BACHARELADO EM DIREITO

GISLAINE SIDOR SALVADOR

A CONDUTA CRIMINOSA NO AMBIENTE VIRTUAL E A RESPONSABILIDADE DOS PROVEDORES DE INTERNET

PITANGA – PARANÁ
2019

GISLAINE SIDOR SALVADOR

A CONDUTA CRIMINOSA NO AMBENTE VIRTUAL E A RESPONSABILIDADE DOS PROVEDORES DE INTERNET

Trabalho de Curso apresentado ao Curso de Direito, Área das Ciências sociais aplicadas, da Faculdade de Ensino Superior do Centro do Paraná-UCP, como requisito à obtenção de grau de Bacharel em Direito.
Professor Orientador: Rodolfo Carvalho Neves dos Santos

PITANGA - PARANÁ
2019

S182c

Salvador, Gislaine Sidor.
A conduta criminosa no ambiente virtual e a responsabilidade dos provedores de internet / Gislaine Sidor Salvador, 2019
56 f.

Orientador: Rodolfo Carvalho Neves dos Santos

Monografia (Graduação) – Faculdade de Ensino Superior do Centro do Paraná, Pitanga, 2019

1. Internet. 2. Crimes virtuais. I. Faculdade de Ensino Superior do Centro do Paraná. II. Título.

Feita pelo bibliotecário Eduardo Ramanauskas
CRB9 -1813

FACULDADES DO CENTRO DO PARANÁ
(42) 3646 5555 - Av. Universitária s/n Pitanga PR

Ensino por Ideal

FACULDADE DE ENSINO SUPERIOR DO CENTRO DO PARANÁ

TERMO DE APROVAÇÃO

GISLAINE SIDOR SALVADOR

"A CONDUTA CRIMINOSA NO AMBIENTE VIRTUAL E A RESPONSABILIDADE DOS PROVEDORES DE INTERNET"

Trabalho de Curso aprovado com nota 10 (dez) **como requisito parcial para obtenção do grau de Bacharel em Direito no Curso de Direito da Faculdade do Centro do Paraná, pela seguinte Banca Examinadora:**

Orientador (Presidente): **Prof. Rodolfo Carvalho Neves dos Santos**
Professor do Curso de Direito, Faculdade do Centro do Paraná

Membro 2: **Prof. Angelita Caroliny Vilela Salvador**
Professor do Curso de Direito, Faculdade do Centro do Paraná

Membro 3: **Prof. Alexandre Manfrinatti Viana Leite**
Professor do Curso de Direito, Faculdade do Centro do Paraná

Pitanga, 5 de dezembro de 2019

Dedico este trabalho primeiramente a Deus, por ter me amparado e me dado forças para concluir este projeto. E a meu marido por toda a paciência, apoio e incentivo durante essa trajetória.

AGRADECIMENTOS

Aos meus pais, meu irmão, meu marido e minhas avós, Leopoldina Israel Salvador *(in memoriam*) e Amélia Halachen Sidor, que com muito apoio e carinho, me encorajaram a concluir mais essa etapa da minha vida.

A todos os professores que me influenciaram nesta trajetória. E em especial, a meu orientador, com quem compartilhei todas as minhas angústias, desesperos e dúvidas a respeito do tema.

A todas as pessoas que de alguma forma me ajudaram a concluir mais essa etapa, como expressão de gratidão deixo aqui meus agradecimentos, pois sem eles a tão sonhada graduação não teria sido possível.

O sucesso nasce do querer, da determinação e persistência em se chegar a um objetivo. Mesmo não atingindo o alvo, quem busca e vence obstáculos, no mínimo fará coisas admiráveis.

José de Alencar.

RESUMO

SALVADOR, Gislaine Sidor. **A conduta criminosa no ambiente virtual e a responsabilidade dos provedores de internet.** 2019. 56 f. Monografia (Graduação). Faculdade de Ensino Superior do Centro do Paraná – UCP, Pitanga, 2019.

O presente trabalho busca abordar as condutas criminosas no ambiente virtual abrangendo ainda a responsabilidade civil daqueles que a promovem. Desta forma, importante salientar a evolução repentina sofrida pela comunicação humana por meio de tecnologias envoltas a internet. O simples passar dos meios virtuais se fazem presentes no cotidiano social, sendo impossível deparar-se com quem dele não faz uso. Infelizmente, abrange também aqueles que a dela se utilizam forma errônea, ou seja, utilizam os ambientes virtuais para cometeram ações delituosas. A legislação tem buscado acompanhar e se adequar a este ponto, criando leis para regulamentar tais ações e responsabilizar os culpados. Fato é que, a internet é um ambiente vasto e de difícil localização, pois não há limites para territorialidade ali. Desta forma, é importante pensar sob o aspecto dos que promovem a internet, sendo assim, fora criado a Lei para regulamentar os chamados provedores de internet, os quais, como se sabe, podem vir a ser responsabilizados civil por esses fatos, uma vez que a responsabilidade para tanto é subjetiva, ou seja, é necessário comprovar o dolo ou a culpa dos provedores de internet.

