domínio público, sendo o estado o zelador da obra (LIMA, 1997).

Segundo Ferreira (2013), um dos problemas mais debatidos na atualidade é a obrigação de restrições à liberdade de expressão na Internet, para tutela dos direitos de personalidade.

Ao falarmos em liberdade de expressão na internet, nos deparamos com o direito à privacidade, direito à intimidade e direito à honra, direitos estes que entram em conflito com a liberdade de expressão, conflitos estes que devem ser regulados pelo direito, por meio de regras fundamentais que permitam apresentar os limites de cada um, de acordo com as normas constitucionais (FERREIRA, 2013).

A Internet representa uma fase avançada entre os meios tecnológicos, ou seja, um novo desafio para o direito. Para a sociedade, a internet apresenta inúmeras vantagens mas, também, representa uma grande ameaça à vida privada do usuário. As ameaças são resultantes da falta de conhecimento do usuário quando se conecta à internet, pois não sabe quando as informações a seu respeitos são coletadas, como, por exemplo, pelos vírus que são instalados no computador, gerando cópias dos arquivos contidos na máquina. O usuário deixa-se levar pelas vantagens que a rede de computadores oferece e acaba esquecendo que informações a seu respeito são reveladas durante o período da navegação (EL-JAICK, 2013).

Para Ferreira, as restrições à Liberdade de Expressão, nesse caso, na internet, devem estar estipuladas em lei. Caso a lei não exista, é necessário recorrer aos princípios de aquiescência e ajuizamento entre os direitos envolvidos e os valores constitucionais, princípios esses que, normalmente, contêm uma maior valoração, uma decisão política relevante, um fundamento ético, que demonstram uma determinada direção a seguir (FERREIRA, 2013).

Sobre a liberdade de expressão, Silva (2000), fala que não são todos os indivíduos que possuem acesso aos meios de comunicação social como: rádio, televisão pública ou a participação do individuo em algum programa radiotelefônico ou televisivo, onde de alguma forma esse programa possa ouvir a opinião do público, através de uma chamada de telefone,

ou ainda através de carta para ser publicada em determinado jornal, quase sempre não são publicadas, com o seguinte critério de não ter espaço na coluna, ficando a opinião retida.

Segundo Tinoco (2012), um dos instrumentos capazes de realizar o direito à informação são o Twitter [1]e o Facebook[2]. O Facebook é uma rede social lançada em 2004, que se expande em grande velocidade, atingindo todos os continentes. Soma cerca de 850 milhões de usuários com previsão de ultrapassar 1 bilhão ainda este ano. O Twitter, por sua vez, possui função semelhante ao Facebook. É conhecido com uma rede de informações que conecta os usuários às últimas notícias, histórias, idéias e opiniões publicadas. Disponibilizado em 20 idiomas e presente no mundo todo, estima-se que há 33,3 milhões de perfis brasileiros no site sendo 29,9 milhões de japoneses e 107,7 milhões de perfis norte americanos[3]. Ambos compartilham fotos, imagens e conversas.

O Twitter e o Facebook são instrumentos pelos quais as pessoas podem manifestar a liberdade de expressão e falar livremente o que pensam, possibilitando a visualização da mensagem à todos aqueles que estão conectados. Nessa linha, Tinoco (2012) afirma que a informação produzida por meio de *posts*, *twet*s ou compartilhamento, atinge um número indeterminado de pessoas potencialmente alto. "*As redes sociais são verdadeiros meios de comunicação que se compatibilizam com a definição de modo a caracterizar instrumento capaz de realizar o direito à informação"* (TINOCO, 2012).

3.3 AS PRÁTICAS TIPIFICADAS COMO CRIMES DE ACORDO COM A REDAÇÃO DO CÓDIGO PENAL E NOS PROJETOS DE LEI

Num mundo globalizado, a internet é grande responsável pela consolidação desta mudança. A forma com que as informações podem ser trocadas pela rede, com rapidez e baixo custo, fazem com que o uso da ferramenta internet desenvolva uma conexão entre as pessoas de maneira acelerada em todo o mundo (GATTO, 2013).

De acordo com Lessig (1999), professor de Direito Constitucional da Universidade de *Harvard*, a responsabilidade por regular as práticas delituosas na internet é dos próprios softwares e não das leis. Se o programa permite determinada ação, a lei é inócua. Se o

[1]http://www.twitter.com
[2]http://www.facebook.com/
[3]http:// www.prgo.mpf.gov.br

software não autoriza inserir determinada informação ou realização de tal ação, nenhuma lei poderia obrigar (LESSIG, 1999).

De acordo com os pensamentos de Gatto (2013), o volume de acesso à internet, tanto para o divertimento, quanto meio de trabalho, fez com que esta ferramenta se tornasse um meio necessário para a sociedade, trazendo questões até então desconhecidas para os operadores do direito. Esta tecnologia fez transparecer a necessidade urgente do direito acompanhar as mudanças da sociedade.

Em decorrência do avanço mundial da internet, o número de crimes no ambiente virtual também aumentou. Crimes que, muitas vezes, ficam impunes, com a criação de comunidades criminosas nomeado de *crackers* que, graças à obscuridade, se vangloriam de crimes praticados na rede sem o menor pudor, crimes que, na maioria das vezes, satisfazem a realização pessoal de invadir outro site, não visando, diretamente, a satisfação material. Crimes informáticos, tais como a invasão de sites da internet, com o simples objetivo de ultrapassar uma barreira de segurança, que ganham maior repercussão quando expostos na internet, nos casos nos casos dos crimes de injúria, difamação ou calúnia que, devido à velocidade na divulgação da mensagem criminosa, alcançam um maior número de pessoas que visualizam a mensagem atentatória (GATTO, 2013).

Está estatuído no artigo 1º, do Código Penal Brasileiro, o princípio da legalidade também conhecido como o princípio da reserva legal, com a seguinte redação: *"Não há crime sem lei anterior que o defenda, nem pena sem prévia cominação legal"* (BRASIL, 2013).

Incumbe ressaltar que a Constituição Federal estabelece, no seu artigo 5º, inciso XXXIX, que:

> "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:
> XXXIX – Não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal (BRASIL, 1988).

Assim sendo, conforme o princípio da legalidade, alguém só poderá ser punido se, anteriormente ao fato praticado, existir uma lei que considere como crime a ação, ainda que o fato seja imoral, danoso ou anti-social, não haverá possibilidade de punir o autor sem uma lei específica (MIRABETE, 2008, p. 201).

