‘’’’’

**MICHELE MARESTONE DOS SANTOS**

# CRIMES VIRTUAIS: INEFICIÊNCIA DA LEGISLAÇÃO

Assis

2014

**Avenida Getúlio Vargas, 1200 - Vila Nova Santana - Assis - SP - 19807-634 Fone/Fax: (18) 3302-1055 – homepage: www.fema.edu.br**

**MICHELE MARESTONE DOS SANTOS**

# CRIMES VIRTUAIS: INEFICIÊNCIA DA LEGISLAÇÃO

Trabalho de Conclusão ao Curso apresentado ao Instituto Municipal de Ensino Superior de Assis – IMESA, como requisito do Curso de Graduação em Direito.

Orientanda: Michele Marestone dos Santos

Orientador: Luiz Antonio Ramalho Zanoti

Assis

2014

# CRIMES VIRTUAIS: INEFICIÊNCIA DA LEGISLAÇÃO

**MICHELE MARESTONE DOS SANTOS**

Trabalho de Conclusão ao Curso apresentado ao Instituto Municipal de Ensino Superior de Assis – IMESA, como requisito do Curso de Graduação em Direito, analisado pela seguinte comissão examinadora:

Orientador: Luiz Antonio Ramalho Zanoti

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Analisador:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Analisador:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Assis

2014

**AGRADECIMENTOS**

Meus sinceros e imensos agradecimentos aos professores do Curso de Direito, que foram indispensáveis para o meu desempenho e desenvolvimento em minha formação profissional, agradeço a Deus que é a base de todas as minhas vitórias e ao meu professor orientador Luiz Antonio Ramalho Zanoti pela atenção e comprometimento realizados ao longo deste trabalho.

Muito obrigada a todos.

As leis mantém seu crédito não porque são justas, e sim porque são leis.

(Montaigne)

# RESUMO

Este trabalho tem por objetivo abordar um problema que vem crescendo e fazendo parte cada vez mais da sociedade, fazendo parte da vida civil de muitos. Com o avanço tecnológico os meios para conseguir acompanhá-los foram ficando devassados, a partir deste ponto muito vem se discutindo para que se faça uma legislação especifica em prol destes atos. Esta demonstrado ao decorrer deste trabalho a evolução tecnológica de redes virtuais e a ineficiência da legislação, observando ainda a comparação feita em outros países e as propostas de lei que estão em andamento no Brasil com o foco de punir e assegurar a segurança da sociedade em relação a esse imenso meio virtual.

**Palavras-chave:** Código Penal; crimes virtuais; legislação específica.

**ABSTRACT**

This research aims to address the thesis defended by liberal currents on the need to make labor rights provided for in the legislation in force. There are those who support this model, through which the workers would suffer some losses on collection of rights that have been accumulated over the past centuries, under the argument that these openings will result in a greater supply of new jobs, with the consequent reduction in levels of unemployment, because employers will have greater ability to invest their profits in their own economic activity. On the other hand, another current that defends the thesis that the labor rights, won with huge fights over so many years, cannot simply be lost, without a concrete contribution of the entrepreneur.

[http://www.microsofttranslator.com/static/img/tooltip_logo.gif?152459](http://www.microsofttranslator.com/)http://www.microsofttranslator.com/static/img/tooltip_close.gif?152459

Original

Há os que defendem esse modelo, por meio do qual os trabalhadores sofrerão algumas perdas no conjunto de direitos que vêm sendo acumulados ao longo dos últimos séculos, sob o argumento de que essas aberturas resultarão numa maior oferta de novos postos de trabalho, com a consequente redução dos níveis de desemprego, pois os empresários terão maior possibilidade de investir seus lucros maiores na sua própria atividade econômica.

**Keywords:** relaxatio; human dignity; labor relations.

[http://www.microsofttranslator.com/static/img/tooltip_logo.gif?152459](http://www.microsofttranslator.com/)http://www.microsofttranslator.com/static/img/tooltip_close.gif?152459

Original

flexibilização, dignidade da pessoa humana, relações trabalhistas.

**SUMÁRIO**

# INTRODUÇÃO............................................................................................................

09

10

10

11

12

19

19

27

27

32

35

37

**CAPÍTULO 1 – INTERNET, SUA HISTÓRIA, COMO O**

**CRIMINOSO A USA E AS LEIS PARA PUNI-LOS..................................................**

**1. AVANÇO DA INTERNET....................................................................................**

1.1 Análise inicial......................................................................................................

* 1. Internet e sua origem..........................................................................................
  2. A Realidade Virtual.............................................................................................

1.4 A Internet no Direito Penal e sua Evolução..........................................................

**CAPÍTULO 2 – LEI DA INTERNET EM OUTROS PAISES......................................**

2.1 Leis internacionais................................................................................................

**CAPÍTULO 3. LEIS EM CURSO NO BRASIL.........................................................**

**4. CONSIDERAÇÕES FINAIS.................................................................................**

### 5. REFERÊNCIAS BIBLIOGRÁFICAS E ELETRÔNICAS.....................................

**INTRODUÇÃO**

Neste trabalho de conclusão de curso, abordaremos um grande problema de nossa realidade, discutiremos da ação criminosa virtual, onde, por intermédio da internet, se realiza inúmeras práticas de crimes e a busca da punição, pela legislação vigente.

É notório o crescimento dessa forma de crime, a legislação não esta acompanhando essa evolução, pois a mesma, criada em meados de 1960, não tinha discernimento do que apareceria pela frente, mas deveria ter introduzido mecanismos que auxiliassem nessa evolução pois *“Si vis pacem para bellum”* (se queres a paz, prepara-te para a guerra).

Trataremos também das leis que estão sendo aplicadas no Brasil e em outros países, do desenvolvimento do meio virtual e sucetivamente do Código Penal, e a incapacidade da legislação penal em relação e esses crimes.

Citaremos os Projetos que estão em andamento no Brasil, e suas ideias de leis para que se tenham efeitos contra o alastramento desses crimes virtuais para que não se perca o controle futuramente.

Nosso objetivo é de lhes mostrar como esses crimes são constantes, como as leis estão descompassadas e como esses delitos podem ser extintos de vez.

**CAPÍTULO 1 – INTERNET, SUA HISTÓRIA, COMO O CRIMINOSO A USA E AS LEIS PARA PUNI-LOS**

Abordaremos a evolução da Internet, do Código Penal e de alguns dispositivos da lei que já existem e as que estão em andamento, no que dizem e suas ações em descrição ao devido assunto.

* 1. **Conceitos Iniciais.**

Os crimes virtuais ainda são poucos citados pelos estudiosos, não sendo um tópico onde se preocupam muito com a punição, autores discorrem sobre esse assunto deixando muitas lacunas.

Outros autores trazem dicas para saber como balancear essas inovações da internet com o lado jurídico, concretizando que: esses problemas só serão resolvidos por meio de informação e contínuo intercâmbio.

Veja o pensamento do autor Correia:

“A tecnologia digital é uma realidade, e justamente por isso estamos diante da criação de lacunas objetivas, as quais o direito tem o dever de estudar, entender e, se necessário preencher. Com a crescente popularização da Grande Rede, evidenciamos a criação de novos conceitos sobre tradicionais valores, tais como a liberdade, a privacidade e o surgimento dos ‘crimes’ digitais” (CORREIA, 2000, p. 03).

Essa é a afirmação que este é um tema que deve ser estudado e dedicado ao direito penal do Brasil, devendo ser ativo concomitantemente tendo desenvolvimento tecnológico a cerca do tema.

Existem meios para identificar os indivíduos que praticam tais crimes virtuais, pois eles não conhecem o sistema, assim fica fácil aplicar-lhes uma sanção, pois o acesso para investigação é mais facilitado, já para os que sabem e conhecem mais sobre a tecnologia acaba tornando mais dificultoso penalizá-los, sendo que até mesmo os estudiosos esporadicamente entende do funcionamento de toda essa estrutura tecnológica.

Deste modo, veremos como funciona esse mundo digital para entendermos mais a cerca de como esses crimes são praticados e o seu *“Dano ex delicto”* (Dano causado pelo delito).