Palavras Chave: Internet. Lei. Crimes Virtuais. Responsabilidade Civil

ABSTRACT

SALVADOR, Gislaine Sidor. Criminal conduct in the virtual environment and the responsibility of internet providers. 2019. 56 f. Monograph (Graduation). College of Higher Education of Central Paraná - UCP, Pitanga, 2019.

This paper seeks to address criminal behavior in the virtual environment and also covers the civil liability of those who promote it. Thus, it is important to highlight the sudden evolution suffered by human communication through technologies involving the internet. The mere passing of virtual media is present in social daily life, being impossible to meet those who do not use it. Unfortunately, it also covers those who misuse it, that is, they use virtual environments to commit criminal actions. Legislation has sought to accompany and adapt to this point, creating laws to regulate such actions and hold the culprits accountable. Fact is, the internet is a vast environment and difficult to locate, because there are no limits to territoriality there. Thus, it is important to think about the aspect of those who promote the internet, so that a law was created to regulate the so-called internet providers, which, as we know, may be held civilly responsible for these facts, since The responsibility for doing so is subjective, ie it is necessary to prove the guile or guilt of the internet providers.

Keywords: Internet. Law. Virtual Crimes. Civil responsability.

SUMÁRIO

1 INTRODUÇÃO

Com a evolução humana, não seria de estranhar que os meios de comunicação passariam, de igual modo, por transformações. Os mecanismos utilizados no passado já não se fazem mais eficazes, como é possível perceber o desuso do envio de cartas como forma de enviar notícias a outra pessoa, a qual se encontra distante fisicamente. Isso ocorreu com os mais diversos sistemas de comunicação, desde o avento do telefone, do computador, da internet, etc.

Nos dias atuais, é praticamente impossível encontrar um indivíduo que não tenha acesso a rede mundial de computadores, isto porque, já não se mostra necessário possuir um computador com várias peças, nem mesmo ligado a uma infinidade de cabos, para que se possa ter acesso a internet e todas as suas facilidades. No entanto, não são apenas facilidades que se pode encontrar, mas sim sujeitos mal-intencionados, que se utilizam da internet e de seu vasto acesso para propagar e disseminar condutas criminosas nesse ambiente.

Assim, se torna necessário buscar uma compreensão acerca da responsabilidade dos provedores quanto a prática dessas condutas ilegais, uma vez que, o ambiente virtual, pode apresentar dificuldades para as investigações desses crimes. Diante dessa dificuldade, os criminosos virtuais por vezes não são descobertos e punidos como deveriam.

Para tanto, será utilizada a pesquisa bibliográfica, está baseada nas informações encontradas em livros, periódicos e artigos a respeito do assunto, as quais darão embasamento ao presente estudo.

1.1 JUSTIFICATIVA

Quando o assunto é crime praticado na seara virtual, é possível se encontrar diversos relatos de pessoas que passaram por situações em que pessoas mal-intencionadas as lesaram via internet. Muitas vezes, esses casos não têm solução, visto a dificuldade para a realização de investigação no ambiente online.

Por tal motivo, torna-se justificável a elaboração da presente pesquisa, visto que, o ambiente virtual possui inúmeras camadas, sendo uma delas, os chamados provedores de internet. Assim, faz-se preciso buscar uma compreensão a respeito da

responsabilidade desses provedores, quanto da prática de atividades criminosas em suas redes.

1.1.1 Problema de pesquisa

Qual a responsabilidade dos provedores nos crimes praticados pela internet?

1.2 OBJETIVOS

1.2.1 Objetivo geral

Compreender a responsabilidade dos provedores quanto aos crimes praticados na internet.

1.2.2 Objetivos específicos

Entender o que se denomina por ciberespaço;
Definir quais são os crimes praticados na internet;
Analisar a legislação nacional e internacional relacionadas ao direito digital;
Compreender a responsabilidade dos provedores.

2. O SURGIMENTO DO COMPUTADOR E DA INTERNET

2.1 A CHEGADA DO COMPUTADOR E DA INTERNET À REALIDADE HUMANA

Não há como negar que o ser humano evoluiu com o passar do tempo, buscando desde os primórdios, formas que viessem a facilitar a convivência em sociedade e sua comunicação, isto porque, para uma convivência social adequada, esta última se torna fundamental. Por isso, os inventos tecnológicos são cada vez mais aclamados por todos, pela facilidade e possibilidade de poder manter contato tanto com pessoas que estão por perto, quanto das que estão longe.