O princípio da legalidade, segundo Delmanto (2002), não pode aceitar leis vagas ou imprecisas. A descrição do fato típico deve ser taxativo evitando-se os tipos penais abertos. O juiz que aplica a lei penal é proibido de empregar a analogia *in malam partem* ou interpretar a

lei de maneira extensiva tornando mais severa a punição. Não cabe ao juiz preencher as falhas da lei incriminadora, ficando vedado completar o trabalho do legislador para punir alguém.

Mirabete (2008) conceitua a tipicidade penal como correspondência exata, adequando ao fato natural concreto como descrito na lei. O tipo penal é composto não só de elementos objetivos mas, também, de antijuridicidade.

Conforme Gatto (2013), são vários os tipos de crimes cometidos por meio da internet e que não estão tipificados no ordenamento jurídico, ou seja, não podem ser passíveis de punição, pois não possuem lei específica. Nesses casos, é comum o uso da analogia jurídica ferindo o princípio da reserva legal, para adequar crimes sem tipificação aos já descritos no ordenamento jurídico. Quando uma informação falsa é veiculada na rede, certamente essa informação terá uma exibição muito mais rápida e abundante, do que se esse mesmo fato fosse veiculado por outros meios, que não através da internet (GATTO, 2013).

Para conceituar e exemplificar o que seria o uso da analogia, o professor e advogado Fernando Capez relata:

> "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, p.59).

Os crimes de informática, de acordo com o texto de Castro (2003), classificam-se em

puros, mistos e comuns sendo todos realizados com o uso da internet.

- Puros: o agente tem a intenção de atingir o computador, o sistema de informação ou os dados contidos no computador.
- Mistos: o agente não esta focado no sistema de informática mas, sim, em usar a informática como instrumento para a consumação da ação delituosa.
- Comuns: o agente não visa o sistema informático e seus componentes, mas faz uso da informática como instrumento para a realização da ação.

Conforme Gatto (2013), quando se fala em responsabilidade nos crimes virtuais, destaca-se a responsabilidade de os provedores de internet em armazenar, em seus bancos de dados, informações sobre seu cliente que poderão, em caso de crime, serem usadas como provas.

Segundo Melo (2000), os provedores de internet são os fornecedores do serviço de conexão à internet do usuário, ou seja, um conjunto de redes e meios de transmissão, roteadores, equipamentos e também protocolos que são usados na comunicação entre computadores.

Abaixo será explanado sobre a nova tipificação de crimes de acordo com a redação dos projetos de lei e suas descrições acerca dos crimes praticados na rede de computadores. Cabe salientar que não será feita uma comparação entre os projetos de lei mas, tão somente a discussão sobre os crimes já previstos no código penal e as possíveis novas condutas típicas vinculadas aos cibercrimes.

3.3.1 Do Crime de Dano

Segundo Nucci (2011), o crime de dano consiste em destruir (arruinar, extinguir ou eliminar), inutilizar (tornar inútil ou imprestável alguma coisa) ou deteriorar (estragar ou corromper alguma coisa parcialmente) coisa alheia. Quem, por algum motivo, desaparece com coisa alheia não responde por crime algum. A expressão desaparecer não significa destruir, inutilizar ou deteriorar a coisa alheia e, somente quem faz sumir coisa de seu desafeto para que fique desesperado a procura do objeto, responde civilmente pelo ato.

Segundo o Código Penal o crime de dano está previsto no artigo 163, tendo como pena de detenção de 1(um) a 6 (meses), ou multa (BRASIL, 2013).

Conforme a redação do projeto de Lei nº 84/99, de autoria do Deputado Luiz Piauhylino, o crime de dano no meio informático tem como pena detenção de 1 (um) a 3(três) anos, e multa. Já o projeto de lei nº 1713/95, de autoria do deputado Cássio Cunha Lima do PMDB/PB, prevê pena de detenção, de 2 (dois) a 4 (quatro) anos, e multa.

3.3.2 Dos Crimes contra a honra

Os crimes contra a honra também são tipos penais que se valeu da internet como ferramenta para a prática delituosa. Para Aref Abdul Latif (2007) os crimes contra a honra dividem-se em três espécies: calúnia, difamação e injúria, estando os mesmos em ordem decrescente de gravidade.

Quando falamos em honra, falamos em atributos morais, físicos e intelectuais, que protegem a auto-estima e a reputação pessoal. A auto-estima está ligada à honra subjetiva e a

reputação, à honra objetiva. A calúnia e a difamação atingem a honra objetiva. A injúria atinge à honra subjetiva (AREF ABDUL LATIF, 2007).

Segundo Estefam (2010) pode-se conceituar esse crime como um conjunto de qualidades da pessoa humana, conferindo-lhe respeito e estima própria. *"O homem, ser gregário, depende não apenas da satisfação do seu instinto de auto-afirmação, portanto de correspondente auto-estima, como também da aprovação do meio em que vive"*(ESTEFAM, 2010, p. 236).

3.3.2.1 Calúnia

Conforme Estefam (2010), é fundamental que seja imputado a alguém fato que constitua crime. Como todo crime contra a honra é um delito de forma livre, pode ser praticado por qualquer um, de forma verbal, falada, mas pode ser, também, por escrito, por mímica, por símbolo ou gestos (ESTEFAM, 2010, p. 252).

Para Damásio (2007), no que se referente à calúnia, esta constitui crime formal, pois o comportamento e o resultado visado pelo sujeito não exige a produção do resultado. Não é necessário que o sujeito consiga obter o resultado alvejado, que é o dano a honra objetiva do agente.

No Código Penal, o crime de calúnia está previsto no artigo 138 e tem, como pena, detenção de 6 (seis) meses a 2 (dois) anos, e multa (BRASIL, 2013).

3.3.2.2 Difamação

De acordo com Prado (2010), a difamação foi apenas inserida como crime no Código Penal de 1940, até então não era considerada crime. *"A Difamação consiste na imputação de fato não delituoso, ofensivo a reputação de alguém."* (PRADO, 2010, p. 237).

A Calúnia nada mais é do que uma modalidade agravada da difamação"(PRADO, 2010, p. 237).