**1.2 A Origem da Internet**

Com o advento dos computadores, surgiu uma imensa rede de comunicação que trouxe consigo aspectos bons para a sociedade, informações imediatas, comunicação em tempo real entre comunidades do mundo inteiro, porém trazendo também aspectos negativos usando-se desta tecnologia para ações criminosas;

A essa comunicação entre os computadores, se deu o nome de *internet*, ela teve origem nos Estados Unidos, no ano de 1969, criada pelo Departamento de Defesa dos Estados Unidos da América, que se preocupava com um ataque nuclear por parte da União Soviética. Sendo criada então para garantir a segurança nas comunicações.

Criou-se então uma rede, dividida em alguns locais, postas em lugares estratégicos, denominados LAN, sendo conectadas em redes de telecomunicação geográficas, denominadas WAN.

Foi desenvolvido por Networking Group, em meados de 1970, um protocolo host-t0-host, que gerava maior aplicabilidade de funcionamento.

Em 1972, com o desenvolvimento da Arpanet em uma Conferência Internacional entre computadores, lançaram o correio eletrônico, mais conhecido entre nós por e-mail, que tinha características de rapidez entre os meio de comunicação, porém como já esperado, o e-mail desviando-se de seu objetivo principal e destinou-se a praticas criminosas, a mais praticada é a ofensa à honra das pessoas.

Mesmo sendo um imenso avanço na tecnologia para aquela época, foi se tornando ultrapassado esse protocolo, surgindo-se então o TCP/IP (Transfer Control Protocol / Internet Protocol) que transmitia com mais clareza os assuntos e dados de um computador de origem ao computador que receberia tais dados.

Em 1973 a internet expandiu para outros networks. Isso aconteceu a partir da criação do Protocolo de Controle de Transmissão, que é o Protocolo da Internet.

Esse é um código que autoriza networks diferentes, a terem acesso a Rede, se comunicando entre sí até então.

Em 1989, documentos, como os que transmitem textos, imagens e hipertextos, tiveram origem em Genebra, chamados de Word Wide Web, popularmente conhecido como WWW ou Web, através de tais códigos, a internet se expandiu no mundo todo.

Conforme Cairncross e Silva (p. 123/124):

“A WWW (World Wide Web) é o serviço oferecido pela internet permitindo a obtenção de acesso a informações grafadas em hipertextos. Trouxe novas formas de operação para internet: levou a multimídia até a rede, uma vez que passou a possibilitar a apresentação de imagens coloridas e em movimento, música, além de dados e textos; introduziu o hipertexto que possibilitou ao usuário passar de uma palavra ou frase assinalada na tela para informação sobre ela localizada em um computador diferente situado em outro local, bem como tornou possível a abertura de outros arquivos clicando na palavra ou figura” (SILVA, 2003, p. 23).

No ano de 2003, já passavam de 40 mil redes em todo mundo, observando esse número, surgiu a necessidade de se saber mais dessa tecnologia da informação, uma vez que vem influenciando no dia-a-dia dos cidadãos, que exige uma proteção do nosso ordenamento jurídico, pensando na “De lege ferenda” (Da lei a ser criada), para não nos tornarmos ‘escravos’ dessas máquinas, sem uma lei de proteção dos nossos direitos.

1.3 A realidade virtual**.**

Na data atual, as informações instantâneas tornaram-se prioridade mundial, pois, é através dela que se desenvolve uma evolução tecnológica.

E é por causa dessa prioridade na comunicação que vem desenvolvendo a necessidade de transmissão de informações a distantes de forma cada vez mais rápida.

Primeiro ocorreu a comunicação pela fala, depois sinais, surgindo também a criação do telefone, mais precisamente em 1876 e por fim a criação de computadores em 1949, surgindo as trocas de informações imediatas.

Ocorre que, para um computador, informações não são apenas conhecimentos de fatos, mais sim, todo e qualquer dado, concludente por meio de um código digital.

Para termos uma maior compreensão dos crimes virtuais, faz-se necessário conhecer o funcionamento da internet, ferramenta utilizada para prática de muitos delitos.

A Internet é um SISTEMA ou REDE, de um conjunto de computadores ligados a satélite e cabos, que possuem certa linguagem e um endereço lógico, que indica assim a posição que tais computadores possuem na Rede. O computador que queira se conectar à internt possui esse endereço lógico, constituído por números denominados IP, que envia e recebe mensagens.

Para facilitar esse acesso, sem o usuário ter a necessidade de digitar diversos números (no caso o endereço lógico), cria-se o NOME DE DOMINIO, que é um endereço de nome de pessoa física ou jurídica que tem em sua composição o endereço de um IP, relativo a algum site.

Inellas escreve da seguinte forma:

“O *Nome de Domínio* é o *endereço*, o nome de pessoa física ou jurídica, tendo, embutido, o endereço IP. Dessa forma, torno-se mais fácil o acesso à *Internet.* O *Nome de Domínio* é assim constituído: *WWW* (Rede Mundial de Computadores); um nome, que identifica o usuário; .com (identifica a destinação do usuário); br (identifica o país). As letras finais, antes da identificação do País, podem ser diferentes , dependendo dos gestores dos *Sites.* Por exemplo: .gov, .org, .net” (INELLAS, 2009, p.05).

A troca de dados por meio destes computadores, é feita através de uma linguagem própria, composta por dois caracteres: zero e o um, ou seja, ausência de sinal e sinal. Eles são marcados conforme a estado que se encontra, podendo estar ligado ou desligado.

Então, os computadores comunicam-se através de um Protocolo IP. Tal protocolo é utilizado de duas formas. A primeira forma delas divide a informação em pequenos pacotes, chamados de packets, que envia mensagens ao computador de destino, cada informação divida (pacote), pode destinar-se a qualquer computador, mesmo que em países distintos.

A segunda forma, permite que o protocolo manipule o endereçamento dos computadores, consentindo que cada um procure e se comunique com o outro. Os bits são utilizados nesta forma, cada computador possui em seu endereçamento, trinta e dois bits, traduzindo quatro algarismos e denominam-se Internet Protocol (IP).

Por meio desses e de outros mecanismos, nasce a possibilidade de apurar um delito praticado via internet, tornando-a mais acessível. O Protocolo (TCP/IP), também funciona na troca de informações na Rede, a saber; o Internet ControlMessageProtocol (ICMP), o Simple Mail TransferProtocol (SMTP) e o AddressResolutionProtocol (ARP).

Tais mecanismos tem sua própria função. O ARP mapeia os endereços da internet, tornando-os endereços físicos, identificando cada pacote.

O ICMP controla mensagens trocadas entre um computador e outro, durante transferência de dados. Já o SMTP permite, através do Protocolo que mensagens eletrônicas sejam enviadas, ou seja, ele autoriza o envio de e-mail.

Existe hoje duas formas de acessar a Internet. A primeira é o SERVIDOR, que ‘serve’ a rede com serviços como a internet, por exemplo. A segunda forma é caracterizada ‘cliente’ que acessa os serviços disponíveis pelo servidor.

Inellas, tomando como exemplo o correio eletrônico:

“Quando o usuário redige uma mensagem na tela de seu computador e o envia pela *Internet,* ele pensa que utilizou um Programa de correio eletrônico para redigir a mensagem, endereçá-la ao destinatário e enviá-la. Ledo engano. Em verdade, o que ocorre é o seguinte: o Programa de correio eletrônico transmite a mensagem para o Servidor do destinatário e este, por sua vez, envia a mensagem para o computador de seu cliente/usuário. Em verdade, todas as comunicações entre computadores, através da *Internet,* são feitas dessa forma, indiretamente, por intermédio dos Servidores ou Provedoras, dependendo, dessarte, tanto do Servidor do usuário que busca serviços ou informações, quanto do usuário que oferece serviços” (INELLAS, 2009, p. 08).