Assim, fora durante o século XX que se deu início as evoluções e avanços tecnológicos, os quais vieram a aperfeiçoar o quadro das comunicações. Exemplo disso é o computador, criado em 1943 sendo um dos meios de comunicação mais

utilizados ainda hoje, nas suas mais várias versões. Posteriormente, no ano de 1969, surgiu a internet, a qual foi se popularizando e evoluindo, tornando-se hoje algo indispensável na vida dos sujeitos (NIGRI, 2000).

Destarte, nos dias de hoje, não há como dissociar o computador e a internet da vida dos indivíduos, uma vez que traz diversas facilidades ao dia a dia, não apenas a comunicação em tempo real com qualquer parte do mundo, como na realização das mais diversas atividades da vida. Atualmente, é possível efetivar compras dos mais variados gêneros, realizar transações bancárias, estudar, dentre tantas outras, sem precisar sair de casa para isso (FELICIANO, 2000).

Ainda assim, o surgimento da internet não é como a maioria das pessoas imagina, não fora criada para essa finalidade, a de comunicação e uso de todos. Era sim, bastante restrita, e bastante modesta. A internet surgiu em 1963, criada pelo matemático Joseph Licklider, nos Estados Unidos. Sua principal função, nesse início, era a de ser uma ferramenta de comunicação capaz de percorrer diversos caminhos para que a mensagem chegasse ao seu destino. Em outras palavras, era necessário que as mensagens transmitidas chegassem de qualquer forma, mesmo que um caminho estivesse obstruído, deveria ser possível ser feito em outro, algo importante em momento de guerra fria (ROSA, 2002). No mesmo sentido:

> O Departamento de Defesa dos EUA apoiou uma pesquisa sobre comunicações e redes que poderiam sobreviver a uma destruição parcial, em caso de guerra nuclear. A intenção era difundi-la de tal forma que, se os EUA viessem a sofrer bombardeiros, tal rede permaneceria ativa, pois não existiria um sistema central e as informações poderiam trafegar por caminhos alternativos até chegar ao seu destinatário. Assim, em 1962, a ARPA encarregou a Brand Corporation (um conselho formado em 1948) de tal mister, que foi apresentar seu primeiro plano em 1967. Em 1969, a rede de comunicações militares foi batizada de ARPANET - rede da agência de projetos avançados de pesquisa (ROSA, 2002, p. 29).

Posteriormente, com maior precisão no fim do ano de 1972, o correio eletrônico é inventado (e-mail), por Ray Tolino, que até hoje é a aplicação mais utilizada na internet. No mesmo ano, veio a público a especificação do protocolo para transferência de arquivos (FTP), outra aplicação fundamental na internet. “Portanto, nesse ano, quem estivesse ligado a ARPANET já podia se logar como terminal em um servidor remoto, copiar arquivos e trocar mensagens [...]” (ROSA, 2002, p. 30).

Assim, a internet nada mais é que, uma rede de computadores, a qual é integrada por outras redes menores que se comunicam entre si, por meio dos

endereços lógicos (chamados de endereço de IP), onde são trocadas uma infinidade de informações. Do mesmo modo, não apenas existem informações a que todos podem ter acesso, disponíveis na rede, mas também informações pessoais, as quais deixam os usuários vulneráveis ao ataque dos chamados hackers e até mesmo de pessoas mal-intencionadas que visam o cometimento de crimes.

Conforme definição de Zanellato, “A Internet é um suporte (ou meio) que permite trocar correspondências, arquivos, ideias, comunicar em tempo real, fazer pesquisa documental ou utilizar serviços e comprar produtos” (2002.p. 173).

Dessa maneira, é possível perceber que, a internet não surgiu com o intuito da prática de crime por parte de alguns usuários, mas sim como um meio de comunicação, para apresentar facilidades aos seus usuários, como, por exemplo, a possibilidade de fazer compras em diversos sites nacionais ou internacionais, realizar transações bancarias, evitando suas filas e por vezes demora. Mas o que acontece, é a conduta delituosa por parte de algumas pessoas, as quais acabam por lesar os usuários, esses são os chamados crimes cibernéticos.

2.2 DEFINIÇÃO DO CHAMADO “CIBERESPAÇO”

No final dos anos 70 as redes de computadores se formaram, foram crescendo e evoluindo, enquanto a quantidade de usuários conectados também obteve um crescimento exorbitante, a internet começou a fazer parte da vida dessas pessoas. Com essa criação impôs um novo curso ao desenvolvimento técnico econômico, onde as tecnologias digitais surgiram e com isso a infraestrutura do ciberespaço, aquele que engloba a sociabilidade, organização, transação de cada indivíduo, a comunicação, a interação e nesse contesto o novo comércio da informação e do conhecimento. (LÉVY, 1999 p. 30).

