CENTRO UNIVERSITÁRIO TABOSA DE ALMEIDA - ASCES/UNITA
BACHARELADO EM DIREITO

INTERNET, UMA TERRA SEM LEI?

DANIELLA THAYSA NEVES VIDAL

CARUARU
2018

DANIELLA THAYSA NEVES VIDAL

INTERNET, UMA TERRA SEM LEI?

Trabalho de Conclusão de Curso, apresentado ao Centro Universitário Tabosa de Almeida - ASCES/ UNITA, como requisito parcial para obtenção do grau de Bacharel em Direito.
Orientador: Prof. Msc. Adrielmo de Moura Silva

CARUARU
2018

BANCA EXAMINADORA

Aprovado em: ____/___/_____

_____

Presidente: Prof. Msc. Adrielmo de Moura Silva

_____

Primeiro Avaliador: Prof.

_____

Segundo Avaliador: Prof.

RESUMO

As relações sociais evoluem e são sempre acompanhadas por novas normas que buscam suprir a necessidades da sociedade para o bom convívio, com a finalidade de regular a convivência entre as pessoas. Com a evolução frenética da Internet, e a forma como ela está inserida no cotidiano das pessoas, seja como ferramenta de trabalho e entretenimento, surgiu a necessidade do direito de regular essas relações que passaram a ser desenvolvidas nesse espaço virtual. O presente trabalho versa sobre as questões dos crimes virtuais. O controle dessas condutas se tornou tema de discussão no Direito, observando as principais divergências da necessidade de legislação específica e a dificuldade de resposta eficaz do Estado à tais atos. Mais precisamente, é abordado quem são esses sujeitos que atuam de forma criminosa em anonimato, quais danos eles podem causar, o que a legislação atual vigente versa sobre tais crimes, quais as dificuldades encontradas, a necessidade da remodelação dessa legislação, o que existe de projetos de leis acerca do assunto, e qual a importância da aprovação desses projetos. No decorrer do trabalho existe a presença de vários termos, todos conceituados, que são típicos de usuários que tem certa familiaridade com uso de computadores, mas o intuito dessa linguagem é proposital com a intenção de deixar o leitor informado, ou mais familiarizados com os termos desse novo mundo digital, além de fazer um alerta ao público do ramo do direito quanto a esse novo problema na escassez de legislação que tende a crescer de forma acelerada sem uma devida solução.

Palavras-Chave: Internet. Crimes. Leis. Escassez.

ABSTRACT

Social relations evolve and are always accompanied by new norms that seek to meet the needs of society for good socializing, with the purpose of regulating the coexistence between people. With the frenetic evolution of the Internet, and the way it is inserted in the everyday of people, as a tool for work and entertainment, the need arose for the right to regulate these relationships that started to be developed in this virtual space. This paper deals with the issues of virtual crimes. The control of these behaviors has become a topic of discussion in the Law, observing the main divergences of the need of specific legislation and the difficulty of effective response of the State to such acts. More precisely, it is approached who are these subjects who act in a criminal way in anonymity, what damages they can cause, what current legislation is about such crimes, what difficulties are encountered, the need to remodel that legislation, what exists Draft laws on the subject, and how important it is to approve such projects. In the course of the work there is the presence of several terms, all of them conceptualized, that are typical of users who have a certain familiarity with the use of computers, but the intention of this language is purposive with the intention of leaving the reader informed, or more familiar with the terms of this new digital world, in addition to alerting the public in the legal field about this new problem in the lack of legislation that tends to grow rapidly without a proper solution.

Keywords: Internet. Crimes. Laws. Scarcity.

SUMÁRIO

INTRODUÇÃO

Desde o princípio, o homem é um ser sociável, ou seja, tem a necessidade de se comunicar, ouvir e ser ouvido, devido essa necessidade que surgiu a dinâmica da tecnologia, os avanços são utilizados para aumentar a praticidade e proporção dessa comunicação. O benefício dessa tecnologia é indiscutível, proporcionou o maior avanço em todos os setores de produção, levando quase que instantaneamente notícias de e para todo o mundo.

O mundo globalizado e a crescente evolução dessa tecnologia encurtaram a relação entre as pessoas, tais relações passaram a ser feitas por meio de equipamentos eletrônicos conectados a uma rede de Internet, a partir disso, culturas diferentes passaram a se encontrar, novas relações começaram a surgir nessa Era digital.

Na última década a informática passou a fazer parte do cotidiano de grande parte da população em todo o mundo. A internet tornou-se uma ferramenta de extrema necessidade para vários tipos de finalidade, sendo um objeto que proporciona conforto e praticidade passou também a ser utilizado como veículo para prática de vários crimes.

A Internet trouxe aos indivíduos a possibilidade de assumir várias identidades, produzir muitas realidades, e o de maior relevância proporcionou o anonimato, o que alimentou no ser humano a sensação de liberdade. Surgindo então a necessidade do direito de regular essas relações e ações.

O presente trabalho foi objeto de pesquisa frente aos principais autores que abordavam sobre a relação do Direito Penal com os crimes que ocorrem nas redes de informática, utilizando assim o método dedutivo. Do mesmo modo, foram explorados artigos científicos e monografias disponíveis na internet para traçar discussões acerca do assunto, para isso foi utilizado o procedimento técnico de pesquisa bibliográfica, analisando materiais já publicados.

Ademais, foram analisados precedentes judiciais, tais quais, decisões e leis já vigentes, acerca da forma de punição ou condenação dos crimes cibernéticos, e da discussão sobre novas leis ou projetos de leis, para tipificação desses crimes. O acesso à essas leis e projetos, durante toda pesquisa, foi buscado diretamente nos sites oficiais, bem como sites jurídicos que dispõe desse acesso.

Os índices de crimes virtuais vêm aumentando com frequência, a escassez de legislação específica é um dos fatores de grande relevância para incentivar essa prática. Este artigo tem como propósito expor as dificuldades encontradas em tipificar e coibir essas

condutas criminosas, devido à escassez de legislação específica, demonstrando a necessidade da remodelação da legislação vigente.