Em síntese, o funcionamento da internet é basicamente desse modo estruturado. Conhecendo o modo como são transmitidas e enviadas as mensagens pela internet, os juristas podem apurar melhor os crimes, aumentando a possibilidade de identificar o meliante, diminuindo o fato de *“neminem laedere”* (não lesar a ninguém), que não seja culpado.

Algumas técnicas também são utilizadas para que criminosos invadam a Rede e cometam os crimes. Chamada de Sniffer. Por meio dela, os criminosos podem ver lugares abertos nos hosts, tendo assim acesso a dados e informações, eles localizam um computador especifico na Internet, possibilitando dessa forma a invasão.

Outra técnica conhecida é a do cracking, que significa quebrar. Ela é utilizada para destruir um sistema de segurança que descobre a chave de acesso (uma senha por exemplo).

Na mesma reta de raciocínio nos ensina Inellas (2009, p. 09), que dispõe que “o vírus é um software que visa à destruição ou alteração de dados na máquina infectada, bem como sua proliferação, infectando outros computadores”.

Outro software é o denominado Trojan Horse (Cavalo de Tróia), que possibilita o controle total do Sistema infectado,invade a privacidade de terceiros, abrindo arquivos e até mesmo os apagando.

Existe hoje dois tipos de Trojan Horse – backdoor (que abre “portas” para a invasão) e o Keylogger (registra tudo que é digitado).

O criminoso virtual é sobretudo pessoa jovem, com amplo conhecimento em TI e sem antecedentes criminais.

Dentro deste parâmetro o escritor Cruz escreveu:

“Os cibernéticos são jovens e sem antecedentes criminais. Eles, porém, geram milhões de despesas e prejuízos às empresas e usuários comuns na internet. A mente criminosa, o programador, é a pessoa mais difícil de ser pega. Segundo o delegado federal, esse criminoso nunca está vinculado a uma quadrilha, porque ele cria o vírus e depois comercializa para terceiros. São jovens e que trabalham na área de TI de alguma empresa ou mesmo em bancos.” (CRUZ, 2009) 2 (http://www.ipnews.com.br/telefoniaip/index)

Dentro do mundo virtual os criminosos que tem maior destaque são os chamados hackersque, pois invadem os computadores, adquirindo os mais diversos tipos de informações, alterando sites, invadindo sistemas, descobrindo senhas de cartões de crédito, banco, levando a vitimas à prejuízo e a constrangimentos imensos.

Sobre esse assunto, Inellas discorreu:

“O *hacker* é considerado o intruso do mundo virtual. A invasão dos Sistemas alheios, pelo *hacker,* geralmente deve-se a um mero desejo de demonstração de sua perícia em informática e à curiosidade. Normalmente, não possui um fim ilícito específico. Todavia, sua conduta, por si só, já é considerada ilícita. Seu conhecimento lhes permite avaliar as falhas de um Sistema e violá-lo. Dessa forma, poderá comandar computadores alheios à distância, invadir Sistemas de empresas e de Governos, alterar *Sites* e ter acesso aos mais diversos tipos de informação. Da mesma forma, com a ideia de socialização do conhecimento, há sites que ensinam como violar os Códigos de Segurança da maioria dos *softwares* disponíveis no mercado. Em verdade, a internet não é segura.” (INELLAS, 2009, p. 21/22).

O judiciário encontra grande dificuldade em penalizar esses criminosos, que por terem conhecimento técnico nunca ou quase nunca deixam vestígios. A Constituição Federal defende o direito das vitimas, que em seu artigo 5°, inciso X, dispõe serem invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, e em seu inciso XXXV, dispõe que a lei não excluirá da apreciação do Poder Judiciário, lesão ou ameaça de direito.

Existe a lei e sua sanção, o que falta é a maneira de descobrir a autoria dos crimes e localizar o individuo, tendo em vista que os crimes praticados pela internet só conseguem ser descobertos quando há indícios de qual computador veio essa pratica delituosa.

Diante de uma análise do sistema informático e de seus agentes praticantes de crimes, nota-se que o funcionamento da internet deve ser de conhecimento dos doutores em direito, para que a justiça esteja presente na era digital, condenando os criminosos desse crime e reduzindo a criminalidade virtual, não só na nossa realidade, mas com a ótica voltada *“ad futurum”,* (para o futuro), para não incorrer nas mesmas dificuldades que enfrentamos hoje.

**1.4 A internet no Direito Penal e sua evolução**

O Direito Penal foi criado com o sentido de estabelecer regras para proteger bens como a saúde, vida, liberdade, propriedade e tantos outros, a fim de visar a segurança social, ele deve se adequar a nosso realidade para não desvirtuar de sua origem.

Como sabemos, antes das leis postas, a justiça era feita pelas próprias mãos, usando-se a arbitragem como um meio de defesa.

No advento do descobrimento do Brasil, esses meios de defesa utilizados pelos povos nativos foram pouco a pouco banidas, isso graças à colonização portuguesa.

Depois de diversas tentativas de se outorgar um Código Penal, em 1830, sancionou-se o primeiro Código Criminal do Império, que tinha como conteúdo um “rascunho” do que seria hoje a individualização da pena, com atenuantes e agravantes que eram de grande importância para aquela época.

No Código Criminal do Império era permitido até mesmo a pena de morte, servindo para colocar medo nos escravos para que os mesmos não praticassem nenhuma conduta delituosa.

O Código foi criado e embasado em razão dos acontecimentos da época, logo ele passou por reformas, pois em suas disposições havia diversos problemas de como ser aplicada essa lei penal.

Acontecendo a proclamação da republica e visando as grandes mudanças politicas que passava naquele momento o Brasil, em meados de 1889, Joaquim Nabuco, apresenta a Câmara dos Deputados, um novo projeto de lei a ser estabelecida no país.

Esse projeto foi inspirado no Código Penal Suiço, em 1884, foi retirados vários artigos do Código vigente, onde todos eles se referiam a escravidão, já que não teria mais porque tê-los já que a abolição dos escravos havia acorrido no ano de 1888, com a Lei Áurea, do mesmo modo que, modificou o nome da legislação penal que de Código Criminal que passou a atender como Código Penal, dessa forma, depois de algumas alterações o novo Código foi aprovado e entrou em vigor em 11 de outubro de 1890 pelo Decreto n° 847.

No entanto, antes de entrar em vigor, o Código Penal de 1890, passou novamente por reformas, como expõe Chaves e Sanchez:

“Antes mesmo de o novo Código entrar em vigor, o Governo baixou o Decreto nª. 774 de 20 de setembro de 1890, que extinguiu as galés, reduziu ao máximo de 30 nos as prisões perpétuas e estabeleceu que deveria computar-se na pena o período da prisão preventiva. O código Penal de 1890 não previa as medidas de segurança, que só seriam introduzidas no atual Código Penal Brasileiro de 1940.” (CHAVES e SANCHEZ, p. 12) 1 (<http://intertemas.unitoledo.br/revista/index.php/ETIC/article/viewFile/2238/2222>).

No século XX, diversas foram as tentativas de reforma do Código Penal de 1890, Alcântara Machado elaborou então um projeto que tinha como meta sanções mais eficientes que do Código vigente, e ao invés de alterar o mesmo, criou-se um novo Código Penal, que está em vigência até os dias atuais.

Em 1942 foi criado nosso Código Penal, de 07/12/1940 com o Decreto-lei n° 2.848, inspirado nos Códigos italiano e suíço, aperfeiçoado as necessidades da década.

No entanto por ser um Código antigo, nosso código atual brasileiro já não está na forma da nossa sociedade atual.

Em um de seus princípios, o próprio Direito Penal defende que o tipo penal deve se ajustar as necessidades da sociedade.

Assim, nos mostra Greco sobre o Princípio da Adequação Social:

“O princípio da adequação social, concebido por Hans Welzel, possui dupla função. Uma delas é a de restringir a abrangência do tipo penal, limitando sua interpretação e dele excluindo as condutas consideradas socialmente adequadas e aceitas pela sociedade. A segunda função é dirigida ao legislador em duas vertentes. A primeira delas orienta o legislador quando da seleção das condutas que deseja proibir ou impor, com a finalidade de proteger os bens considerados mais importantes. A segunda vertente destina-se a fazer com que o legislador repense os tipos penais e retire do ordenamento jurídico a proteção sobre aqueles bens cujas condutas já se adaptaram perfeitamente à evolução da sociedade” (GRECO, 2010, p. 04).