Damásio de Jesus, em sua obra Direito Penal, 2° volume parte especial, Dos Crimes Contra a Pessoa e dos Crimes Contra o Patrimônio (2007), diferencia o crime de difamação da calúnia e da injúria. Na calúnia, o fato imputado é definido como crime, na difamação, o fato que é imputado ao ofendido somente é ofensivo à sua reputação. Na calúnia exige-se o

elemento de falsidade da imputação, o que é irrelevante na difamação. A injúria versa sobre a qualidade negativa da vítima, ofendendo a honra subjetiva, na difamação, há a ofensa da reputação do ofendido.

O Código Penal de 1940 prevê, em seu artigo 139, o crime de difamação, tendo como pena, a detenção de 3 (três) meses a 1 (um) ano, e multa (BRASIL, 2013).

3.3.2.3 Injúria

Segundo Nucci (2011), injuriar significa ofender alguém de forma vulgar ou até mesmo xingar. *"É preciso que a ofensa atinja a dignidade (respeitabilidade ou o amor próprio) ou o decoro (correção moral ou compostura) de alguém."* (NUCCI, 2011, p. 694).

Segundo as palavras de Costa Júnior (1999), a injúria ofende o sentimento de dignidade,a honra subjetiva do ofendido. Não é tratada como na difamação, que atinge a honra exterior da vítima. Trata-se de ofender a dignidade da vítima.

O Código Penal de 1940 prevê, em seu artigo 140, o crime de injúria e tem como pena de 1 (um) a 6 (seis) meses de detenção, ou multa.

3.3.3 Acesso indevido ou não autorizado

O atual Código Penal não traz em sua redação nada específico sobre a sanção para o acesso indevido ou não autorizado de dados de computador. Somente no artigo 325, inciso I, fala do acesso de pessoas não autorizadas a sistemas de informações ou banco de dados da Administração Pública:

> Art. 325 - Revelar fato de que tem ciência em razão do cargo e que deva permanecer em segredo, ou facilitar-lhe a revelação:
> I – permite ou facilita, mediante atribuição, fornecimento e empréstimo de senha ou qualquer outra forma, o acesso de pessoas não autorizadas a sistemas de informações ou banco de dados da Administração Pública;
> Pena – reclusão, de 2 (dois) a 6 (seis) anos, e multa (BRASIL, 2013)

O Projeto de Lei de nº 84/99, de autoria do Deputado Luiz Piauhylino, traz em seu artigo 9º, a seguinte redação, tipificando esse crime: *Art. 9º - Obter acesso, indevido ou não autorizado, a computador ou rede de computadores. Pena: detenção, de seis meses a um ano e multa.*

Na mesma linha, o projeto de lei nº 1713/95, de autoria do deputado Cássio Cunha Lima do PMDB/PB, tipifica, em seu artigo 18, o crime de acesso indevido e não autorizado:

Art. 18 – obter acesso, indevidamente, a um sistema de computador ou uma rede integrada de computadores: Pena – detenção, de 3 (três) meses a 6 (seis) meses, ou multa.

3.3.4 Apropriação indébita

Segundo Estefam, a ação ou a omissão que caracteriza o delito de apropriação, ocorre quando alguém detém objeto alheio, passando a agir como se dono fosse. Para ficar caracterizado o crime de apropriação indébita, o ofendido deve entregar o objeto de forma livre e espontânea ao agente. Caso ocorra fraude na entrega da coisa, caracteriza-se o estelionato e, se houver violência ou grave ameaça à pessoa, caracteriza roubo.

O Código Penal, traz em sua redação, especificamente, nos seus artigos 168 a 170, o crime de apropriação indébita que tem, como pena, detenção de 1 (um) mês a 1 (um) ano ou multa (BRASIL, 2013).

No projeto de lei nº 1713/95, de autoria do deputado Cássio Cunha Lima do PMDB/PB em seu artigo 19, especifica o crime de apropriação indébita de informações, apresentando uma pena superior a do Código Penal, que é de reclusão de 1 (um) ano a 3 (três) anos, e multa.

Ainda, o projeto de lei do deputado Cássio Cunha Lima, menciona o crime em seu artigo 21, que caracteriza como apropriação indevida de valores, de que tem posse ou detenção através da manipulação de qualquer sistema de processamento de dados obtendo, assim, vantagem econômica para si ou para outrem e tem, como pena, reclusão de 1 (um) a 5 (cinco) anos, e multa.

3.3.5 Invasão de dispositivo informático: Arts 154-A e 154-B

Cavalcante explica o novo artigo 154-A e 154-B do Código Penal: invasão informática no sistema ou na memória do dispositivo informático, equipamento físico chamado *hardware*, podendo ser utilizado para rodar programas *softwares* ou, ainda, para ser conectado a outros equipamentos como por exemplos, computador, *tablet, smartphone*, memória externa, entre outros (CAVALCANTE, 2012).

Ainda segundo Cavalcante, invadir dispositivo alheio significa que o bem a ser invadido deve pertencer à terceiro. Em regra, o desbloqueio de alguns dispositivos informáticos é prática comum entre os *hackers* para que eles possam realizar certas funções originalmente não previstas de fábrica (CAVALCANTE, 2012)

O projeto de lei nº 234/96, de autoria do Senador Júlio Campos, dispõe sobre o crime contra a inviolabilidade de comunicação e traz, em seu artigo 1º, a seguinte redação:

> **Art.1º** - É crime contra a inviolabilidade de comunicação de dados de computador:
> I – manipular, sabotar, espionar, acessar de qualquer maneira, sem a autorização competente, o conteúdo de computador.
> Pena: detenção, de um a dois anos, e multa.
> II - utilizar abusivamente se a devida autorização das instalações de processamento de dados.
> Pena: detenção, de um ano a seis meses, ou multa.

Ao Código Penal foram acrescentados os artigos 154-A e 154-B com a seguinte nomenclatura:

> 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
> 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 (BRASIL, 2013).

3.3.6 Falsificação de documento particular: Art. 298 do CP

Conforme Nucci (2011), a falsificação de documentos consiste em reproduzir, ou imitar um documento particular. Particular é todo aquele produzido por alguém que manifesta sua vontade.

O Código Penal vigente, quando fala em falsificação de documento traz somente o artigo 298, com seguinte redação: *Art. 298 - Falsificar, no todo ou em parte, documento particular ou alterar documento particular verdadeiro: Pena - reclusão, de um a cinco anos, e multa* (BRASIL, 2013).