1 CHEGADA DA INTERNET NO BRASIL

Com os avanços tecnológicos relacionados à tecnologia, computação, em especial a Internet, agilizaram o processo de globalização econômica e cultural, fazendo o computador se tornar uma ferramenta indispensável no dia a dia das pessoas e nos mais diversos lugares.

A sociedade após esses avanços pôde descobrir o poder da informação, havendo uma mudança da cultura escrita para a cultura multimídia, todas essas informações e avanços trouxeram para o meio novas formas de comunicação.

O que conhecemos hoje como Internet teve início em 1969, nos tempos da Guerra Fria, quando a empresa ARPA (Advanged Research and Projects Agency), com a finalidade de manter comunicação das bases militares dos Estados Unidos, criou uma rede batizada por ARPANET (Advanced Research Projects Agency Network). O objetivo de sua criação era com essa rede conseguir espalhar os dados mais valiosos do governo americano, ao invés de deixá-los centralizados em um servidor apenas, evitando assim a perda dos dados em um ataque inimigo.

Na década de 1990, aconteceu uma expansão significativa na Internet, para facilitar a navegação surgiram vários navegadores, como por exemplo e ainda utilizado por muitos, o Internet Explore, na mesma época e devido ao desenvolvimento desses navegadores, começou a utilização dos portais de serviços online. No começo a Internet era utilizada mais para serviços de *e-mail,* ou transferências de arquivos, logo depois os estudantes começaram utiliza-la como fonte de pesquisa, e até mesmo o começo da utilização de *sites de games* para diversão. Já no tocante as empresas, viram na internet um excelente caminho para melhorar seus lucros, começando assim o "mundo" de compras online. (GUIMARÃES, 2013.).

Apenas em 1991, a famosa Internet chegou ao Brasil, com a RNP (Rede Nacional de Pesquisa), o objetivo no Brasil era atender à conexão das redes de universidade e centros de pesquisas, porém logo após as esferas federal e estadual também se interligaram. (GUIMARÃES, 2013.).

Em 1994, com a finalidade de melhoria da internet a Embratel lançou o serviço experimental, um ano após esse fato, em 1995, os Ministérios de Comunicação e de Ciência e Tecnologia, abriram o setor privado da Internet para exploração comercial, podendo assim

contratar conexões com a RNP, e logo após, com a Embratel. A Internet hoje representa um salto no desenvolvimento da humanidade, e como consequência disso a mudança no pensar e no agir da sociedade. Esse avanço trouxe consigo novos paradigmas para a sociedade pós-moderna e com isso, para os sistemas que organizam e regulam, como o Direito.

O computador, junto com a Internet, é possível produzir muitas realidades, onde cada indivíduo pode criar a sua. Podem assumir muitas faces, mascarar-se, desempenhar inúmeros papéis, e até mesmo mudar de raça, sexo, idade, e pode com isso assumir várias identidades novas e falsas, em parte, vem cada dia mais substituindo os parceiros reais, isso significa a dissolução do sujeito, da pessoa, da identidade até mesmo da essência humana, criando o anonimato e a distância entre os seres.

Surgiram com esses avanços indivíduos que tem como atividade básica lançar ataques virtuais contra outros computadores, o invasor em questão é capaz através de um profundo conhecimento do meio e da linguagem, destruir e coletar informações pessoais, furtar números de cartão de crédito e senhas bancárias, conseguir senhas de redes sociais, podendo assim se passar pela pessoa, propagar vírus no computador, isso tanto contra cidadãos comuns, como empresas e órgãos públicos.

Isso ocorre em mundo virtual popularmente conhecido como “ciberespaço”. Esse é um ambiente virtualmente criado pela utilização de meios de comunicação modernos, entre eles a Internet. Isso ocorre devido haver possibilidade de pessoas e equipamentos trocarem informações das mais variadas formas, gerando a chamada cibercultura. A cibercultura é produzida no ciberespaço que é um novo meio de comunicação que surge da interconexão de computadores.

Segundo o filósofo, sociólogo e pesquisador em ciência da informação e da comunicação que estuda o impacto da Internet na sociedade, Pierre Lévy (1999, p. 17):

> O termo ciberespaço especifica não apenas a infraestrutura material da comunicação digital, mas também o universo de informação que ela abriga, assim como os seres humanos que navegam e alimentam esse universo. Quanto a cibercultura, especifica o conjunto de técnicas (materiais e intelectuais), de práticas, de atitudes, de modos de pensamento e de valores que se desenvolvem juntamente com o crescimento do ciberespaço.

Estamos passando por um processo de universalização da cibercultura, pois dia-a-dia estamos mais envoltos nas novas relações de comunicação, rapidez e produção de conhecimento que ela nos oferece, porém como consequência disso acabamos gerando novas formas de relações sociais com códigos e estruturas próprias.

É justamente nesse ambiente livre e sem fronteiras, devido esses avanços frenéticos proporcionados pelas novas tecnologias, em especial a Internet, que o Direito Penal passou a encontrar dificuldades de adaptação, não conseguindo acompanhar tais avanços, em decorrência disso, passou a acontecer a chamada criminalidade virtual, onde agentes se aproveitam da possibilidade de anonimato e ausência de regras para atuar.

Os primeiros casos de crimes informáticos foram na década de 1960, eram delitos onde o infrator manipulava, sabotava, espionava ou tinha o uso abusivo de computadores e sistemas. Já em 1980, houve a expansão dessas ações, que refletiram em manipulações de caixas bancários, pirataria de programas pornô infantil, hoje, infelizmente, algo ainda presente no nosso cotidiano. (GUIMARÃES, 2013.)

Diante do exposto, problemas relacionados, por exemplo, ao armazenamento, à divulgação de dados pessoais, assim como a existência de várias demandas judiciais, requerendo indenizações por danos morais, por violações ocorridas pela internet, existe a necessidade de abordar algumas questões supracitadas, com intuito de expor a forma como são tratados no Brasil os fatos ocorridos na Internet.