À frente desse fato, constata-se que o Direito Penal esta em desacordo com os seus próprios princípios.

Não está utilizando o legislador dos princípios como um forma de reformar o Código Penal e adequar a realidade atual. Esses crimes praticados através da internet estão sendo cada vez mais frequentes, a legislação se torna inerte para resolve-los.

A criação de lei específica muito se discute hoje. Como nos ensina Inellas:

“A necessidade urgente de leis específicas, penais e processuais penais, com relação aos crimes praticados através da Internet, foi alertada pelo Desembargador Castro Meira, no Tribunal Regional da Quinta Região, durante o Congresso Internacional de Direito e Tecnologias da Informação” (INELLAS, 2009, p. 14).

Comprova-se portanto, que a urgência de criação de lei especifica, ou a reforma do Código Penal brasileiro, tem-se como medida de necessidade, para que, delitos desse tipo sejam combatidos e, que profissionais de direito se especializem cada vez mais para lidar com tais crimes.

**CAPÍTULO 2 – LEIS DA INTERNET EM OUTRO PAISES**

**2.1 Leis Internacionais.**

Para tratar sobre a legislação de outros países, vale mencionar os meios de segurança utilizados em nosso Pais para coibir tais crimes.

Com o alastrante uso da internet, que é cada vez mais utilizado no Brasil, criou-se o Comitê de Gestor da Internet do Brasil, que estabelece regras para o Registro do Nome de Domínio, pela Resolução n° 2.1998, que atribui à Fapesp (Fundação de Amparp à Pesquisa do Estado de São Paulo), a aplicação do Registro do Nome de Domínio, a distribuição dos Internet Protocols e a manutenção da Internet, isso*”* para fins de prova *“Ad probationem”.*

Assim, mesmo com mecanismos para que não haja fraudes ou para que a internet não fosse utilizada para práticas delituosas, os crimes da internet, denominados crimes da era digital ou até mesmo, cibercrimes, apareceram trazendo junto a insegurança aos usuários.

De acordo com Inellas:

“A *Internet* possui, hoje, mais de cem milhões de pessoas conectadas, em mais de cento e sessenta países. Em abril de 2000, o perfil do usuário da *Internet,* no Brasil, era o seguinte: 56% eram do sexo masculino e 44% eram do sexo feminino (*Revista Internet.br,* n. 47, abril 2000, p. 31). Alia-se a isso, a total falta de controle e entenderemos a razão da disseminação das atividades criminosas através de sua utilização.” (INELLAS, 2009, p. 13).

É fato confirmado que a maioria dos usuários da internet são do sexo masculino, o perfil do criminoso é justamente homem, uma vez que a maioria dos praticantes dos delitos tem amplo conhecimento em Tecnologia da Informação, frequentemente exercidas pelo sexo masculino.

Tinha como objetivo o Comitê de Gestor, estabelecer regras para a utilização e funcionamento da internet, e testaram a segurança que usuários poderiam utilizar, conectou-se anonimamente às provedoras gratuitas, utilizando nome e senha genérica e conseguiu invadir um computador da Rede de Provedoras Nacional.

Assim, o comitê conseguiu provar que as medidas de segurança até aquele momento eram válidas, uma vez que depois da simulação da invasão, mostrou que caso ocorresse tal situação, era possível identificar o usuário responsável pela invasão.

Porém, como as infrações penais são diversas, e com a rapidez na evolução da internet, os meios adotados pelo Comitê Gestor ficaram ineptos, atingindo os crimes virtuais, maior números de vítimas.

Com os meios disponíveis, a justiça tenta impedir tal prática. Nesse mesmo foco, o Delegado de Polícia de São Paulo, Capital, Titular do Setor de Crimes pela internet da Polícia de São Paulo, publicou um artigo que diz:

“A sociedade tem que ter em mente que o crime sempre, sempre está um passo a frente da polícia e o que define se essa polícia é eficiente, ou, não, é a distância desse passo, o chamado *gap* entre o crime e a polícia. Para diminuir este *gap,* a palavra de ordem é se preparar e antecipar, e no caso da investigação de crimes digitais, devemos maximizar a cooperação entre as polícias nacionais e internacionais, preparando e treinando policiais com novas técnicas de investigação, que devem agir rápido como a era digital exige.” (INELLAS. 2009. p. 14).

Observa-se que sem leis processuais penais e penais, o crime cometido pela internet, cada dia mais evolui, a medida que meios tecnológicos também vão evoluindo.

Para a investigação da autoria dos cibercrimes, em outros países, a quebra da gravação de dados ou de sigilo, é feita sem a autorização judicial, que sendo assim, apressa as diligências, aumentando assim as chances de conseguir punir o autor do crime.

Esses crimes estão distribuídos por todo o mundo. Expõe Inellas, em alguns históricos que diz respeito a prática de tais delitos:

“Em junho de 1998, na República Checa e na República Eslováquia, *hackers* invadem um banco, o *Site* local da UNICEF, uma revista dedicada à polícia e agência de notícias. Na Austrália, vários Servidores são invadidos e afetados por um ataque identificado como *NumberCrunch.* Devido a isso, os sistemas de todos os arquivos executáveis de Diretórios Windows 95, foram apagados, surgindo em seu lugar, outros arquivos com o nome *NumberCrunch´sReadme*”. (INELLAS. 2009. p. 15).

Observando os relatos acima, até mesmo sites considerados como a UNICEF, e arquivos do Windows se encontrão livres da invasão dos indivíduos que praticam esses crimes virtuais. Também, nota-se que esses crimes ocorreram em países diferentes. Como a China, México, Egito.

A julgar pelos crimes praticados na China, em outubro de 1998, a polícia chinesa executou a prisão de criminosos virtuais que haviam invadido o Sistema do Zhenjiang Industrial and Commercial Bank e subtraído a quantia de USS 117, 000 (cento e dezessete mil dólares americanos), através da invasão de um terminal de computadores e criação de contas falsas. Esses criminosos são especialistas em roubos a Bancos.

Os autores desse crime nesse país, são penalizados de acordo com a legislação Penal local. No entanto, tais ataques ainda continuam tendo o governo chinês criado uma base militar para investigação e autoria desses criminosos. Essa base, conta com o apoio de instituições privadas e também ações do governo, trabalho que demanda tempo, pela sua complexidade, uma vez que a internet é um meio de comunicação que funciona em tempo real em todos os lugares do mundo.

Crimes ocorridos na China, Espanha, África do Sul e Romênia, também merecem destaque, vejamos:

“No ano de 1999, no mês de janeiro, na China, um *hacker* usa o nome do próprio pai, para acessar o Serviço de Informação do Governo. Em seguida, modifica os códigos dos computadores e consegue controlar o gerenciador de contas de um sistema de telecomunicações. No mês de julho, na Espanha, um *hacker* invade os arquivos do Ministério do Interior, através de um Servidor, conectado á *Internet*. Em setembro, na África do Sul, o Sistema Oficial de Índices Econômicos é invadido. Suas estatísticas de preços de bens de consumo são alteradas e substituídas por textos obscenos. Em novembro, na Romênia, *hackres*violam o Sistema do Ministério das Finanças e modificam a cotação da moeda no País.” (INELLAS. 2009. p. 16).

Como se vê, sites oficiais são frequentementes invadidos, estando em risco dados que movem setoriais sociais, políticos e econômicos de um mundo em geral.

Esses crimes citados, já ocorriam na década de 90, onde os recursos tecnológicos não eram tamanhos como os atuais, que cada vez mais, cria meios mais eficazes e rápidos para a invasão de sistemas e de dados, tanto de particulares como de dados de órgãos importantes.

Ademais, além dos crimes virtuais serem de complexidade elevada, há outros problemas, como o de territorialidade. Nota-se que os crimes citados acontecem em países diferentes, fazendo da aplicabilidade da lei um problema a ser discutido.