Para Pierri Levy, (1999, p.39):

> O ciberespaço não compreende apenas materiais, informações e seres humanos, é também constituído e povoado por seres estranhos, meio textos meios máquinas, meio atores, meio cenários: os programas. Um programa, ou software, é uma lista bastante organizada de instruções codificadas, destinadas a fazer com que um ou mais processadores executem uma tarefa. Através dos circuitos que comandam, os programas interpretam dados, agem sobre informações, transformam outros programas, fazem funcionar computadores e redes, acionam máquinas físicas, viajam, reproduzem-se etc.

Portanto o ciberespaço pode ser muito mais que apenas informações e pessoas usufruindo de aplicativos de comunicação, podem ser programas que desempenham funções dentro da rede, trazendo a execução de tarefas e auxiliando o usuário a concluir os seus serviços.

De acordo com Lévy (1999, p.42) “Alguns programas calculam automaticamente o pagamento dos empregados de uma empresa, outros emitem faturas para clientes ou permitem o gerenciamento de estoques.”. Um editor de texto, por exemplo, permite alterar a redação, organizar os assuntos de forma simples e da maneira que foi desejada.

Os programas estão se tornando insubstituíveis, mais abertos a evolução de funções e personalização, tomando a posse das necessidades dos indivíduos dentro da sociedade.

O dizer “ciberespaço” teve a sua criação por Wiliam Gibson, no ano de 1984, em seu livro de ficção cientifica, o romance chama-se Neuromante. Tal termo refere-se ao universo do mundo virtual, descrito por ele como um campo de batalhas entre multinacionais, uma fronteira econômica e cultural e um palco para a ocorrência de conflitos mundiais. Já para Pierri Lévy (1999, p. 92) o ciberespaço é definido “como um espaço de comunicação aberto pela interconexão mundial dos computadores e das memórias dos computadores.”

Contudo, a cada instante a internet vai ganhando o acesso de várias pessoas e com isso variedades de equipamentos informáticos conectados, inserindo novas informações na rede, ampliando o ciberespaço e o tornando universal.

2.3 A INTERNET E SEUS ASPECTOS JURIDICOS

A internet em sua descrição técnica é uma grande rede que interliga vários computadores em todo o planeta, mas a resposta não é clara e muita menos íntegra, trazendo dúvidas em sua descrição e entendimento. Cada computador pode fornecer uma incontável quantidade de informações que dificilmente poderia ser obtida em um simples telefonema.

Segundo Paesani, (2013, p.12):

> Existem aspectos relevantes na Internet: a constatação de que se depara com uma gigantesca fonte de informações destinadas ao navegador da Internet, que é uma pessoa. Portanto, a rede telemática é uma oportunidade de encontro, de confronto, de troca de opiniões, de crescimento de relações interpessoais (global village), com todas as vantagens e os riscos das relações sociais.

O computador veio para despertar alguns atrasos, desconfianças e perplexidades no mundo do direito, sem contar as cautelas exigidas para lidar com tais fenômenos decorrentes do mal-uso. De acordo com Paesani (2013, p.13) “Podem ser evidenciadas duas reações típicas dos juristas: a *desconfiança,* característica do mundo fechado do Direito, quando confronta com as inovações tecnológicas; e a *defesa* – típica do Direito -, que se fecha e procura expelir o elemento perturbador para neutralizar as forças invasoras. ”

Contudo, a Constituição Federal de 1988, fundamenta a liberdade da forma de comunicação em seu artigo 220, deixando claro que a manifestação do pensamento sob a forma de processo ou veículo não sofrerá nenhuma restrição, deixando a sociedade livre para expressar seus dizeres e opiniões.

A atual evolução da informática e informação mostra a liberdade de acesso a qualquer rede, requerendo dos constitucionalistas, no plano de princípios, uma simples tomada de consciência, para que tal liberdade de acesso não deixe o usuário desprotegido.

Não há o que se questionar que na era digital que estamos vivenciando o instrumento de poder é inquestionavelmente a informação, vinculando a liberdade individual e a soberania do Estado que são medidas pelo acesso à informação e sua capacidade. A mudança flui constantemente e os avanços da tecnologia afetam diretamente as relações sociais, devendo o Direito o envolvimento necessário e costumeiro, se baseando em dinamismo e em estratégias jurídicas. Para Pinheiro (2013, p.75):

> O Direito Digital consiste na evolução do próprio Direito, abrangendo todos os princípios fundamentais e institutos que estão vigentes e são aplicados até hoje, assim como introduzindo novos institutos e elementos para o pensamento jurídico, em todas as suas áreas (Direito Civil, Direito Autoral, Direito Comercial, Direito Contratual, Direito Econômico, Direito Financeiro, Direito Tributário, Direito Penal, Direito Internacional etc.). Quem não lembra da resistência ao videocassete? Agora temos o Internet *Banking*, DVD, MP3, HDTV - *Hight Definition Television* -, TV Interativa, TV Digital, Banda Larga, WAP, VoIP. O que todas essas siglas significam no mundo jurídico atual? Significa que são os novos profissionais do Direito os responsáveis por garantir o direito à privacidade, a proteção do direito autoral, do direito de imagem, da propriedade intelectual, dos *royalties,* da segurança da informação, dos acordos e parcerias estratégicas, dos processos contra hackers e muito mais. Para isso, o Direito Digital deve ser entendido e estudado de modo a criar novos instrumentos capazes de atender a esses anseios.