2 FALTA SEGURANÇA ATÉ NA INTERNET E QUAIS AS CONSEQUÊNCIAS

Não existe uma simples forma de definir o que é Internet, ou algum conceito aceito mundialmente para defini-la. O que conhecemos hoje por Internet, é uma grande rede interligada por todo o Mundo, que emite e recebe informações de forma rápida e fácil, e para isso utiliza determinada codificação para transferência de dados.

No artigo 5º, inciso I, do Projeto de Lei nº 2.126/2011, em análise no Congresso Nacional, também conhecido como “Marco Civil da internet”, tem definição como: “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”.

Segundo, Marcel Leonardi, (2009, p. 344), Internet é “... uma rede internacional de computadores conectados entre si. É hoje um meio de comunicação que possibilita o intercâmbio de informações de toda natureza, em escala global, com um nível de interatividade jamais visto anteriormente”.

Hoje praticamente todas as pessoas sejam elas físicas ou jurídicas, interagem no chamado ciberespaço, a Internet se tornou um meio indispensável, seja ele para comunicação,

trabalho ou diversão. Porém, por se expandir dessa forma em residências, órgãos públicos e empresas, seu livre acesso vem resultando em problemas diretamente ligados à segurança, sobretudo quando envolve informações sigilosas.

O problema de segurança na Internet pode ser dividido em vários aspectos, porém existem três mais relevantes, sendo eles, a autenticação, confidencialidade e integridade. A autenticação é o processo pelo qual é validada a entidade do utilizador. A confidencialidade tem como finalidade, reunir todas as vertentes de segurança que limitam o acesso à informação apenas às entidades autorizadas, previamente autenticadas, sejam eles utilizadores humanos ou máquinas. Já a integridade permite garantir que a informação a ser armazenada ou processada é autêntica, ou seja, se essa informação é corrompida ou não. Todos esses aspectos objetivam impedir, ou diminuir, uma série de crimes e atos ilícitos que podem ser perpetrados pelos meios informáticos.

É de grande relevância definir os sujeitos que sofrem e que atuam tais ataques, sendo eles, sujeito passivo e sujeito ativo.

Sujeito passivo ou a vítima dos crimes, é o ente pelo qual recai a conduta omissiva ou comissiva realizada pelo sujeito ativo, podem ser essas vítimas, indivíduos, instituições, governos e entre outras que utilizem sistemas de informação, sejam eles conectados ou não à internet. O engano e a fraude são de difícil distinção, o que leva a essas vítimas a serem de grande maioria usuários que tem pouco conhecimento com essa nova tecnologia.

Porém, não são apenas usuários que não sabem lidar com essas inovações da tecnologia que sofrem com a fragilidade da segurança quanto ao uso da internet. Como diz o estudo da Symantec, que trata sobre segurança da Internet no Brasil, aponta que 67% das empresas nacionais já foram vítimas de ataques em suas redes. Tais números demonstram a facilidade de cometer esses ataques no país. (Disponível em: <www.symantec.com.br>, acesso em 21 de maio de 2017.)

De qualquer modo, as vítimas que podem sofrer crimes de informática, são qualquer pessoa física ou jurídica e mesmo de natureza pública ou privada.

Quanto ao sujeito ativo, são inúmeras as possibilidades de conduta delituosa. Tantas opções fez com que originasse uma classificação, para que assim pudesse ser identificado pelo seu objeto ou pelos meios de atuação. Para diversos autores, esses indivíduos são denominados "*computer criminals*", considerando a habilidade de lidar com os computadores, para Klaus Tiedemann em Criminalidade mediante Computadores, seriam esses sujeitos "criminosos informáticos" em face de seus comportamentos ilegais serem sempre no meio informático.

Portanto, os indivíduos que comentem “crimes de computador” possuem certas características bem particulares, ainda são os costumeiros criminosos dessa área os habilidosos operadores de computadores e sistemas, e muitos deles nem atingiram a maioridade penal. Esses indivíduos são definidos de modo geral por vários autores por: *hackers, crackers, phreakers e carders.* (LIMA, 2011, p. 40.)

> a) *Hackers:* em regra, são invasores dos sistemas eletrônicos;
> b) *Crackers:* são aqueles que “quebram” os códigos de segurança de forma ilegal, para ter acesso a senhas de redes e códigos de programas;
> c) *Phreakers:* são popularmente conhecidos como os “maníacos por telefonia”, esses conseguem acesso direto a centrais de telefonia, podendo desligar e ligar telefones, assim como apagar contas;
> d) *Carders:* como deixa a entender o nome, são especialistas em roubar senhas de cartões, sejam eles de crédito ou conta bancária para realizarem fraudes online.

Essa classificação como já exposto, são indivíduos com grande conhecimento de sistemas operacionais e de linguagem de programação, todos eles buscam achar as falhas na segurança dos sistemas com a única intenção de invasão.

Assim como houve a necessidade de classificar os indivíduos que atuam de forma delituosa os computadores, para que houvesse a distinção de cada um, houve a necessidade de classificar as condutas realizadas por esses agentes, são as de mais relevância: *Spywares*, *Cookies* e o *Trojan Horse* ou Cavalo de Tróia. (MUOIO, 2006, p. 169.)

> a) *Spywares:* são programas intrusos que vasculham a intimidade do usuário da rede e fornece informações sigilosas para outro usuário;
> b) *Cookies:* vem do inglês “biscoito” e são programas que conseguem guardar identificações e senhas de acesso quando a vítima vai de uma página de navegação para outra, além de disseminar outros vírus;
> c) *Trojan Horse* ou Cavalo de Tróia: é um vírus que abre toda via de acesso nos computadores, permitindo assim o livre e total acesso ao computador da vítima.

Ainda no tocante sobre condutas ilícitas, o fenômeno chamado “vírus de computador” é o mais difundido em todo o país, e é um programa de computador que possui a capacidade de se reproduzir sem autorização do usuário e interfere nos procedimentos normais da máquina.