A nomenclatura do projeto de lei nº 1713/95, tipifica a falsificação de documento particular, em seu artigo 24, com a seguinte redação: *Art. 24 – Falsificar, alterar ou apagar documentos através de sistema ou rede integrada de computadores e seus periféricos: Pena – reclusão, de 1 (um) a 5 (cinco) anos, e multa.*

Segundo Delmanto, cabe salientar a importância de se observar a distinção que existe entre o falso material e o falso ideológico. Na falsidade material, se frauda a forma do documento a qual é alterada, no todo ou em parte, e o agente fraudador cria um documento

novo. A falsidade ideológica, ao contrário, a forma em que se encontra o documento é verdadeira, mas o conteúdo existente é falso, ou seja, o que está contido no documento não corresponde à verdade (DELMANTO, 1991).

3.3.7 Falsificação de cartão

Com a aprovação do Projeto de Lei nº 35/2012, atual Lei nº 12.737 de 30 de novembro de 2012, apelidado de Lei Carolina Dieckmann, a Lei dos Crimes Cibernéticos, de autoria do deputado Paulo Teixeira (PT-SP), acrescentou no artigo 298 do Código Penal, o parágrafo único, que consiste na Falsificação de Cartão, com a seguinte nomenclatura: *Parágrafo único. Para fins do disposto no caput, equipara-se a documento particular o cartão de crédito ou débito*. *Pena - reclusão, de um a cinco anos, e multa.* (BRASIL, 2013).

Ao falar em cartão de crédito, podemos conceituar como um documento particular e a falsificação da tarja magnética viola o artigo 298 do Código Penal. O cartão de crédito é uma tecnologia recente, criado no início deste século. A interpretação e aplicação da norma penal causa muita polemica, uma vez que o cartão de crédito ou bancário enquadra-se no conceito de documento particular, pois existe um vínculo jurídico entre o titular e a instituição financeira, através do qual é possível adquirir mercadorias no comércio credenciado ou acessar os serviços bancários (Fonte: www.stj.gov.br acesso em 29 de novembro de 2013).

4 CONCLUSÃO

Um novo modelo de sociedade está sendo estruturado: a sociedade virtual. O volume de informação gerado e o aumento da conectividade de dispositivos eletrônicos na rede mundial de computadores contribuem massivamente para isto. A evolução da sociedade digital é exponencialmente superior às normas jurídicas existentes que regulam as hipóteses vinculadas aos cibercrimes. Assim como o direito rege a sociedade atual para que não haja conflitos, existe a necessidade de reger uma sociedade digital.

O Direito Digital é a evolução do Direito tradicional para responder as questões relacionadas à internet e as relações existentes na mesma, trazendo soluções técnicas e jurídicas para os conflitos e impasses gerados no ambiente virtual.

O grande volume de acessos à internet e a rápida disseminação de informações trazem consigo os desafios e crimes praticados por usuários mal intencionados. Desafios no âmbito jurídico de como punir e regular o mundo digital e os crimes cibernéticos comumente praticados na rede.

Atualmente as regras que norteiam o uso da internet existem apenas para regulamentar os provedores de internet e normas específicas dos sites. Quanto à auto-regulamentação, existem diversos questionamentos a cerca das limitações que esta poderá gerar, como a liberdade de expressão e de conexão.

Compreende-se que a internet por se tratar de uma sociedade digital com interação entre seus usuários possui influência na política, no direito, na vida e no trabalho das pessoas. Portanto o direito não pode ficar alheio ao mundo virtual. É necessário que haja normas para regular, filtrar e conduzir o mundo virtual da Internet, obtendo controle sobre o volume de informações produzidas, não desconsiderando a preservação de direitos fundamentais como a privacidade, a liberdade de expressão e os direitos autorais.

Em função dos moldes desta nova sociedade, “a digital”, é de suma importância à existência de uma legislação para regular o uso de computadores e a internet, no intuito de atender aos anseios da comunidade como um todo, seja física ou virtual. Para isso, torna-se necessária a aprovação dos projetos de leis em trâmite no Congresso Nacional.

REFERÊNCIAS

ARAS, Vladimir. **Crimes de informática**. Uma nova criminalidade. **Jus Navigandi**, Teresina, ano 5, n. 51, out. 2001. Disponível em: (Acesso em: 20 setembro de 2012).

AREF ABDUL LATIF, Omar. Dos crimes contra a honra. In: **Âmbito Jurídico**, Rio Grande, X, n. 41, maio 2007. Disponível em: <http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=1829>. Acesso em set 2013.

BOBBIO, Norberto. **A Era dos Direitos**. Rio de Janeiro: Campus, 1992. UNESCO, 2009.

BRASIL, Angela Bittencourt. Assinatura digital. Jus Navigandi, Teresina, ano 5, n. 40, 1 mar. 2000. Disponível em: <http://jus.com.br/revista/texto/1782>. Acesso em: 17 out. 2012.

CASTRO, Carla Rodrigues Araújo. **Crimes de Informática e seus Aspectos Processuais**. Rio de Janeiro: Lumen Juris, 2003.

BRASIL, Constituição, 1988. **Constituição da República Federativa do Brasil, 1988**. São Paulo, Saraiva, 1989

BRASIL. **Código Penal:** DECRETO-LEI No 2.848, DE 7 DE DEZEMBRO DE 1940. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm>. Acesso em: 02 set. 2013.

CÂMARA DOS DEPUTADOS. Disponível em: <http://www.camara.gov.br>. Acesso em: 27 maio 2013.

CÂMARA DOS DEPUTADOS. Projetos de Leis e Outras Proposições: PL 84/1999. Disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=15028>. Acesso em: 13 ago. 2013.

CANEN, Doris. **AS PARCERIAS ENTRE O SETOR PÚBLICO E O SETOR PRIVADO COMO MECANISMO DE REGULAÇÃO JURÍDICA DA INTERNET NO DIREITO BRASILEIRO. 2009.** Disponível em: <http://www.dominiopublico.gov.br/download/teste/arqs/cp097203.pdf>. Acesso em: 23 set. 2013.