A velocidade dessas transformações em meio a sociedade, pode se considerar uma barreira à legislação. Portanto qualquer lei que nasça para tratar de assuntos e institutos jurídicos dever ser genérica e flexível para sobrevier ao tempo e para poder atender diversas situações que podem surgir em um único caso.

Os operadores do direito deverão apurar questões jurídicas relacionadas a internet usando o bom senso, buscando sempre correlacionar o ordenamento jurídico com a parte técnica de cada situação. Com tais analises, sejam elas simples ou aprofundadas, possibilitarão um fácil entendimento das questões cotidianas de nossos tribunais, para que os futuros responsáveis do direito possam resolver esses conflitos de forma eficaz. Pois:

> Por ser algo muito novo, e por versar sobre rotinas falíveis, a Grande Rede constitui-se em um desafio, muito especial, para aquilo que visa pacificar e dirimir conflitos sociais, o direito. É nosso dever evitar que a ciência jurídica seja desgastada por algo responsável pelo seu desenvolvimento: a tecnologia.
> (CORRÊA, 2010, p. 133)

Segundo Pinheiro (2013, p.311):

> O Direito Digital traz a obrigação de atualização tecnológica não só para advogados e juízes, como para delegados, procuradores, investigadores, peritos e todos os demais participantes do processo. Tal mudança de postura é necessária para que possamos ter uma sociedade digital segura: caso contrário, coloca-se em risco o próprio ordenamento jurídico. O maior estimulo aos crimes virtuais é dada pela crença de que o meio digital é um ambiente marginal, um submundo em que a ilegalidade impera. Essa postura existe porque a sociedade não sente que o meio é suficientemente vigiado e que seus crimes são adequadamente punidos.

Perante toda a nova era da informação e preocupação com o crescimento inevitavelmente rápido, a Europa no ano de 2001, no dia 23 de novembro, apresenta o primeiro acordo internacional voltado aos crimes cometidos por meio da internet, o acordo ficou conhecido como a convenção de Budapeste, tem como objetivo segundo Paesani (2013, p.29): “estabelecer uma política comum entre os Estados – Membros mediante a adoção de uma legislação apropriada, que permita tratar o crime informático de maneira coordenada.” Se destinando a harmonização dos elementos que por sua vez são extremamente fundamentais a essas espécies de crimes com os ordenamentos dos estados e aplicar normas eficazes para inquéritos e perseguições dentro do mundo da informática.

2.4. OS CRIMES CIBERNETICOS

Como visto, a internet se disseminou de maneira rápida desde o seu surgimento, passando de mero canal para transmissão de mensagens no período da

guerra fria, para se tornar um dos itens indispensáveis a vida do ser humano. Nos dias de hoje, o acesso à internet é bastante facilitado, dado ao surgimento de computadores portáteis, dos celulares, das redes abertas que podem ser encontradas em alguns ambientes, sendo utilizado como mecanismo de marketing para os estabelecimentos comerciais, os quais destinam o acesso à internet aos seus clientes.

No entanto, ainda que seja a internet um mecanismo que vise facilitar a vida das pessoas, muitas vezes estas podem vir a ser alvo de outras pessoas mal-intencionadas, que possuem um conhecimento mais avançado acerca do tema e, utilizam-se desse conhecimento para acabar lesando os usuários que, muitas vezes, nem se dão conta de que estão sendo vítimas de criminosos virtuais, tendo seus dados pessoais roubados.

Assim, com a rápida expansão dos computadores e do acesso à internet, inclusive pelo uso dos próprios smartphones, surgiram também aqueles que se especializaram na linguagem da internet e usam desse conhecimento para o cometimento de crimes. Os crimes cometidos em ambiente virtual, são conhecidos como crimes cibernéticos. (CRESPO, 2011).

Dessa forma, é possível definir crime virtual como:

> [...] os crimes perpetrados neste ambiente se caracterizam pela ausência física do agente ativo, por isso, ficaram usualmente definidos como sendo crimes virtuais, ou seja, os delitos praticados por meio da internet são denominados de crimes virtuais, devido à ausência física de seus autores e seus asseclas (TERCEIRO, 2005, s/p).