Tais condutas acima citadas são chamadas de Crimes Informáticos, que são aqueles que irão causar algum tipo de dano a máquina da vítima, esse dano ocorre por meio de programas enviados via Internet, ou por meio de dispositivos de inicialização do computador.

São diversas as formas de ataque que um computador pode sofrer, podendo vir a ser danificado parcialmente ou até mesmo totalmente.

No que diz respeito à crimes informáticos, Gustavo Testa Correa define que seriam: “Todos aqueles relacionados às informações arquivadas ou em trânsito por computadores, sendo esses dados, acessados ilicitamente, usados para ameaçar ou fraudar. ”, já para Tellez Valdez são: “atitudes ilícitas em que se têm aos computadores como instrumento ou fim (conceito atípico) ou as condutas típicas, antijurídicas e culpáveis em que se têm aos computadores como instrumento ou fim (conceito típico).

Nesse segmento, para Furlaneto Neto, crime informático significa “qualquer conduta ilegal, não ética ou não autorizada que envolva o processamento automático de dados e/ou a transmissão de dados”, interessante também a definição proposta por Marco Aurélio Costa quando afirma que:

> É a conduta que atenta contra o estado natural dos dados e recursos oferecidos por um sistema de processamento de dados, seja pela compilação, armazenamento ou transmissão de dados, na sua forma, compreendida pelos elementos que compõe um sistema de tratamento, transmissão ou armazenagem de dados, ou seja, ainda, na forma mais rudimentar. Isto posto, depreende-se que o crime de informática é todo aquele procedimento que atenta contra os dados, que o faz na forma em que estejam armazenados, compilados, transmissíveis ou em transmissão. Assim, o crime de informática pressupõe dois elementos indissolúveis: contra os dados que estejam preparados às operações do computador e, também através do computador, utilizando-se software e hardware, para perpetrá-los.
> (Disponível em <http://www.jus.com.br/doutrina/crinfo.html>, acesso em 11 de maio de 2017.)

Túlio Lima Vianna (2003, p. 37), classifica crime informático em:

> a) Crimes informáticos impróprios: aqueles nos quais o computador é usado como instrumento para a execução do crime, mas não há ofensa ao bem jurídico inviolabilidade da informação automatizada (dados);
> b) Crimes informáticos próprios: aqueles em que o bem jurídico protegido pela norma penal é a inviolabilidade das informações automatizadas (dados);
> c) Delitos informáticos mistos: são crimes complexos em que, além da proteção da inviolabilidade dos dados, a norma visa a tutelar bem jurídico de natureza diversa;
> d) Crimes informáticos mediatos ou indiretos: é o delito-fim não informático que herdou esta característica do delito-meio informático realizado para possibilitar a sua consumação.

Crime informático, cibercrime, crime eletrônico ou digital, são termos utilizados para se referir a toda atividade em que um computador ou uma rede de computadores é utilizada como ferramenta, seja como base de ataque ou meio de crime.

Os direitos mais afetados pela evolução do uso da Internet, foram o Direito à Privacidade e à Intimidade, devido a facilidade, frequência e acessibilidade no uso dos computadores e redes, e como consequência disso a grande exposição dos indivíduos e a facilidade em acessar toda essa rede informática com a sensação de anonimato.

O artigo 5º, inciso X da Constituição Federal dispõe sobre a inviolabilidade da privacidade e da intimidade:

> 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.

É assegurado a todos o direito à Privacidade, porém este direito não é absoluto. Existe uma enorme variação de acordo com a sociedade, com o indivíduo, e com a época. O limite da privacidade é subjetivo, se tornando uma difícil tarefa para o legislador regulamentar e defendê-la em todas as situações.

Para Bastos, o direito à Privacidade é "a faculdade que tem cada indivíduo de obstar a intromissão de estranhos em sua vida privada e familiar, assim como de impedir-lhes o acesso a informações sobre a privacidade de cada um, e também impedir que sejam divulgadas informações sobre esta área da manifestação existencial do ser humano".

Conforme exposto anteriormente, a inviolabilidade da privacidade e da intimidade está disposta no artigo 5º, inciso X da Constituição Federal, o qual diferencia o direito à intimidade e à vida privada, porém alguns doutrinadores definem os dois como sinônimos. Apesar desses direitos estarem associados e serem muito parecidos, a diferença está no fato de que o direito à privacidade é bem mais amplo do que o direito à intimidade.

O direito à privacidade, é o direito de impossibilitar a intervenção de terceiros em sua vida íntima, além de regular as informações sobre elas divulgadas. Já o direito à intimidade seria a esfera de proteção que envolve a parte mais íntima da pessoa, como exemplo, ideias, pensamentos, desejos e emoções.

Assim, o direito à vida privada e intimidade permitem a preservação pelas pessoas de uma esfera íntima de suas vidas, tanto a exclusiva, que seria a intimidade, como a área em que envolve fatos e acontecimentos compartilhados com pessoas íntimas, ou seja, a vida privada, tudo para preservar o indivíduo da invasão ou ingerência de terceiro.

3 ESCASSEZ DA LEGISLAÇÃO ATUAL E NOVOS PROJETOS DE LEI PARA TIPIFICAÇÃO DESSAS CONDUSTAS

A busca por globalização gerou a inserção dos cidadãos no mundo informático, isso também fez com que os mesmos fiquem expostos a uma série de novos riscos, por não existir proteção a bens jurídicos penalmente relevantes e que são violentados diariamente.

Diversas condutas nesse "novo mundo do crime" não são tipificadas, exceto e conhecidos por nós estelionato e furto, os quais não são totalmente adequados ao combate dessa nova criminalidade, e que em muitos casos a analogia se torna proibida, em respeito aos princípios da legalidade, tipicidade e anterioridade.

Analisando a atual Legislação Penal Brasileira quanto aos crimes de informática, é necessário que se entenda a déficit de legislar por não haver tipificação de tais crimes e que mudanças são indispensáveis para a melhor adaptação a realidade tecnológica que hoje nos cerca.