CAPEZ, Fernando. **Curso de Direito Penal**, volume 1, parte geral. São Paulo; Saraiva, 2010

CARVALLO, Kildare Gonçalves. **Técnica Legislativa.** Belo Horizonte: Del Rey, 1993

CASTRO, Aldemario Araújo. **Internet e os Tipos Penais que Reclamam Ação Criminosa em Público**. 2003. In: Webly. Disponível em <http://www.webly.com.br/forum/lofiversion/index.php/t11293.html>. Acesso em 07 jul 2013.

CASTRO, Carla Rodrigues Araújo. **Crimes de Informática e seus Aspectos Processuais**. Rio de Janeiro: Lumen Juris, 2003.

CAVALCANTE, Márcio André Lopes. **Primeiros comentários à Lei 12.737/2012**, que tipifica a invasão de dispositivo informático.2012. Disponível em: <http://www.dizerodireito.com.br/2012/12/primeiros-comentarios-lei-127372012-que.html>. Acesso em: 10 set. 2013.

CAVALIERI, Sergio Filho. **Programa de Responsabilidade Civil**. Rio de Janeiro. Forense, 1997

CHEQUER, Cláudio. **A Liberdade de Expressão como Direito Prima Facie** - análise crítica e proposta de revisão ao padrão jurisprudencial brasileiro. RJ: Lumen Juris, 2011

CORRÊA, Gustavo Testa. **Aspectos jurídicos da Internet.** São Paulo: Saraiva, 2000

COSTA JÙNIOR, Paulo José da, **Direito Penal**: Curso Completo. 6ª Ed. – São Paulo: Saraiva. 1999.

DELMANTO, Celso. **Código Penal Comentado**. 6 ed. atual. e amp. Rio de Janeiro: Renovar, 2002

DELMANTO, Celso. Código Penal comentado. Rio de Janeiro: Renovar, 1991

EL-JAICK, Juliana Grillo. **Normatividade Jurídica**: Conflitos entre o Direito à Intimidade e à Vida Privada e o Direito à Informação, Liberdade de Expressão e de Comunicação.ed. EMERJ Rio de Janeiro. 2013. -. Disponível em: <http://www.emerj.tjrj.jus.br/serieaperfeicoamentodemagistrados/paginas/series/11/normatividadejuridica.pdf#page=110>. Acesso em: 18 set. 2013.

ESTEFAM, André. **Direito Penal**. Volume 2.São Paulo: Saraiva, 2010.

FARIA, Caroline. Código de Hamurabi. 19.06.08. Disponível em <http://www.infoescola.com/historia/codigo-de-hamurabi/>. Acesso em 13/08/2013.

FARIAS, Edilsom Pereira de. **Colisão de Direitos**. A Honra, A Intimidade, A Vida Privada e a Imagem Versus a Liberdade de Expressão e Informação. Porto Alegre, RS: PENA, 2000 (http://www.planalto.gov.br acesso em 13/08/2013)

FARIAS, Edilsom. **Liberdade de Expressão e Comunicação**: teoria e proteção constitucional. São Paulo: Revista dos Tribunais, 2004

FERREIRA, Elaine Garcia. **Quais são as Restrições á Liberdade de Expressão na Internet?:** -. -. Disponível em: <http://enoreg-rj.com.br/wp/quais-sao-as-restricoes-a-liberdade-de-expressao-na-internet/>. Acesso em: 02 set. 2013.

FERREIRA, Érica Lourenço de Lima. **Criminalidade Economia Empresarial e Cibernética.** O Empresário como Delinquente Econômico e os Crimes Cometidos através da Internet. Florianópolis: Momento Atual, 2004. 122 p.

FONSECA Filho, Cléuzio. **História da computação:** O Caminho do Pensamento e da Tecnologia. Porto Alegre : EDIPUCRS, 2007. 205 p.

FRANÇA, Antônio de S. Limongi. **Cibernética Jurídica.** São Paulo, Revista do Direito Civil

FRANÇA, R. L.(coord.) - Enciclopédia Saraiva do Direito. São Paulo, Saraiva, 1977. v. 48, p. 430.

GATTO, Victor Henrique Gouveia. **Internet e Informática:** Tipicidade penal dos crimes cometidos na internet. -. Disponível em: <http://www.ambito-juridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=10065&revista_caderno=17>. Acesso em: 02 set. 2013.

GOUVÊA, Sandra. **O Direito na Era digital:** Crimes Praticados por meio da Informática. Rio de Janeiro: Mauad, 1997. 164 p.

http://<www.SaferNet.org.br> (Acesso em: 20 de setembro de 2012)

http://www.ibope.com.br/calandraWeb/servlet/CalandraRedirect?temp=5&proj=PortalIBOPE

&pub=T&db=caldb&comp=Noticias&docid=C2A2CAE41B62E75E83257907000EC04F>.

Acesso em: 01 mar. 2012.

http://www.safernet.org.br/site/prevencao/pesquisas(acesso em 03 de agosto de 2012)

INELLAS, Gabriel César Zaccaria de. **Crimes na Internet.** 2ª Edição. Editora Juarez de Oliveira. São Paulo. 2009.

JABUR, Gilberto Haddad**. Liberdade de pensamento e direito à vida privada**: conflitos entre direitos de personalidade. São Paulo: Revista dos Tribunais, 2000, p.160.

JESUS, Damásio Evangelista de. **Direito penal: parte especial: dos crimes contra a pessoa e dos crimes contra o patrimônio**. São Paulo: Editora Saraiva, 2005
http://www.jus.com.br/revista/texto/21330/dano-moral-em-sites-de-relacionamento/3 (acesso em 20 de setembro de 2012)

JESUS, Damásio, **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

KOWALTOWSKI, Tomasz. Von Neumann: suas contribuições à Computação. **Estud. av**., São Paulo, v. 10, n. 26, Abr. 1996.

LENZA, Pedro. **Direito Constitucional Esquematizado.** 15. Ed. Ver. Atual e ampl. São Paulo: Saraiva, 2011. p. 1196

LESSIG, Lawrence. **Code and other laws of cyberspace**:1999. Disponível em: <http://www.emerj.tjrj.jus.br/paginas/trabalhos_conclusao/1semestre2012/trabalhos_12012/nabilajensignetinoco.pdf>. Acesso em: 26 ago. 2013.

LIMA, Cassio Cunha. **Projetos de Leis e Outras Proposições:** PL 1713/1996. Disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=17120>. Acesso em: 08 ago. 2013.