Ou ainda:

> [...] o conceito de “delito informático” poderia ser talhado como aquela conduta típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, praticada por pessoa física ou jurídica, com o uso da informática, em ambiente de rede ou fora dele, e que ofenda, direta ou indiretamente, a segurança informática, que tem por elementos a integridade, a disponibilidade a confidencialidade. (ROSSINI, 2004, p. 110).

As definições de crimes virtuais ou cibernéticos, abarcam tanto os crimes quantos as contravenções penais delimitadas na legislação, não necessitando ser feito apenas em ambiente virtual, mas também toda e qualquer conduta que possua relações com sistemas informáticos.

O ambiente virtual facilita e, até mesmo incentiva, a prática de condutas criminosas, uma vez que dá a impressão de liberdade, pois muitas vezes são

marcados pelo anonimato, sem contar que, na internet não existem fronteiras, podendo as atividades criminosas ser praticadas por um brasileiro em qualquer lugar do mundo. No mais das vezes, as condutas praticadas são complexas, exigindo uma investigação e solução rápida, o que nem sempre é possível.

Além das dificuldades de investigação inerentes à Internet, a polícia também esbarra na questão da territorialidade, pois se o site está hospedado em um provedor estrangeiro, de um país como os Estados Unidos da América, onde é totalmente livre qualquer tipo de manifestação de opinião, então não é possível exigir a retirada do site ou das mensagens, nem mesmo processar o autor do crime. (PINHEIRO, 2010, p. 300/301).

Destarte, torna-se dificultoso dar agilidade a investigações realizadas em seara virtual, pois como visto, os sites por vezes não possuem hospedagem no território brasileiro. Bem como, alguns dos usuários que cometem crimes nesse espaço, sabem como esconder seus próprios rastros.

2.4.1 Espionagem eletrônica

Devido ao crescimento súbito do uso da internet, é essencial analisar em qual ramo da sociedade o crime de espionagem está inserido. Com a grande quantidade de pessoas e até mesmo empresas usufruindo das facilidades da era da informação, cresce também os casos de espionagem por essas vias eletrônicas, que muitas vezes são facilitadas pela falta de preparo com prevenção e proteção, não sendo nenhuma novidade devidos aos hábitos falhos estabelecidos em um nível de cultura que não exploram a segurança da informação. (PINHEIRO, 2013, p. 388/389).

Segundo Braga, (2015, p.8), as espionagens conhecidas como industriais:

> São empresas procurando se apoderar de segredos de fabricação dos produtos de outras para que possam fazer um igual, ou melhor, sem a necessidade de gastos de desenvolvimento, o que lhes dá uma vantagem competitiva, pois podem ter preços menores.

As empresas são as maiores vítimas do crime de espionagem eletrônica no Brasil, por viverem numa realidade, de certo modo, mais espionada e monitorada. Antes tal crime era tipificado devido a invasão de hackers, hoje em dia situação está mais evoluída, pode ser ocasionada devido à falta de cuidado de algum funcionário,

ou até mesmo intencionalmente, deixando o acesso livre ao indivíduo que foi designado a recolher informações, ou envia-las, podendo até mesmo exclui-las da rede.

As empresas devem investir em mais segurança, pois as ameaças internas são diversas e é difícil identifica-las rapidamente. Devem aplicar medidas de prevenção que são primordiais para o combate de tais ataques, como: ter um controle de acesso diário em conjunto com a máquina de trabalho, usar softwares de monitoramento e a regulamentação de bloqueios de portas USB. Acessar dados confidencias somente quando necessário também é uma forma eficiente de prevenir a espionagem.

Destaca-se como forma geral de fundamentação da punição dos delinquentes o artigo 154- A do Código Penal:

> Invadir dispositivo informático alheio, conectado ou não a rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
> Pena- detenção, de 3 (três) meses a 1 (um) ano, e multa.

Tal artigo é apresentado na Lei 12.737 de 2012, conhecida como a Lei Carolina Dieckmann, que julga também, os crimes cometidos na esfera virtual.

Para se proteger dos ataques, é essencial “uma estratégia que amarra aspectos técnicos e jurídicos, com uso de alguns *softwares* de monitoramento, com a devida adequação legal para que ele possa ser feito sem riscos para a empresa.” (PINHEIRO, 2013, p.393). Podendo ser utilizado também, restrições de determinadas mídias, bloquear portas usb, definir uma identidade de maquinas em acessos, não usar somente o login e senha, contudo, toda forma de prevenção é cabível, pois as invasões e ataques são frequentes.

Dessa forma, a espionagem eletrônica não é somente aquela praticada contra empresas, o delito ocorre também contra qualquer pessoa física, o que basta é apenas a obtenção de dados e informações de forma antiética e ilegal. Podendo ser por meio de escutas ambientais que são gravações sem o uso do telefone, feitas de forma clandestina ambientalmente e telefones grampeados.