É necessário ressaltar que a Internet e o Direito Penal possuam total interação, por que o ciberespaço e toda sua cultura afetam significativamente as relações do mundo real, fazendo assim com que utilizemos do Direito para observar e disciplinar as condutas ali praticadas contrárias aos bens jurídicos, que ao final são relações entre indivíduos.

No tocante ao nosso atual Direito Penal de Informática ser quase inexistente, é real, muito pouco se tem quanto ao âmbito legislativo no que se refere ao campo da informática. A primeira iniciativa legislativa veio no de 1984 com o advento do Plano Nacional de Informática e Automação (CONIN).

Com a chegada desse Plano aqui no Brasil, surge então a primeira lei específica no ramo da informática, a Lei 7.232/84. Logo em seguida no ano de 1987 surge a Lei de nº 7.646, a primeira a descrever condutas e infrações de informática, esta foi revogada pela Lei de nº 9.609, no ano de 1998.

Com a Lei nº 9.609 atualmente ainda aplicada, resta tipificada as seguintes condutas:

> Art. 12. Violar direitos de autor de programa de computador:
> Pena - Detenção de seis meses a dois anos ou multa.
> § 1º Se a violação consistir na reprodução, por qualquer meio, de programa de computador, no todo ou em parte, para fins de comércio, sem autorização expressa do autor ou de quem o represente:
> Pena - Reclusão de um a quatro anos e multa.
> § 2º Na mesma pena do parágrafo anterior incorre quem vende, expõe à venda, introduz no País, adquire, oculta ou tem em depósito, para fins de

> comércio, original ou cópia de programa de computador, produzido com violação de direito autoral.
> § 3º Nos crimes previstos neste artigo, somente se procede mediante queixa, salvo:
> I - quando praticados em prejuízo de entidade de direito público, autarquia, empresa pública, sociedade de economia mista ou fundação instituída pelo poder público;
> II - quando, em decorrência de ato delituoso, resultar sonegação fiscal, perda de arrecadação tributária ou prática de quaisquer dos crimes contra a ordem tributária ou contra as relações de consumo.
> § 4º No caso do inciso II do parágrafo anterior, a exigibilidade do tributo, ou contribuição social e qualquer acessório, processar-se-á independentemente de representação. (Disponível em <http://www.planalto.gov.br/ccivil_03/leis/L9609.htm>, acesso em 12 de maio de 2017.)

Outros artigos e leis de grande relevância que ainda são utilizados atualmente e que tipificam condutas são:

> a) Art.153, §1º-A, do Código Penal: "Divulgar, sem justa causa, informações sigilosas ou reservadas, assim definidas em lei, contidas ou não nos sistemas de informações ou banco de dados da Administração Pública", (Incluído pela Lei nº 9.983, de 2000), com pena de detenção de 1 a 4 anos, e multa;
> b) Art. 313-A, do Código Penal: "Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano", (Incluído pela Lei nº 9.983, de 2000), pena de reclusão de 2 a 12 anos, e multa;
> c) Art. 313-B, do Código Penal: "Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente", (Incluído pela Lei nº 9.983, de 2000), pena de detenção de 3 meses a dois anos, e multa;
> d) Art. 325, §1º, incisos I e II: "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" e "II - se utiliza, indevidamente, do acesso restrito", (Incluído pela Lei nº 9.983, de 2000), ambos com pena de detenção de 6 meses a 2 anos, e multa;
> e) Art. 2º, inciso V, da Lei nº 8.137/90: "V - utilizar ou divulgar programa de processamento de dados que permita ao sujeito passivo da obrigação tributária possuir informação contábil diversa daquela que é, por lei, fornecida à Fazenda Pública. ", pena de detenção de 6 meses a 2 anos, e multa;
> f) Art. 72 da Lei nº 9.504/97: "Constituem crimes, puníveis com reclusão, de cinco a dez anos:
> I - obter acesso a sistema de tratamento automático de dados usado pelo serviço eleitoral, a fim de alterar a apuração ou a contagem de votos;
> II - desenvolver ou introduzir comando, instrução, ou programa de computador capaz de destruir, apagar, eliminar, alterar, gravar ou transmitir dado, instrução ou programa ou provocar qualquer outro resultado diverso do esperado em sistema de tratamento automático de dados usados pelo serviço eleitoral;

> III - causar, propositadamente, dano físico ao equipamento usado na votação ou na totalização de votos ou a suas partes. (Lima, 2011, p. 113.)

No que concerne aos crimes de informática, essas são basicamente todas as condutas típicas existentes no Brasil e diante do exposto, fica evidente que a legislação existente no ordenamento jurídico brasileiro atual, em relação as infrações cometidas no âmbito informático, não é eficaz para reprimir todas as condutas hoje cometidas diariamente nessa área.

No tocante, Ivette Senise Ferreira (2001, p. 391), diz:

> Essas leis, todavia, longe de esgotarem o assunto, deixaram mais patente a necessidade do aperfeiçoamento de uma legislação relativa à informática para a prevenção e a repressão de atos ilícitos específicos, não previstos ou não cabíveis nos limites da tipificação penal de uma legislação que já conta com mais de meio século de existência. O Código Penal Brasileiro, cuja Parte Especial data de 1940, e portanto, elaborado numa época em que se dava primazia à proteção individual, apesar do volume da legislação especial que o acompanhou posteriormente, não se mostra suficiente e adequado para suprir as necessidades nesse setor e coibir abusos que se verificam de forma a interesses legítimos, no plano individual e social, que ao Estado cumpre coibir sobretudo através do direito penal, se os conflitos não puderem ser solucionados de outra forma, como dispõe a boa doutrina, segundo o princípio da subsidiariedade.

Fica evidente mais uma vez quão escassa é nossa legislação quanto aos delitos cometidos no ramo da informática. É inegável a existência da dificuldade na punição dessas ações, da mesma forma que seria impossível jogar fora toda uma legislação existente. Em parte, isso se dá por serem tais ações efetivadas com a utilização de tecnologia muito específica, com características peculiares e com mudanças céleres, a acontecer todos os dias, o que impossibilita o legislador de antever a problemática possível de ocorrer.