LIMA, George Marmelstein. **A reprodução não-autorizada de obras literárias na Internet**. Jus Navigandi, Teresina, ano 2, n. 21, 19 nov. 1997 . Disponível em: <http://jus.com.br/artigos/1792>. Acesso em: 2 set. 2013.

MANSO, Eduardo Vieira. **Direito Autoral; Exceções Impostas aos Direitos Autorais (Limitações e Derrogações)**. São Paulo: José Burshatsky, 1980.

MELO. José Eduardo Soares de. ICMS.ISS **– Comunicação Eletrônica**. Revista de Direito Tributário. Malheiros, São Paulo,2000.

MENDEL, Toby.Liberdade de informação: um estudo de direito comparado.2.ed. Brasília: 2009.

MENDES, Gilmar Ferreira. COELHO, Inocêncio Mártires. BRANCO, Paulo Gustavo Gonet. **Curso de Direito Constitucional.** São Paulo. Ed. 2ª. Saraiva, 2008. p. 1432.

MEYER-PFLUG, Samantha Ribeiro. **Liberdade de Expressão e Discurso do Ódio**. São Paulo: Editora Revista dos Tribunais, 2009

MIRABETE, Julio Fabbrini. **Manual do Direito Penal**, volume 1: parte geral Julio Fabbrini Mirabete, Renato N. Fabbrini – 24 ed São Paulo: Atlas, 2008

MONTESQUIEU, Charles Louis de Secondat . **Cartas Persas**. Lisboa : Estampa,1989.

MORAES, Alexandre de. **Direito Constitucional.** 27 ed. São Paulo:Atlas, 2011. 944 p.

NUCCI, Guilherme de Souza. **Manual de direito penal**: parte geral, parte especial. 7. ed. rev., atual. e ampl. São Paulo: Revista dos Tribunais, 2011.

PEREIRA, Elizabeth Dias Kanthack. **Proteção Jurídica do Software no Brasil.** 1ª Ed. Curitiba: Juruá, 2011. 185 p.

PIAUHYLINO, Luiz. PL 84/99: Disponível em: <http://www.mpba.mp.br/atuacao/infancia/leis/crimes/projeto_lei_084_1999.pdf>. Acesso em: 13 ago. 2013

PIMENTEL, Alexandre Freire. **O Direito Cibernético.** Um enfoque teórico e Lógico-

Aplicativo. Rio de Janeiro: Renovar, 2000. 267 p.

PINHEIRO, Patrícia Peck. **Direito digital.** 2. ed. rev., atual. e ampl. São Paulo:Saraiva, 2007.

PINHO, Rodrigo César Rebello. **Teoria Geral das Constituições e Direitos Fundamentais** - Sinopses Jurídicas. São Paulo: Saraiva, 11ª edição, volume 17, 2011.

PRADO, Luiz Regis. **Curso de direito penal brasileiro**, volume 2: parte especial. Arts. 121ª 249.9.ed. rev., atual. e ampl São Paulo: Revista dos Tribunais, 2010.

REALE, Miguel. **Lições Preliminares de Direito.** 27ª ed. São Paulo: Saraiva. 2002.

REINALDO FILHO, Demócrito. O projeto de lei sobre crimes tecnológicos (PL nº 84/99). Notas ao parecer do Senador Marcello Crivella. **Jus Navigandi**, Teresina, ano 9, n. 375, 17 jul. 2004.

REVISTA ABRIL (São Paulo) (Org.). **Dispositivos móveis alavancam acesso à internet no Brasil.** Disponível em: http://exame.abril.com.br/tecnologia/noticias/dispositivos-moveis-alavancam-acesso-a-internet-no-brasil>. Acesso em: 02 mar. 2012.

ROBERT, Jacques & DUFFAR, Jean. **Droits de l'Homme et Libertés Fondamentales**. 7.ª ed. Paris: Éditions Montchrestien, 1999.

ROSENOER, Jonathan. ***Cyberlaw**: The Law of the Internet.* New York: Springer, 1996.

SAMPAIO Nelson de Souza. **O Processo Legislativo**. 2.ed.rev. e atual. Por UadiLammêgo Bulos. Belo Horizonte: Del Rey, 1996.

SENADO FEDERAL. **Dilma sanciona Lei dos Crimes Cibernéticos.** Disponível em: <http://www12.senado.gov.br/noticias/materias/2012/12/03/presidente-dilma-sanciona-lei-dos-crimes-ciberneticos>. Acesso em: 06 ago. 2013.

SENADO FEDERAL. Disponível em: <http://www.senado.gov.br/>. Acesso em: 05 ago. 2013.

SENADO FEDERAL. **Senado aprova projeto que define crimes cibernéticos.** Disponível em: <http://www12.senado.gov.br/noticias/materias/2012/10/31/senado-aprova-projeto-que-define-crimes-ciberneticos>. Acesso em: 06 ago. 2013

SILVA José Afonso da. **Comentário contextual à Constituição**. São Paulo: Malheiros Editores, 2005. p. 437

SILVA, Tadeu Antonio Dix. **Liberdade de expressão e direito penal no Estado democrático de direito**. São Paulo: IBCCRIM, 2000.

SOUZA, Ailton Benedito de. **Promoção Ministerial nos Autos n.1704-39-2012.4.01.3500. Ministério Público** Federal. Procuradoria da República em Goiás. Disponível em: <http://www.prgo.mpf.gov.br/images/stories/ascom/promo_1288.pdf>. Acesso em: 03jul. 2013.

Supremo Tribunal de Justiça, 20 de Outubro de 2010, Relator. Pires da Graça acórdão de n.º 78/07.6JAFAR.E2.S1

TAKAHASHI, Tadao. **Sociedade da Informação no Brasil**. Livro Verde. Brasília, Ministério da Ciência e Tecnologia, 2000

TAVARES, André Ramos. **Curso de Direito Constitucional.** São Paulo. Ed. 6ª. Saraiva, 2008. p. 1279

TAVARES, André Ramos. **Curso de Direito Constitucional**. São Paulo: Saraiva, 2010

TEMER, Michel. **Internet: aspectos legislativos**. In: DE LUCCA, Newton; SIMÃO FILHO, Adalbertov(Coord). **Direito & internet:** aspectos jurídicos relevantes. Bauru: EDIPRO, 2001. p. 494.