2.4.2 Pornografia virtual

Atualmente já se tornou normal possuir equipamentos informáticos com câmeras, o que facilita extraordinariamente o compartilhamento de fotos e vídeos na rede de internet, podendo ser de seu próprio cotidiano, ou de outras pessoas, como amigos e familiares. Contudo, muitas vezes a divulgação dessas imagens não são autorizadas, acarretando transtornos, tanto para o causador, como para o lesado. Surge-se então o direito de imagem, garantia que está situada no artigo 5º, inciso X da Constituição Federal de 1988: “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 da sua violação.” (BRASIL, 1988).

Devido a facilidade para espalhar imagens nos dias atuais o assunto relacionado a pornografia não é tão atual assim, essa pratica vem acontecendo desde meados dos anos 80, onde acessavam conteúdos obscenos e de sexo explícito. Sendo que devido à época, somente pesquisadores e universitários tinham acesso a redes de internet.

A pornografia pode ser subdividida em 3 categorias, a primeira é aquela em que os indivíduos se interessavam em apenas fotografias eróticas, aquelas enviadas por e-mail, onde crivam uma lista de discussão que englobava apenas usuários adultos, mantendo sempre o sigilo e com o devido cuidado para que as fotos não causassem o constrangimento de nenhuma pessoa. (CORRÊA, p.65, 2010).

Devido ao crescimento da informação, surge a segunda categoria, onde a pornografia começou a se espalhar de forma on-line. Empresas se manifestaram usando essas imagens como forma de ganhar dinheiro, elas se tornaram as responsáveis pela administração desse conteúdo na rede, vendiam como serviços. Aqueles usuários que quisessem usufruir das imagens deveriam pagar valores determinados para essas empresas, as quais que só após o recebimento liberariam o acesso do conteúdo pornográfico.

Contudo a terceira categoria é a mais preocupante, engloba conteúdos pornográficos relacionados a pedofilia, imagens de mutilações explicitas e rituais feitos de forma macabra. Situações que tem a divulgação facilitada, devido ao acesso livre dos usuários e do poder de se esconder no anonimato dos autores, aproveitando da alta tecnologia para esconder essas ilicitudes. Os materiais pornográficos são espalhados por meio de comunidades fechadas, sem relação com empresas que cobram o serviço. (CORRÊA, p.65/66, 2010).

A Lei 13.718 de 2018 traz em seu artigo 218- C a punição cabível para aqueles que divulgarem cenas de sexo ou pornografia:

> 218 – C. Oferecer, trocar, disponibilizar, transmitir, vender ou expor à venda, distribuir, publicar ou divulgar, por qualquer meio - inclusive por meio de comunicação de massa ou sistema de informática ou telemática -, fotografia, vídeo ou outro registro audiovisual que contenha cena de estupro ou de estupro de vulnerável ou que faça apologia ou induza a sua prática, ou, sem o consentimento da vítima, cena de sexo, nudez ou pornografia:
> Pena - reclusão, de 1 (um) a 5 (cinco) anos, se o fato não constitui crime mais grave. (BRASIL, 2018).

Os provedores de internet também não escaparam da responsabilização:

> o Projeto de Lei n. 84/99, hoje Lei n. 12.735/2012, trazia em seu art. 22 obrigações para provedores do serviço de acesso à internet no Brasil.
> *Art. 22. O responsável pelo provimento de acesso a rede de computadores mundial, comercial ou do setor público, bem como os prestadores de serviço de conteúdo, são obrigados a:*
> *I – manter em ambiente controlado e de segurança, pelo prazo de 3 (três) anos, com o objetivo de provimento de investigação publica formalizada, os dados de endereçamento eletrônico da origem, destino, hora, data e a referência GMT da conexão efetuada por meio de rede de computadores e fornecê-los exclusivamente à autoridade investigatória e o Ministério Publico mediante requisição;*
> *II – Preservar imediatamente, após requisição, outras informações requisitadas em curso de investigação, respondendo civil e penalmente pela sua absoluta confidencialidade e inviolabilidade;*
> *III – informar, de maneira sigilosa, à autoridade policial ou judicial, informação em seu poder ou que tenha conhecimento e que contenha indícios da prática de crime sujeito a acionamento penal, cuja prática haja ocorrido no âmbito da rede de computadores sob sua responsabilidade, ressalvada a responsabilização administrativa, civil e penal da pessoa jurídica, sem exclusão das pessoas físicas, autoras, coautoras ou participes do mesmo fato.* (JESUS; MILAGRE, 2016, p.81).