Todas as críticas existentes quanto a Parte Especial do Código Penal são pertinentes, as infrações soam por demais contemporâneas, e somente com esforço podem ser adaptadas às normas ali existente. Oportuna é a criação de novas leis, que determinem novas condutas típicas, e facilitem a punição desses agentes criminosos. Existem várias iniciativas legislativas que estão em tramite no Congresso Nacional quanto aos crimes de computador, e algumas delas merecem destaque.

O primeiro que merece destaque é o Projeto de Lei nº 76/00, do Senador e Ex-ministro da Justiça Renan Calheiros, esse encontra-se exposto integralmente no anexo A.

Se aceito esse projeto de lei, se tornará crime a adulteração ou transferência de arquivos eletrônicos correspondentes a operações financeiras, a difusão de material ofensivo à

honra, a sonegação de tributos decorrentes de operação virtuais, incriminará a corrupção de menores praticada com uso do meio informático e discorrerá sobre a divulgação da intimidade das pessoas.

De grande relevância, cria o aumento de pena quando as condutas delitivas são contra empresas de serviços públicos ou órgão de administração pública, assim como estabelece multas iguais ao valor do proveito pretendido ou do risco e prejuízo da vítima, e por fim, apresenta o progresso quando traça normas relativas às proposituras das ações penais.

Há uma variedade de crimes e bens jurídicos a serem preservados, além de tantas peculiaridades relacionadas a multas, penas e agravantes, demonstrando mesmo a necessidade de uma consolidação de normas ou de uma alteração na parte em que abrange essa variedade de crimes relacionadas aos crimes de informática.

Ainda sobre projetos de lei, o de maior importância e ainda em trâmite na Câmara dos Deputados aguardando votação, foi o Projeto de Lei de nº 84/99 proposto pelo Deputado Federal Luiz Piauhylino, no ano de 2010, também exposto integralmente do anexo B.

O Projeto de Lei nº 84/99 tem como intenção principal suprir a necessidade da tipificação de condutas havidas no meio informático, essas que possam vir a lesar dados eletrônicos ou bens jurídicos, regulando assim, os crimes referentes à informática sem prejuízo das demais figuras delitivas previstas em outras normas legais.

O referido projeto traz também algumas definições de condutas de grande importância, sendo elas, o dano a dado ou programa de computador, o acesso indevido ou não autorizado, alteração de senha ou mecanismo de acesso a programa ou dados, obtenção indevida ou não autorizada de dado ou instrução de computador, a violação de segredo armazenado em computador e quanto a veiculação de pornografia através de rede de computador. Essas condutas são previstas no projeto com penas de até seis anos de reclusão e multa.

É de grande destaque nesse projeto a iniciativa legislativa de preservar o direito a intimidade, punindo a violação de segredo armazenados em computador, seja ele por qualquer meio. Merece destaque também, a tipificação de conduta de disseminação de vírus de computador, daquele que efetiva a criação, desenvolvimento ou inserção em computador com fins nocivos.

Embora aconteça a aprovação desse projeto, irão continuar algumas deficiências no ordenamento jurídico penal na área de informática, mas sem dúvida esse é o projeto que acaba por sanar grande parte dessas lacunas existentes, fazendo dele uma das melhores iniciativas surgidas. Assim afirma também Vladimir Aras (2002, p. 7):

> Não se pode deixar de lamentar a perda de oportunidade para uma regulamentação mais abrangente da cibercriminalidade, enfocando não só o direito material, mas também o direito processual. Como quer que seja, o projeto do deputado Luiz Piauhylino Filho, é uma das iniciativas de melhor qualidade em curso no Congresso Nacional. Espera-se que o projeto seja acolhido em breve no Plenário da Câmara dos Deputados e pelas comissões que o analisarão no Senado. Espera-se também que possuam ser acrescidas inovações, corrigidos os pequenos equívocos existentes e supridas as omissões, a fim de que o ordenamento jurídico nacional venha a fazer frente à ameaça cibernética.

Os crimes de computador devem ser normatizados dentro do Código Penal, com o a objetivo de harmonizar seus conceitos com os já preexistentes em nossa legislação substantiva, dando não só importância às condutas criminosas praticadas contra os computadores, mas cuidando em preservar os bens jurídicos comuns que venham a ser atingidos por condutas cometidas por meio do computador.

É evidente que a demora na aprovação dos projetos supracitados, bem como o próprio constante desenvolvimento da tecnologia informática, acabam por sucatear os mecanismos de repreensão penal criados, vez que todos os dias surgem novas maneiras de transpor os dispositivos de segurança eletrônica, aumentando ainda mais os crimes e danos nessa área da informática.

A título de informação, no dia 8 de maio de 2017 entrou em vigor a Lei de nº 13.441 que altera a Lei de nº 8.069/90, e que veio para “prever a infiltração de agentes de polícia na internet com o fim de investigar crimes contra a dignidade sexual de criança e de adolescente”, tem uma significância essa alteração, principalmente para crimes que envolvem pornografia com menores, mas ainda assim, é pouco para as alterações que são necessárias se fazer na legislação.

Vivemos em um mundo onde damos mais importância aos crimes praticados diariamente, como roubos, furtos, entre outros, e não é que eles não merecem tamanha atenção, porém os crimes cibernéticos têm ganhado espaço e vem acontecendo com bem mais frequência que antes, e a tendência sem que haja uma legislação eficaz é que esses números cresçam cada vez mais.

A criminalidade vem migrando para esse espaço cibernético, e são esses crimes que envolvem grandes fortunas, e podem atingir várias pessoas ao mesmo tempo em todo o mundo, sem nem que os criminosos tenham que sair do conforto das próprias casas, não podemos mais fechar os olhos quanto a essa situação.

Como exemplo desses crimes, podemos citar um bem recente, que foi o ataque cibernético do dia 12 de maio de 2017, que atingiu em torno 100 países, e foi considerado o

maior ataque da história. Esse ataque movimentou bilhões de reais, e conseguiu roubar 1,2 bilhões de *logins* e senhas, com esses roubos, os hackers passaram a pedir o resgate dessas contas as vítimas, e com isso movimentaram toda essa quantidade supracitada em dinheiro.