Esses problemas de inicio, são a falta de legislação penal e processual penal especial. É aí que aparece o problema da territorialidade, trazendo consigo questões de tipicidade, competência e autoria, que tendo em base a internet, é de difícil análise, já que vários crimes são transnacionais.

Do mesmo modo, é de frizar que além da criação de uma lei especifica, também é necessário que tal legislação seja progressiva, andando de mãos dadas com as evoluções tecnológicas, assim como que seja reais as punições dos delitos praticados via internet, ativados em segundos e executados em toda parte do mundo.

Em razão desse assunto, o Senador Calheiros diz que: “Para crimes cometidos em ambientes virtuais, precisamos ter leis e penas reais com o intuito de coibir o delito.”

Os delitos praticados via internet em outros países, já estão sendo promulgados varias leis para coibição e punição dos crimes e desses criminosos.

Em razão disso o Parlamento espanhol aprovou uma lei que tem por objetivo regulamentar o comércio eletrônico, que, de acordo com Inellas: “(...) tornando as Provedoras de Acesso, mais responsáveis pelo conteúdo de suas páginas e exigindo que os Dados Cadastrais dos usuários fiquem armazenados por no mínimo, um ano”.

A lei, denominada de “Lei da Sociedade de Informação e do Comércio Eletrônico (*Ley de Servicios de La Sociedad de laInformación y Comercio Electrónico – LSSI)*”, que tem como objetivo implementar a mesma organização jurídica que é utilizada para negócios normais.

Depois de algumas alterações feitas pelo Senado espanhol, a medida imposta as Provedoras de Acesso de manter os dados cadastrais de seus usuários pelo período de um ano, gerou críticas, assim nos mostra Inellas:

“O Partido Popular, de centro-direita e que representa a situação, insistiu que a medida era imprescindível para as investigações criminais, enquanto o Partido Socialista, de oposição, insurgiu-se, afirmando ser, tal determinação, invasão de privacidade” (INELLAS. 2009. p. 152).

A apreciação feita pela oposição, foi feita por ser no caso partido político contrário ao que implantou a ideia, uma vez que em se tratando de crime que está longe do alcance de conhecimentos técnicos de juristas, um dos mínimos jeitos de coibir essa prática é se utilizar de meios de investigação.

Até mesmo a Inglaterra inovou a sua legislação, promulgando a Lei Terrorismo n. 2.000, que, segundo Inellas, “classifica como ciberterroristas, as pessoas que ‘põem vidas em risco através da manifestação de sistemas de computadores públicos’”.

O Departamento governamental da Inglaterra, chamado de *Home Office*, quefiscaliza a imigração e o crime, aclarou os objetivos da Lei Terrorismo n. 2.000, que tem por objetivo ampliar a definição de terrorista, aumentando seu conceito, junto com outros grupos como o IRA (*IrishRepublicanArmy*) e o *Hezbollhah,* os *hackers* e os políticos opositores.

Não muito diferente da Inglaterra, foi criada em Portugal a Lei nº. 109, de 17 de agosto de 1991, que cuida dos crimes virtuais. Essa lei fixou, dentre outras diversas coisas, a responsabilidade penal da pessoa jurídica, nos casos de crimes pela internet, e o furto, praticado pelo mesmo meio virtual.

Em descrição a responsabilidade penal da pessoa jurídica, está estabelecido em seu artigo 3º, que dispõe:

“As pessoas coletivas, sociedades e meras associações de fato são penalmente responsáveis pelos crimes previstos na lei, quando cometidos em seu nome e no interesse coletivo pelos seus órgãos ou representantes” (INELLAS. 2009. p. 152).

O furto, é tratado como o acesso não autorizado a Sistemas Informáticos, com o intuito de atingir benefício e vantagens indevidas. Em seu livro, Inellas cita alguns tipos de benefícios ou vantagens indevidas, como por exemplo: “podem ser dinheiro, cópias não autorizadas de Programas de computador (pirataria), segredos ou dados confidenciais”. Em relação a modalidade de conhecimento de segredos ou dados confidenciais, prevê-se para esse crime então agravante.

Um outro artigo que também merece atenção é o artigo 6º, da mesma lei, que dispõe sobre o crime de dano, e recebeu o nome de sabotagem informática. Essa sabotagem é definida como a modalidade de introduzir, alterar, suprimir ou destruir dados a até mesmo Programas Informáticos.

Um outro país, uma das maiores potências mundiais, também não escapou dos crimes praticados via internet.

Os Estados Unidos da América criou uma lei, em nível federal, mais conhecida por *Fraudand Related Activity in Connection with Computers,* Lei nº. 18 – U.S.C./1030. Essa lei foi criada para proteger computadores governamentais e os não-governamentais e particulares.

Tal Lei nº. 18 – U.S.C./1030 prevê, em sua alínea “a”, incisos I, II e IV, o crime de furto, como nos mostra Inellas:

“O inciso I cuida da proteção dos computadores dos órgãos públicos governamentais; o inciso II proíbe a cópia de informações, dos computadores das instituições financeiras e de departamentos ou agências não governamentais e o inciso IV cuida da proteção dos computadores particulares, proibindo a obtenção de qualquer tipo de vantagem econômica, através de invasão nos sistemas de computador”. (INELLAS. 2009. p. 153).

Se tratando ainda da Lei nº. 18 – U.S.C./1030 existe também os crimes de dano, que prevê três condutas, as quais definem Inellas:

“(...) na primeira, pune o agente que, dolosamente, transmite Programa, informação, código ou comando, tendo, como resultado, dano a computador protegido. A segunda ação pune o agente que acessar computadores protegidos e culposamente, causar dano. A terceira ação pune o agente que, intencionalmente, acessar computadores protegidos, sem autorização e causar dano. Nas três hipóteses, entende-se por dano, o vírus do computador”. (INELLAS. 2009. p. 153).

No caso da segunda conduta, a modalidade culpa, corresponde somente a negligência do agente. A terceira hipótese de conduta já pune o mesmo, dolosamente. Especificamente nesta lei criada para crimes virtuais, entende-se por dano, nos casos das condutas, o vírus de computador.

Além de toda estrutura dada a criação desta Lei, os Estados Unidos da América, falha em aplicar a legislação somente aos computadores protegidos, deixando os utilizados pelo usuário comum à mercê destes crimes.

Essas três hipóteses de ações que, cometidas, são punidas de forma rigorosa. Caso o criminoso pratique a primeira conduta, terá sua pena fixada em até 20 (vinte) anos de prisão e multa. Na segunda ação, por ser crime de modalidade culposa, a pena será de até 10 (dez) anos de prisão e multa. E na terceira conduta, a pena é de cinco anos de prisão e multa, contudo, a mesma somente será fixada caso o *hacker* conseguir invadir e, obter vantagens, como por exemplo, a econômica indevida no caso.

Em relação ainda ao dano, a Corte de Apelações norte-americana, interpretando o *Criminal DamageAct,* estabelece:

“*Where (...) the interference with the disc amounts to an impairment of the value or usefulness of the disc to the owner, then the necessary damage is established” (*INELLAS. 2009. p. 154).

Diz assim quis dizer Inellas:

“Onde (....) a interface com toda a quantidade de discos tem comprometimento dos seus valores ou utilidades de mídias proprietárias, então o dano é necessário".

Em razão a outras leis já existentes nos Estados Unidos da América, há as criadas no âmbito estadual, como o Código de Vírginia, que, em seu artigo 18.2.152.4, firma que seja punido aquele que fizer uso de computador sem autorização, com a intenção de causar dano a um indivíduo.

Foram criados leis nos Estados de Connecticut e Wiscosin. No estado de Wiscos in, a *Computer Lan,* que fixa como crime de dano informático, toda modificação ou destruição de dados, e sua pena pode cominar em 20 (vinte) anos de prisão e mais dez mil dólares de multa.