TINOCO, Nábila Jensigne de Abreu. **Liberdade de informação e expressão na Internet: Mídias sociais e blitze da operação lei seca. Rio de Janeiro 2012:** -. -. Disponível em: <http://www.emerj.tjrj.jus.br/paginas/trabalhos_conclusao/1semestre2012/trabalhos_12012/nabilajensignetinoco.pdf>. Acesso em: 02 set. 2013.

TOFFOLI, José Antonio Dias. **Íntegra do voto do ministro Dias Toffoli na ação que suspendeu dispositivos da Lei Eleitor...** Disponível em: <http://jurisway.jusbrasil.com.br/noticias/2360841/integra-do-voto-do-ministro-dias-toffoli-na-acao-que-suspendeu-dispositivos-da-lei-eleitor>. Acesso em: 02 set. 2013.

TOURINHO, Daniela de Oliveira. Provimento de acesso de alta velocidade na internet. **Revista do Advogado,** São Paulo, v. 23, 2003.

VIANNA, Túlio Lima. **Cibernética Penal**. Boletim do instituto de ciências penais, Belo Horizonte, 2001.

ANEXO(S)

ANEXO A – Marco Civil PL 2126/2011

PROJETO DE LEI

Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

O CONGRESSO NACIONAL decreta:

CAPÍTULO I

DISPOSIÇÕES PRELIMINARES

Art. 1º Esta Lei estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria.

Art. 2º A disciplina do uso da Internet no Brasil tem como fundamentos:

I - o reconhecimento da escala mundial da rede;
II - os direitos humanos e o exercício da cidadania em meios digitais;
III - a pluralidade e a diversidade;
IV - a abertura e a colaboração; e
V - a livre iniciativa, a livre concorrência e a defesa do consumidor.

Art. 3º A disciplina do uso da Internet no Brasil tem os seguintes princípios:

I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição;
II - proteção da privacidade;
III - proteção aos dados pessoais, na forma da lei;
IV - preservação e garantia da neutralidade da rede, conforme regulamentação;
V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;

VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei; e

VII - preservação da natureza participativa da rede.

Parágrafo único. Os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria, ou nos tratados internacionais em que a República Federativa do Brasil seja parte.

Art. 4º A disciplina do uso da Internet no Brasil tem os seguintes objetivos:

I - promover o direito de acesso à Internet a todos os cidadãos;

II - promover o acesso à informação, ao conhecimento e à participação na vida cultural e na condução dos assuntos públicos;

III- promover a inovação e fomentar a ampla difusão de novas tecnologias e modelos de uso e acesso; e

IV - promover a adesão a padrões tecnológicos abertos que permitam a comunicação, a acessibilidade e a interoperabilidade entre aplicações e bases de dados.

Art. 5º Para os efeitos desta Lei, considera-se:

I - Internet - o sistema constituído de conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes;

II - terminal - computador ou qualquer dispositivo que se conecte à Internet;

III - administrador de sistema autônomo - pessoa física ou jurídica que administra blocos de endereço Internet Protocol - IP específicos e o respectivo sistema autônomo de roteamento, devidamente cadastrada no ente nacional responsável pelo registro e distribuição de endereços IP geograficamente referentes ao País;

IV - endereço IP - código atribuído a um terminal de uma rede para permitir sua identificação, definido segundo parâmetros internacionais;

V - conexão à Internet - habilitação de um terminal para envio e recebimento de pacotes de dados pela Internet, mediante a atribuição ou autenticação de um endereço IP;

VI - registro de conexão - conjunto de informações referentes à data e hora de início e término de uma conexão à Internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados;

VII - aplicações de Internet - conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à Internet; e

VIII - registros de acesso a aplicações de Internet - conjunto de informações referentes à data e hora de uso de uma determinada aplicação de Internet a partir de um determinado endereço IP.

Art. 6º Na 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.

CAPÍTULO II

DOS DIREITOS E GARANTIAS DOS USUÁRIOS

Art. 7º O acesso à Internet é essencial ao exercício da cidadania e ao usuário são assegurados os seguintes direitos:

I - à inviolabilidade e ao sigilo de suas comunicações pela Internet, salvo por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;

II - à não suspensão da conexão à Internet, salvo por débito diretamente decorrente de sua utilização;

III - à manutenção da qualidade contratada da conexão à Internet, observado o disposto no art. 9º;

IV - a informações claras e completas constantes dos contratos de prestação de serviços, com previsão expressa sobre o regime de proteção aos seus dados pessoais, aos registros de conexão e aos registros de acesso a aplicações de Internet, bem como sobre práticas de gerenciamento da rede que possam afetar a qualidade dos serviços oferecidos; e

V - ao não fornecimento a terceiros de seus registros de conexão e de acesso a aplicações de Internet, salvo mediante consentimento ou nas hipóteses previstas em lei.

Art. 8º A garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à Internet.

CAPÍTULO III

DA PROVISÃO DE CONEXÃO E DE APLICAÇÕES DE INTERNET

Seção I

Do Tráfego de Dados

Art. 9º O responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicativo, sendo vedada qualquer discriminação ou degradação do tráfego que não decorra de requisitos técnicos necessários à prestação adequada dos serviços, conforme regulamentação.

Parágrafo único. Na provisão de conexão à Internet, onerosa ou gratuita, é vedado monitorar, filtrar, analisar ou fiscalizar o conteúdo dos pacotes de dados, ressalvadas as hipóteses admitidas em lei.

Seção II

Da Guarda de Registros

Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de Internet de que trata esta Lei devem atender à preservação da intimidade, vida privada, honra e imagem das partes direta ou indiretamente envolvidas.

§ 1º O provedor responsável pela guarda somente será obrigado a disponibilizar as informações que permitam a identificação do usuário mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo.

§ 2° As medidas e procedimentos de segurança e sigilo devem ser informados pelo responsável pela provisão de serviços de conexão de forma clara e atender a padrões definidos em regulamento.

§ 3º A violação do dever de sigilo previsto no caput sujeita o infrator às sanções cíveis, criminais e administrativas previstas em lei.

Subseção I

Da Guarda de Registros de Conexão

Art. 11. Na provisão de conexão à Internet, cabe ao administrador do sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de um ano, nos termos do regulamento.

§ 1º A responsabilidade pela manutenção dos registros de conexão não poderá ser transferida a terceiros.