Esse ataque foi de grande repercussão mundial, mas existem inúmeros crimes cibernéticos nacionais e de grande repercussão, o que prova a necessidade da modificação dessa atual legislação onde há várias lacunas, e que sem essa alteração e atenção necessária para esses crimes, irão ficar cada dia mais comuns.

Conclui-se que o progresso na tecnologia da comunicação, principalmente com o surgimento da Internet, trouxe novas relações jurídicas com novos conflitos. O Direito vem mudando para conseguir exercer com a necessária rapidez e eficiência o controle social dessas inovações, tentando modificar as estruturas legislativas para lidar de forma adequada quanto a essas novas questões.

CONSIDERAÇÕES FINAIS

A tecnologia como um todo, e a Internet em conjunto, vem se desenvolvendo de forma muito acelerada, com isso, nossa sociedade acompanha essa evolução, impulsionando a globalização e trazendo para sociedade o poder da informação, a mudança de uma cultura escrita para uma cultura multimídia.

Esse desenvolvimento da internet trouxe consigo muitos benefícios e facilidades para nós quanto sociedade, seja para relações de trabalho, ou até mesmo entretenimento em geral, apesar de tudo isso, trouxe também alguns malefícios, como nossa vulnerabilidade nas inúmeras redes e meios de comunicação, acarretando uma nova criminalidade.

Tem ficado cada dia mais claro que a criminalidade tem migrado para essa área digital, fica evidente quando observamos a quantidade de crimes virtuais que vem acontecendo diariamente, crimes esses que conseguem alcançar vários países de uma vez, várias máquinas e pessoas em um só ‘*click*’.

Atualmente nossa dependência quanto a essa nova forma de comunicação, de trabalho, de acesso a informação e facilidade em acessar o que quer que seja nas redes, é o que nos faz sermos tão vulneráveis a esses crimes.

O ser humano mediante esse processo se encontrou, e ainda se encontra de forma livre. Livre para produzir várias realidades, assumir muitas faces, muitas delas irreais, com isso, surgiram novas relações jurídicas, novos conflitos e uma série infindável de controvérsias,

pois é justamente nesse ambiente livre que se encontra a maior influência para realização desses delitos.

Atualmente, a Internet está sendo vista como uma terra sem leis, sem regras, onde qualquer um pode fazer aquilo que bem entender, o que não é verdade. A Internet na mais é que a réplica virtual do nosso mundo material, sendo assim, aqueles que quebrarem regras, normas, deverão ser punidos.

A Internet hoje é a maior rede de comunicação existente, e quanto a isso vale ressaltar o grande avanço que ainda está por vir e a necessidade de uma regulamentação mais eficaz acerca da utilização da rede, o que hoje é um dos maiores paradigmas para o Direito, devido a quantidade de divergências e lacunas encontradas na legislação atual, assim como a dificuldade de coibir e julgar tais condutas criminosas.

São consideráveis e de grande importância as alterações que a legislação já sofreu até os dias de hoje, como foram expostas algumas no presente artigo, mas mesmo com essas alterações e devido ao crescente número de crimes que vem acontecendo, ainda há a necessidade de tipificação desses crimes, ainda há a escassez de legislação para essas condutas.

Devemos modificar a estrutura normativa vigente, que resulta incapaz de dar resposta aos novos delitos, sendo assim necessário incorporar a essa os elementos indispensáveis de informática, permitindo-nos obter a segurança jurídica necessária para seguirmos realizando avanços significativos no novo contexto a partir desta verdadeira revolução tecnológica.

A necessidade de incorporação dos conceitos de informática à legislação vigente não implica que devemos esquecer todo nosso sistema e começar do zero. Pelo contrário, nosso atual sistema encontra-se desenhado para suportar as modificações necessárias. O Brasil precisa adaptar a legislação penal para coibir essas ameaças às liberdades individuais e de interesse público, toda a legislação, deve reparar quanto a proteção dos bens jurídicos informáticos e de outros que possam ser ofendidos por meio de computadores.

A intenção maior com o presente artigo é alertar que aos poucos a sociedade está migrando para uma sociedade mais digital. É necessário o alerta aos profissionais do Direito que se adequem a nova realidade no que tange aos crimes cometidos por meio informático, assim como a necessidade de o poder público aprovar os projetos existentes, ainda em análise, para melhor aplicação das penas a essas condutas criminosas

ANEXOS

Anexo A - Projeto de Lei nº 76/00

Art. 1º Constitui crime de uso indevido da informática:
§1º contra a inviolabilidade de dados e sua comunicação:
I – a destruição de dados ou sistemas de computação, inclusive sua inutilização;
II – a apropriação de dados alheios ou de um sistema de computação devidamente patenteado;
III – o uso indevido de dados ou registros sem consentimento de seus titulares;
IV – a modificação, a supressão de dados ou adulteração de seu conteúdo;
V – a programação de instruções que produzam bloqueio geral no sistema ou que comprometam a sua confiabilidade;
Pena: detenção, de um a seis meses e multa.
§2º contra a propriedade e o patrimônio:
I – a retirada de informação privada contida em base de dados;
II – a alteração ou transferência de contas representativas de valores;
Pena: detenção, de um a dois anos e multa.
§3º contra honra e vida privada:
I – difusão de material injurioso por meio de mecanismos virtuais;
II – divulgação de informações sobre a intimidade das pessoa sem prévio consentimento;
Pena: detenção, de um a seis meses e multa.
§4º contra a vida e integridade física das pessoas:
I – o uso de mecanismos da informática para ativação de artefatos explosivos, causando danos, lesões ou homicídios;
II – a elaboração de sistema de computador vinculado a equipamento mecânico, consistindo-se em artefato explosivo;
Pena: reclusão, de um a seis anos e multa.
§5º contra o patrimônio fiscal:
I – alteração de base de dados habilitados para registro de operações tributárias;
II – evasão de tributos ou taxas derivadas de transações ‘virtuais’;
Pena: detenção, de um a dois anos e multa.
§6º contra a moral pública e opção sexual:
I – a corrupção de menores de idade;
II – divulgação de material pornográfico;
III – divulgação pública de sons, imagens ou informação contrária aos bons costumes.
Pena: reclusão, de um a seis anos e multa.
§7º contra segurança nacional:
I – a adulteração ou revelação de dados como reservados por questões de segurança nacional;
II – a intervenção nos sistemas de computadores que controlam o uso ou ativação de armamentos;
III – a indução a atos de subversão;
IV – a difusão de informação atentatória a soberania nacional
Pena: detenção, de um a dois anos e multa. (Disponível em <http://www.revistaseletronicas.fmu.br/index.php/FMUD/article/view/77/76>, acesso em 18 de maio de 2017.)