Interpretação feita pelo Estado de Nova Jersey, em seu Código, em seu artigo 2C:20-24, mostra como crime informático o uso não autorizado de um computador, chamado tal ação como furto de tempo do Sistema. O objetivo deste artigo é proteger crimes praticados por funcionários que utilizam para uso particular o computador da empresa.

Conforme Inellas, as condutas são:

“Na primeira, pune-se a pessoa que, intencionalmente e sem autorização, causar mau funcionamento ou interromper a operação de um Sistema informático. Na segunda conduta, pune-se a pessoa que alterar, danificar ou destruir dados arquivados em um computador. As penas previstas para estes crimes variam de um a cinco anos de prisão e multa, que varia de mil a cinco mil dólares”. (INELLAS. 2009. p. 155).

Observa-se que as legislações estaduais, protegem os computadores de uma forma geral, não apenas os computadores enquadrados como “computadores protegidos” no caso.

No Estado de Idaho, foi criado, em seu Título 18, Capítulo 22, artigo 1º, do Código Penal, o crime de furto, que conceitua como tal, segundo Inellas, “o acesso não autorizado aos computadores, individualmente e aos Sistemas e ás Redes de computadores, com o fim de subtrair dinheiro, propriedades ou serviços”.

Segundo a definição dado por Inellas, em seu artigo 2º, caracteriza como crime de dano: “Sistemas Informáticos, tipificando três condutas: alteração, danificação e destruição de dados de computadores”.

Com as invasões sofridas, nota-se a urgência necessidade de se criar uma legislação punitiva em relação aos *hackers,* que, com o intuito de ajudar ou não a população, estão praticando atos contra a administração pública, que, se não tomada nenhuma providencia poderá prejudicar muito bens nacionais e até mesmo projetos de grande importância para todos nós.

**CAPÍTULO 3 LEIS DA INTERNET NO BRASIL**

3.1 LEIS EM CURSO NO BRASIL

Podemos começar esse tópico ilustrando com um crime virtual praticado recentemente contra a atriz Carolina Dieckman em 07 de maio de 2012, onde a mesma foi vítima de fotos intimas suas que foram soltas na internet sem sua autorização.

A Lei em questão é 12.737/2012 conhecida como “extraoficial” que já entrou em vigor e foi apelidada por “Lei Carolina Dieckman” essa Lei modifica o Código Penal em relação a crimes praticados pela internet, ela cria punição especifica em tais casos, influenciando efetivamente para aprovação da lei chamada: “ **Marco Civil da Internet”** (oficialmente chamado de **Lei nº 12.965**, de [23 de abril](http://pt.wikipedia.org/wiki/23_de_abril) de [2014](http://pt.wikipedia.org/wiki/2014)) é a lei que regula o uso da Internet no Brasil, que analisaremos mais a frente.

Tal Lei “Carolina Dieckmam”, foi estabelecida pelo Deputado Paulo Teixeira, que criou a mesma com o objetivo de punir a invasão desses meios virtuais para obter, destruir e adulterar tais informações tidas como sigilosas.

A punição prevê de três meses a dois anos, além de multa.

De acordo com Paulo Teixeira que salienta:

“Nós precisávamos dessa lei, o Código Penal não dava conta disso” (Do UOL, em São Paulo, 02/04/2013).

Já existe também Congresso Nacional, projetos de Lei. O Deputado Freire Junior, propôs em seu Projeto de Lei, um acréscimo no artigo de lei do crime de furto, colocando mais dois incisos no artigo 155, §3º, do Código Penal. A partir desses dois incisos, o crime de furto praticado via *internet.*

O Projeto de Lei nº. 84/1999, criado pelo Deputado Luiz Pauhylino, coloca em pauta que o Código Penal vigente, vai passar a conter a Seção V, do Capítulo VI, do Título I, que terá os crimes informáticos.

O Deputado Luiz Pauhylino, tratou apenas dos crimes dos Sistemas Informáticos, criando uma norma penalizadora especifica e eficaz.

A vítima que sofrer introdução indevida deve mostrar e manifestar interesse em punir o autor desse delito, assim esse crime é de ação penal pública condicionada à representação, diferentemente dos crimes praticados contra entes públicos, que neste caso serão crimes de ação penal pública incondicionada.

Houve também a modificação do artigo 163, incluindo parágrafos no texto de lei, a ver:

“Art. 3º O art. 163, do Decreto-lei nº. 2.848, de 7 de dezembro de 1940, o Código Penal, passa a vigorar com as seguintes alterações, renumerando-se o parágrafo único para o §1º:

‘Art. 163.

Dado eletrônico

§2º Equipara-se à coisa:

I – o dado, a informação ou a base de dados presente em meio eletrônico ou sistema informatizado;

II – a senha ou qualquer meio de identificação que permita o acesso a meio eletrônico ou sistema informatizado.

Difusão de vírus eletrônico.

§3º Nas mesmas penas do §1º incorre quem cria, insere ou difunde dado ou informação em meio eletrônico ou sistema informatizado, indevidamente ou sem autorização, com a finalidade de destruí-lo, inutilizá-lo, modificá-lo ou dificultar-lhe o funcionamento”. (INELLAS. 2009. p. 159).

O projeto de lei, visa incluir como coisa, os meios eletrônicos, para que assim, sejam punidos os autores desses delitos.

Foi criado também e passou a incluir no nosso Código Penal, o crime de pornografia infantil. Que assim reza:

“Art. 218-A. Fotografar, publicar ou divulgar, por qualquer meio, cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:

Pena – reclusão, de um a quatro anos, e multa.

§1º As penas são aumentadas de metade até 2/3 (dois terços) se o crime é cometido por meio de rede de computadores ou outro meio de alta programação.

§2º A ação penal é pública incondicionada.” (INELLAS. 2009. p. 160).

Esse assunto é muito discutido pois, vem tentando ser combatido a muito tempo, policiais federais tentam de todas as formas coibir essa pratica delituosa, pois é um crime de grande potencial ofensivo.

O Projeto de lei nº. 84/1999, não deixaria de elaborar uma sanção para esses criminosos. A lei, estabelece como ação penal pública incondicionada, não dependendo nesta hipótese da vontade da vítima para se iniciar a ação penal.

Um outro projeto de lei que merece destaque, é o Projeto de Lei nº.1.713/1996, do Deputado Cássio Cunha Lima, que, em seu artigo 18, trata a ação de, segundo Inellas, “obter acesso, indevidamente, a um Sistema de computador ou a uma Rede integrada de computadores”.

Ele traz no §3º, do mesmo artigo, diz que: “se o acesso tem por escopo causar dano a outrem, a pena é de Detenção, de dois a quatro anos e multa”.

Ele tenta dessa forma coibir a invasão dos criminosos de hackers em sistemas informáticos por exemplo que causariam danos a terceiros.

O deputado Cássio Cunha Lima, no artigo 24, se manifesta também sobre crime de falsificação e alteração de documentos por meio do Sistema digital, onde considera-se documento no caso, disquete, CD-ROM, disco compacto e outras coisas que possam armazenar tais dados.

Vejamos constantemente que o legislador tem um cuidado maior em relação a conduta do agente, para que assim não haja empecilho para que se cumpra a lei.

Nenhum destes projetos de Lei expostos anteriormente conseguiram ser realmente colocados em prática, a questão maior é que teria que ser criado uma Lei especifica que entraria na parte geral da Legislação Penal, criando-se por exemplo uma legislação somente para crime virtual.

O Código Penal para tais crimes se vale a partir da Teoria da Atividade, ou seja o crime é considerado praticado na data da conduta, o Código Penal, reza em seu artigo 4° que:

“Art. 4º. Considera-se praticado o crime no momento da ação ou omissão, ainda que outro seja o momento do resultado”.

Assim, considera-se realizado no momento da ação ou omissão do agente.

O artigo 6º, do Código Penal também nos exemplifica sobre o lugar do delito:

“Art. 6º. Considera-se praticado o crime no lugar em que ocorreu a ação ou omissão, no todo ou em parte, bem como onde se produziu ou deveria produzir-se o resultado.”

Onde se encontra os aparelhos informáticos das vitimas, é o considerado “lugar do crime”.