§ 2º A autoridade policial ou administrativa poderá requerer cautelarmente a guarda de registros de conexão por prazo superior ao previsto no caput.

§ 3º Na hipótese do § 2º, a autoridade requerente terá o prazo de sessenta dias, contados a partir do requerimento, para ingressar com o pedido de autorização judicial de acesso aos registros previstos no caput.

§ 4º O provedor responsável pela guarda dos registros deverá manter sigilo em relação ao requerimento previsto no § 2º, que perderá sua eficácia caso o pedido de autorização judicial seja indeferido ou não tenha sido impetrado no prazo previsto no § 3º.

Subseção II

Da Guarda de Registros de Acesso a Aplicações de Internet

Art. 12. Na provisão de conexão, onerosa ou gratuita, é vedado guardar os registros de acesso a aplicações de Internet.

Art. 13. Na provisão de aplicações de Internet é facultado guardar os registros de acesso dos usuários, respeitado o disposto no art. 7º.

§ 1º A opção por não guardar os registros de acesso a aplicações de Internet não implica responsabilidade sobre danos decorrentes do uso desses serviços por terceiros.

§ 2º Ordem judicial poderá obrigar, por tempo certo, a guarda de registros de acesso a aplicações de Internet, desde que se tratem de registros relativos a fatos específicos em período determinado, ficando o fornecimento das informações submetido ao disposto na Seção IV deste Capítulo.

§ 3º Observado o disposto no §2º, a autoridade policial ou administrativa poderá requerer cautelarmente a guarda dos registros de aplicações de Internet, observados o procedimento e os prazos previstos nos §§ 3º e 4º do art. 11.

Seção III

Da Responsabilidade por Danos Decorrentes de Conteúdo Gerado por Terceiros

Art. 14. O provedor de conexão à Internet não será responsabilizado por danos decorrentes de conteúdo gerado por terceiros.

Art. 15. Salvo disposição legal em contrário, o provedor de aplicações de Internet somente poderá ser responsabilizado por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente.

Parágrafo único. A ordem judicial de que trata o caput deverá conter, sob pena de nulidade, identificação clara e específica do conteúdo apontado como infringente, que permita a localização inequívoca do material.

Art. 16. Sempre que tiver informações de contato do usuário diretamente responsável pelo conteúdo a que se refere o art. 15, caberá ao provedor de aplicações de Internet informar-lhe sobre o cumprimento da ordem judicial.

Seção IV

Da Requisição Judicial de Registros

Art. 17. A parte interessada poderá, com o propósito de formar conjunto probatório em processo judicial cível ou penal, em caráter incidental ou autônomo, requerer ao juiz que ordene ao responsável pela guarda o fornecimento de registros de conexão ou de registros de acesso a aplicações de Internet.

Parágrafo único. Sem prejuízo dos demais requisitos legais, o requerimento deverá conter, sob pena de inadmissibilidade:

I - fundados indícios da ocorrência do ilícito;

II - justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória; e

III - período ao qual se referem os registros.

Art. 18. Cabe ao juiz tomar as providências necessárias à garantia do sigilo das informações recebidas e à preservação da intimidade, vida privada, honra e imagem do usuário, podendo determinar segredo de justiça, inclusive quanto aos pedidos de guarda de registro.

CAPÍTULO IV

DA ATUAÇÃO DO PODER PÚBLICO

Art. 19. Constituem diretrizes para a atuação da União, dos Estados, do Distrito Federal e dos Municípios no desenvolvimento da Internet no Brasil:

I - estabelecimento de mecanismos de governança transparentes, colaborativos e democráticos, com a participação dos vários setores da sociedade;

II - promoção da racionalização e da interoperabilidade tecnológica dos serviços de governo eletrônico, entre os diferentes Poderes e níveis da federação, para permitir o intercâmbio de informações e a celeridade de procedimentos;

III - promoção da interoperabilidade entre sistemas e terminais diversos, inclusive entre os diferentes níveis federativos e diversos setores da sociedade;

IV - adoção preferencial de tecnologias, padrões e formatos abertos e livres;

V - publicidade e disseminação de dados e informações públicos, de forma aberta e estruturada;

VI - otimização da infraestrutura das redes, promovendo a qualidade técnica, a inovação e a disseminação das aplicações de Internet, sem prejuízo à abertura, à neutralidade e à natureza participativa;

VII - desenvolvimento de ações e programas de capacitação para uso da Internet;

VIII - promoção da cultura e da cidadania; e

IX - prestação de serviços públicos de atendimento ao cidadão de forma integrada, eficiente, simplificada e por múltiplos canais de acesso.

Art. 20. Os sítios e portais de Internet de entes do Poder Público devem buscar:

I - compatibilidade dos serviços de governo eletrônico com diversos terminais, sistemas operacionais e aplicativos para seu acesso;

II - acessibilidade a todos os interessados, independentemente de suas capacidades físico-motoras, perceptivas, culturais e sociais, resguardados os aspectos de sigilo e restrições administrativas e legais;

III - compatibilidade tanto com a leitura humana quanto com o tratamento automatizado das informações;

IV - facilidade de uso dos serviços de governo eletrônico; e

V - fortalecimento da participação social nas políticas públicas.

Art. 21. O cumprimento do dever constitucional do Estado na prestação da educação, em todos os níveis de ensino, inclui a capacitação, integrada a outras práticas educacionais, para o uso seguro, consciente e responsável da Internet como ferramenta para o exercício da cidadania, a promoção de cultura e o desenvolvimento tecnológico.

Art. 22. As iniciativas públicas de fomento à cultura digital e de promoção da Internet como ferramenta social devem:

I - promover a inclusão digital;

II - buscar reduzir as desigualdades, sobretudo entre as diferentes regiões do País, no acesso às tecnologias da informação e comunicação e no seu uso; e

III - fomentar a produção e circulação de conteúdo nacional.

Art. 23. O Estado deve, periodicamente, formular e fomentar estudos, bem como fixar metas, estratégias, planos e cronogramas referentes ao uso e desenvolvimento da Internet no País.

CAPÍTULO V

DISPOSIÇÕES FINAIS

Art. 24. A defesa dos interesses e direitos estabelecidos nesta Lei poderá ser exercida em juízo, individual ou coletivamente, na forma da lei.

Art. 25. Esta Lei entra em vigor sessenta dias após a data de sua publicação.

Brasília,