Anexo B – Projeto de Lei nº 84/99

Seção I
Dano a dado ou programa de computador
Art. 8º Apagar, destruir, modificar ou 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 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 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.
Parágrafo primeiro. 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.
Parágrafo segundo. 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 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 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 dados 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 de multa.
Parágrafo único. 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 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 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 V
Violação de segredo armazenado em computador, meio magnético, de natureza magnética, óptica ou similar
Art.12. Obter segredos, de industrias ou comércio, ou informações pessoais armazenadas em computador, rede de computadores, meio eletrônico de natureza magnética, óptica ou similar, de forma indevida ou não autorizada.
Pena: detenção, de um a três anos e multa.
Seção VI
Criação, desenvolvimento ou inserção em computador de dados ou programas de computador nocivos
Art. 13. Criar, desenvolver ou inserir, dado ou programa em computador ou rede de computadores, de forma indevida ou não autorizada com a finalidade de apagar, destruir, inutilizar ou modificar dado ou programa de computador ou de qualquer forma dificultar ou impossibilitar, total ou parcialmente, a utilização de computador ou rede de computadores.
Pena: detenção, de um a quatro anos e multa.
Parágrafo único. Se o crime é cometido:
I – contra 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 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 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 seis anos e multa.
Seção VII
Veiculação de pornografia através de rede de computadores
Art. 14. Oferecer serviço ou informação de caráter pornográfico, em rede de computadores, sem exibir, previamente, de forma facilmente visível e destacada, aviso sobre sua natureza, indicando o seu conteúdo e a inadequação para crianças ou adolescentes.
Pena: detenção, de um a três anos e multa. (Disponível em < http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=15028 >, acesso em 18 de maio de 2017.)

REFERÊNCIAS

ARAS, Vladimir. Crimes de informática – uma nova criminalidade. Disponível em: <http://www.informatica-juridica.com/trabajos/artigo_crimesinformaticos.asp>. Acesso em 06 de maio de 2017.

BASTOS, Celso Ribeiro. Curso de direito constitucional. 21ª ed. São Paulo: Saraiva, 2000.

_____. Comentários à Constituição do Brasil. 3ª ed. São Paulo: Saraiva, 2004.

BRASIL. Constituição, 1988.

_____.Lei nº 7.232, de 29 de outubro de 1984.

_____. Lei nº 7.646, de 18 de dezembro de 1987.

_____.Lei nº 9.609, de 19 de fevereiro de 1998.

_____. Lei nº 9.983, de 14 de julho de 2000.

_____.Lei nº 8.137, de 27 de dezembro de 1990.

_____.Lei nº 9.504, de 30 de setembro de 1997.

_____. Lei nº 13.441 de 08 de maio de 2017.

Câmara dos Deputados. Disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=15028>. Acesso em 18 de maio de 2017.

CORRÊA, Gustavo Testa. Aspectos jurídicos da Internet. 1ª Ed., São Paulo: Saraiva, 2000.

COSTA, Marco Aurélio Rodrigues da. Crimes de informática. Revista Eletrônica Jus Navengandi. (on-line). Disponível em: <http://www.jus.com.br/doutrina/crinfo.html> acesso em 24 de abril de 2017.

FERREIRA, Ivette Senise. A Criminalidade Informática. Direito & Internet: Aspectos Jurídicos Relevante. Bauru: Edipro, 2001.

GUIMARÃES, Emanuel Alberto Sperandio Garcia. Crimes Virtuais. 2013. Disponível em <http://docplayer.com.br/19354658-Crimes-virtuais-autor-emanuel-alberto-sperandio-garcia-gimenes-juiz-federal-substituto.html>, acesso em 21 de maio de 2017.

LEONARDI, M. Tutela da privacidade na internet. 2009. 344 f. Tese (Doutorado em Direito) – Faculdade de Direito da Universidade de São Paulo, São Paulo, 2009.

LÉVY, P. Trad. Carlos Irineu da Costa. São Paulo: Editora 34, 1999.

LIMA, Paulo Marco Ferreira. Crimes de computador e segurança computacional. 2ª ed., São Paulo: Atlas, 2011.

MUOIO, Arlete Figueiredo. Crimes na rede: o perigo que se esconde no computador. Companhia Ilimitada. São Paulo, 2006.

NETO, Mário Furlaneto; Guimarães, José Augusto Chaves. Crimes na Internet: elementos para uma reflexão sobre a ética informacional. Disponível em: <http://www.cjf.gov.br/revista/numero20/artigo9.pdf>. Acesso em: 25 de março de 2017.

Planalto. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L9609.htm>. Acesso em 18 de maio de 2017.

Revista Eletrônica FMU. Disponível em: <http://www.revistaseletronicas.fmu.br/index.php/FMUD/article/view/77/76>. Acesso em 18 de maio de 2017.

TIEDEMANN, Klaus. Criminalidade mediante Computadores. Barcelona, Ariel, 1985.

VALDEZ, Julio Tellez. Derecho Informático. México: Mc. Graw Hill, 1996.

VIANNA, Túlio Lima. Fundamentos de Direito Penal Informático. Rio de Janeiro: Forense, 2003.