Temos a ubiquidade a nosso favor nestes casos, pois se o fato ocorreu em território brasileiro, mesmo que o resultado se de fora daqui, a lei brasileira prevalecera.

Mesmo esses crimes atingindo cada vez mais a sociedade, com essas sanções a nosso favor é provável a coibição dessas práticas delituosas.

3.2 - LEI MARCO CIVIL DA INTERNET

Essa lei é a mais atual, Sancionada pela nossa “Presidenta Dilma Rousseff”, no evento acontecido em São Paulo no dia 20 de maio de 2014. Chamado “NETmundial – Encontro Multissetorial Global Sobre o Futuro da Governança da Internet”

Essa lei regula o uso da Internet no Brasil, por meio da previsão de princípios, garantias, direitos e deveres para quem usa a rede, bem como da determinação de diretrizes para a atuação do Estado. Teve seu projeto aprovado em 2009 na [Câmara dos deputados](http://pt.wikipedia.org/wiki/C%C3%A2mara_dos_deputados), em 25 de março de 2014 no [senado federal](http://pt.wikipedia.org/wiki/Senado_federal)  e por fim em 23 de abril de 2014, sancionada.

Essa lei teve um longo percurso na sua elaboração, no início em 2007, foi adotada pelo governo federal em função da resistência social ao [projeto de lei de cibercrimes](http://pt.wikipedia.org/wiki/Cibercrime#Projeto_de_Lei) conhecido como [Lei Azeredo](http://pt.wikipedia.org/wiki/Lei_Azeredo), muito criticado sob a alcunha de AI-5 Digital.

Depois de um debate desenvolvido, colaborativamente aberto por meio de um blog, em 2011 o “Marco Civil” foi apresentado como um [Projeto de Lei](http://pt.wikipedia.org/wiki/Projeto_de_Lei) do [Poder Executivo](http://pt.wikipedia.org/wiki/Poder_Executivo) à [Câmara dos Deputados](http://pt.wikipedia.org/wiki/C%C3%A2mara_dos_Deputados_do_Brasil), sob o número PL 2126/2011. No Senado, desde 26 de março de 2014 o projeto tramita sob o número PLC 21 de 2014.

O texto do projeto trata de temas como [neutralidade da rede](http://pt.wikipedia.org/wiki/Neutralidade_da_rede), [privacidade](http://pt.wikipedia.org/wiki/Privacidade), retenção de dados, a função social que a rede precisará cumprir, especialmente garantir a liberdade de expressão e a transmissão de conhecimento, além de impor obrigações de [responsabilidade civil](http://pt.wikipedia.org/wiki/Responsabilidade_civil) aos usuários e provedores, regulamentando assim o que é de saber de todos, e já vinha sendo usando, mas sem lei específica, até então.

|  |
| --- |
| No final de abril na internet “Café com a Presidenta”, saite ([www.brasil.gov.br](http://www.brasil.gov.br)), nossa  Presidenta deu as seguintes declarações ao entrevistador Luciano:  “... O Brasil tem agora um instrumento efetivo para garantir a liberdade de expressão, o respeito à privacidade das pessoas e das empresas, e o respeito aos direitos humanos na internet. Ela acrescentou que o Marco Civil da Internet foi saudado na Netmundial como um exemplo para o aperfeiçoamento e a democratização da governança global da internet e para torná-la cada vez mais aberta, multissetorial, multilateral, democrática e transparente. Esses são objetivos com que o mundo tem de se preocupar imediatamente face aos inaceitáveis e condenáveis episódios recentes de monitoramento e espionagem na rede, disse a Dilma Rousseff no programa Café com a Presidenta.  Transcrição  Apresentador: Olá, bom dia! Eu sou o Luciano Seixas e começa agora mais um Café com a Presidenta Dilma. Bom dia, presidenta!  Presidenta: Bom dia, Luciano! E bom dia para você que nos acompanha aqui no Café hoje!  Apresentador: Presidenta, hoje, vamos falar sobre o Marco Civil da Internet, aprovado pelo Congresso e sancionado pela senhora na semana passada. Qual é a importância dessa lei para a sociedade, presidenta?  Presidenta: Olha, Luciano, o Marco Civil da Internet é uma lei muito importante, porque estabelece os direitos e as responsabilidades, tanto dos usuários quanto dos provedores de internet. Com esta lei, a partir de agora o Brasil tem um instrumento efetivo para garantir a liberdade de expressão, o respeito à privacidade das pessoas e das empresas, e também, Luciano, o respeito aos direitos humanos na internet. O conceito básico desta lei, Luciano, é o de que a internet não tem donos, ela pertence a todos. Aliás, o Brasil está na vanguarda dessa legislação, porque somos o primeiro país do mundo a ter uma lei que consolida a internet como um espaço livre e democrático, o que é essencial para a participação social, para a inovação e, principalmente, para o exercício da cidadania.  Apresentador: E a senhora sancionou a lei do Marco Civil da Internet durante a Net Mundial, evento que reuniu, em São Paulo, os mais representativos líderes mundiais da internet. Como foi a repercussão da nossa nova lei no evento?   Presidenta: Foi excelente. O Marco Civil brasileiro foi saudado como um exemplo para o mundo, um instrumento importantíssimo para aperfeiçoar e democratizar a governança global da internet, para construir consensos e torná-la cada vez mais aberta, multissetorial, multilateral, democrática e transparente. Esses são objetivos com que o mundo tem de se preocupar imediatamente face aos inaceitáveis e condenáveis episódios recentes de monitoramento e espionagem na rede.  Apresentador: Presidenta, como fica a questão da armazenagem dos dados do Marco Civil da Internet?  Presidenta: Para começar, Luciano, o Marco Civil da Internet garante a privacidade dos internautas. Isso é muito importante, porque significa que os dados dos usuários da internet colhidos aqui no Brasil têm de ser protegidos, ainda que estejam armazenados em outro país. Veja bem, Luciano, com a nova lei, não importa se a empresa é brasileira ou estrangeira, ou se os dados estão armazenados aqui ou fora do país. Para todos os dados coletados no Brasil vale a lei brasileira e os direitos do usuário da internet têm que ser respeitados. Com isso, a partir de agora, qualquer cidadão que tiver seus dados utilizados e divulgados sem a sua expressa autorização pode recorrer à Justiça para exigir a proteção de seus direitos.  Apresentador: Como ficou a proteção à liberdade de expressão?   Presidenta: O Marco Civil da Internet garante, em primeiro lugar, que qualquer pessoa poderá se expressar livremente nos chamados espaços virtuais, o que é importante para o processo de amadurecimento de qualquer democracia e, em particular, da nossa. Mais que isso, Luciano, ele leva para o ambiente virtual a mesma regra que vale para qualquer espaço público. As pessoas são responsáveis pelo que dizem. Com isso, ele traz um equilíbrio entre as garantias constitucionais de proteção da liberdade de expressão e de proteção da intimidade, da honra e da imagem das pessoas. Aliás, a regra é clara: os direitos offline terão de ser os mesmos direitos garantidos ao cidadão online. Se alguém se sentir caluniado no meio virtual pode recorrer à Justiça da mesma forma que ocorre em qualquer outro espaço público. Como a repercussão dessas coisas na internet é muito rápida, a lei prevê ainda um procedimento simplificado para decisão dessas questões por meio de juizados especiais. O Marco Civil da Internet também traz uma regra específica para a retirada de imagens não autorizadas contendo, por exemplo, cenas de pedofilia e cenas de nudez. Aliás, este é um problema que atinge, sobretudo, as mulheres, vítimas do furto de dados ou mesmo de vingança praticada por um ex-parceiro, um ex-companheiro. Nesse caso, a pessoa que tiver sua intimidade indevidamente exposta poderá solicitar diretamente ao responsável pelo site a imediata retirada das imagens do ar. Se o responsável pelo site não retirar as imagens, ele responderá civil e criminalmente junto com o autor da postagem. Com isso, a vítima da divulgação não autorizada, de perversões ou de imagens íntimas terá um mecanismo rápido e, principalmente, discreto para se proteger.  Apresentador: Como ficou a responsabilidade pela publicação de conteúdos na internet?  Presidenta: Até hoje, Luciano, não estava claro de quem era a responsabilidade quando alguém prejudica o direito dos outros na internet, quando, por exemplo, publicam um texto ou imagem ofensiva. De quem é a culpa? O Marco Civil da Internet resolve isso ao dizer claramente que cada um responde pelo que faz na internet. Não dá para culpar um site ou um serviço de vídeo por alguma coisa que um usuário fez nele. Se alguém fez alguma coisa errada, Luciano, na internet, se violou o direito de outra pessoa, quem fez isso é que tem que assumir a responsabilidade. O responsável pelo site ou pelo serviço de vídeo somente responderá pelo conteúdo colocado por outras pessoas se se recusar a retirar a exibição de cenas de nudez ou outras, como a pedofilia, que não são admissíveis, depois de ser notificado pela vítima da invasão de privacidade ou depois de ser notificado judicialmente.   Apresentador: Outro ponto de destaque é a chamada neutralidade da rede. Explique isso, presidenta.  Presidenta: O nosso Marco Civil consagra a neutralidade da rede. É uma grande conquista que nós, depois de um amplo debate, conseguimos tornar consensual. O princípio da neutralidade, Luciano, estabelece o seguinte: o provedor tem que oferecer a internet sem limitar serviços que possam ser acessados pelos usuários. Isto é, Luciano, o provedor não pode interferir naquilo que você pode acessar. Ele, por exemplo, não pode te vender um serviço que diz o seguinte: você só pode acessar um site ou uma página específica. O provedor tem que te garantir acesso amplo, geral e irrestrito a todos os sites, a todos os serviços. A internet tem que ser oferecida, Luciano, por inteiro, sem discriminação, dentro da velocidade que foi contratada. A neutralidade impede que provedores de conexão privilegiem o acesso a determinados sites e serviços em razão de acordos econômicos. Se isso fosse permitido, o sucesso de um site ou de um serviço na internet passaria a depender do poder econômico de seu responsável, e não de sua qualidade. Todo mundo deve poder trocar informação, trocar conhecimento com todo mundo na internet, sem bloqueio, sem interferência, sem censura. A grande vantagem da internet é permitir que qualquer pessoa, com muito ou pouco dinheiro, possa divulgar suas ideias, seus serviços ou sua empresa. O poder de escolher o que quer acessar na internet é do usuário, seja ele rico, pobre ou mediano, e não da empresa que está vendendo a conexão. Por isso, defendemos a neutralidade da rede, defendemos que a neutralidade estivesse prevista claramente nos parágrafos da lei do Marco Civil da Internet. E conseguimos, é uma vitória do Brasil e dos brasileiros. Aliás, Luciano, faço questão de ressaltar o trabalho dos deputados e senadores que nos ajudaram a tornar o Marco Civil da Internet uma realidade.  Apresentador: O Marco Civil traz outros avanços à vida dos brasileiros?   Presidenta: Traz sim, Luciano. O Marco Civil da Internet é mais uma importante resposta à crescente demanda de participação da sociedade na política. É também um instrumento para a universalização da internet no nosso país. Ampliar o acesso à internet, garantir a liberdade de expressão, garantir o respeito dos direitos humanos, garantir a diversidade cultural, étnica, religiosa é fundamental para o desenvolvimento e para a construção de uma sociedade cada vez mais inclusiva e menos desigual. A internet, essa impressionante ferramenta de comunicação no mundo moderno, deve cada vez mais estar a serviço da sociedade, da democracia, da inclusão social, da paz e da liberdade.  Apresentador: Presidenta, infelizmente, o nosso tempo acabou. Obrigado por mais esse Café com a Presidenta.  Presidenta: Obrigada, Luciano. E um abraço para os nossos ouvintes. Até a próxima semana! E um "high five" para você, viu, Luciano!  Apresentador: Um "high five" para a senhora, presidenta! Você que nos ouve pode acessar o Café com a Presidenta na internet, o endereço é www.brasil.gov.br. Nós voltamos na próxima segunda-feira. Até lá!  E nessa intensa realidade de mudanças, onde o direito desfila suas bases e busca caminhar junto com as mudanças, muitos serão os erros até encontrar uma fórmula para diminuir contrastes entre a lei e sua aplicabilidade, pois somente assim poderemos resolver nossas “lides internauticas”, deixando os usuários da internet com maior tranquilidade para navegar nesse mundo de mudanças constantes. |
|  |

**CONSIDERAÇÕES FINAIS**

A internet cada vez mais vem se tornando fundamental em toda terra, pois se tornou no meio de tanta correria e falta de tempo das pessoas, o meio de comunicação mais rápido e mais capaz, estando a cada dia mais presente em nosso meio, no entanto trouxe com toda essa tecnologia a prática delituosa consigo.

Esse meio tecnológico só havia sido criado para membros do Governo americano se comunicarem entre si, portanto a internet acabou se tornando fundamental para a sociedade, não sendo mais somente utilizados para fins lícitos mais também para constante práticas delituosas que vem se tornando um problema, tirando da sociedade sua segurança.

Como o nosso Código Penal foi criado em época passada, se tornou o mesmo ineficaz para sanção de tais crimes, pela falta de avanço e pela falta de leis em relação a esses crimes é que se vê uma urgência em criar novos meios punitivos para que se coíba esses delitos, juntando especialistas da área de informática e entendentes do campo jurídico, poderia daí elaborar leis eficientes contra esses criminosos.

Vários desses delitos ocorreram também em diversos outros países, e em quase todos eles foram feitas leis modernas que coíbem essas ações.

Foi criado um Comitê no Brasil, em 1998, que não alcançou as tecnologias que foram surgindo, porém com o entendimento de deputados, foram criados vários Projetos, mais que ainda não foram colocados, de modo geral, em prática.

Finalizando então percebemos como falta uma legislação eficaz para coibição dessas práticas delituosas e para que capturaresses hackers para que se possa garantir a segurança.

Deste modo, note-se a necessária criação de uma legislação penal específica para a apuração dos crimes informáticos, com a devida autorização para diligências onde possa haver quebra de sigilos, para que assim, a eficácia se torne a garantia se maior segurança em meio a um planeta que mais do que nunca necessita da internet do seu dia-a-dia, esperamos assim, e estamos otimistas, que com essa nova Lei “MARCO CIVIL DA INTERNET” sancionada a pouco traga mais garantias fundamentadas, ao cidadão de bem, que usa a internet.

**REFERÊNCIAS**

**Bibliográficas**

BEVILAQUAqua, Clovis. **Teoria geral do direito civil**. Brasília: Ministério da Justiça, 1972 (1928).

CORRÊA, Gustavo Testa. **Aspectos Jurídicos da Internet**. 1ª ed. São Paulo: Saraiva, 2000.

INELLAS, Gabriel César Zaccaria .**Crimes na Internet.** 2ªed. São Paulo: Juarez de Oliveira, 2009.

GARCIA, Dinio de Santis. **Introdução à Informática Jurídica**. 1ª ed. São Paulo: Universidade de São Paulo, 1976.

GRECO, Rogério. **Código Penal Comentado**. 4ª ed. Rio de Janeiro: Impetus, 2010.

KELSEN, Hans. **Teoria pura do direito*,*** 1ª versão. São Paulo: Revista dos Tribunais, 2a ed., 2002 (1933).

MONTESQUIEU. **Do espírito das leis*.*** Rio de Janeiro: Ediouro.

SILVA, Rita de Cássia Lopes. **Direito Penal e Sistema Informático.** 1ªed. São Paulo: RT, 2003.

**UOL. Tecnologia.uol.com.br.** São Paulo, 2013.

**Eletrônicas**

[www.aultimaarcadenoe.com.br/](http://www.aultimaarcadenoe.com.br/palavras-e-expressoes)

[www.brasil.gov.br](http://www.brasil.gov.br).

[www.ebc.com.br/](http://www.ebc.com.br/.../dilma-marco-civil-da-internet-foi-saudado-como-ex)