Porém, essa disposição foi retirada do projeto de lei, antes mesmo de ser transferido para a Lei nª 12.735 de 2012, sem dúvida, seria uma das mais polêmicas, pois empunhava aos provedores que guardassem registros de acessos por 3 anos, e liberava as autoridades o acesso a essas informações, sem necessidades de nenhuma ordem judicial. Atualmente a Lei 12.965 de 2014, conhecida como o Marco Civil da Internet, traz em seu artigo 13 e seguintes parágrafos a responsabilidade dos provedores sobre a guarda dos registros de conexões:

> Art. 13. Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo,

> em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento.
> § 1º A responsabilidade pela manutenção dos registros de conexão não poderá ser transferida a terceiros.
> § 2º A autoridade policial ou administrativa ou o Ministério Público poderá requerer cautelarmente que os registros de conexão sejam guardados por prazo superior ao previsto no **caput**.
> § 3º Na hipótese do § 2º, a autoridade requerente terá o prazo de 60 (sessenta) dias, contados a partir do requerimento, para ingressar com o pedido de autorização judicial de acesso aos registros previstos no **caput**.
> § 4º O provedor responsável pela guarda dos registros deverá manter sigilo em relação ao requerimento previsto no § 2º, que perderá sua eficácia caso o pedido de autorização judicial seja indeferido ou não tenha sido protocolado no prazo previsto no § 3º.
> § 5º Em qualquer hipótese, a disponibilização ao requerente dos registros de que trata este artigo deverá ser precedida de autorização judicial, conforme disposto na Seção IV deste Capítulo.
> § 6º Na aplicação de sanções pelo descumprimento ao disposto neste artigo, serão considerados a natureza e a gravidade da infração, os danos dela resultantes, eventual vantagem auferida pelo infrator, as circunstâncias agravantes, os antecedentes do infrator e a reincidência. (BRASL, 2014).

A referida Lei traz a obrigatoriedade para o os provedores de internet de arquivar os registros de acesso por 1 ano, para que se futuramente houver algum crime, que seja causado através do serviço de internet desse fornecedor, possa ser identificado e tomado as medidas necessárias (JESUS; MILAGRE, 2016, p.82).

2.4.3 Fraudes eletrônicas

Devido à internet estar de tornando um meio de comunicação global e por ter seu acesso facilitado, surge o aparecimento de comerciantes e indivíduos querendo trocar e comprar produtos. Nessas situações, há aqueles que querem tirar vantagens e aproveitam o anonimato para enganar as outras pessoas, segundo Corrêa (2010, p.69/70): “O tipo fundamental de fraude dentro da Rede é o que envolve um falso comerciante e um consumidor com boas intenções, visando adquirir uma mercadoria oferecida à venda. ”

Para Pinheiro (2013, p.321):

> Toda fraude, independentemente da natureza, tem como pressuposto a utilização de um subterfugio para ludibriar a vítima, seja por meio da ação ou da omissão do agente, isto é, o fraudador fornece informação errônea á vitima ou ainda omite.

Portanto as fraudes no mundo virtual podem ser tanto na forma de vendas, serviços e produtos, como até mesmo dados de contas bancárias que são capturados por meio de e-mails falsos.

Segundo Gil (1997 apud Pinheiro, 2013, p.321) a fraude eletrônica é uma:

> ação intencional e prejudicial a um ativo intangível causada por procedimentos e informações (software e bancos de dados), de propriedade de pessoa física, ou jurídica, com o objetivo de alcançar benefício, ou satisfação psicológica, financeira e material.

Na maioria das vezes os criminosos se sobressaem em seus atos devido à falta de conhecimento dos usuários, os quais acabam acreditando em anúncios falsos na rede de internet e até mesmo acabam clicando em sites, links e e-mails não confiáveis, transferindo para o seu computador códigos maliciosos que abrem a porta para os delinquentes.

Em relação a aplicabilidade de penas o Código Penal em seu artigo 155 traz que: “Subtrair, para si ou outrem, coisa alheia móvel: Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa.” (BRASIL, 1940).

A melhor forma de prevenção contra as fraudes virtuais são os cuidados dos usuários:

> 1)Não abrir arquivos anexados, pois geralmente são programas executáveis que podem causar danos ao computador ou capturar informações confidenciais;
> 2)Não clicar em links para endereços da Internet, mesmo que conste o nome da empresa ou instituição, ou, ainda, mensagem como “clique aqui”:
> 3)Em caso de dúvidas sobre a origem e veracidade de determinada mensagem, procurar excluir o *e-mail* evitando executar seus anexos ou acessar os *links* em seu conteúdo:
> 4)Em casos de contaminação por vírus ou outro código malicioso, reformatar a máquina, reinstalar totalmente o sistema operacional e os aplicativos, evitando restaurar *backups* antigos:
> 5)Utilizar softwares de proteção (antivírus, anti – *spam*, anti – *spyware* e *firewall* pessoal) nos computadores de uso doméstico e corporativo, mantendo-os com a versão, assinaturas e configuração atualizadas;
> 6)Não emprestar sua senha de *e-mail*, de internet, de rede da empresa em hipótese alguma;
> 7)Duvidar do perfil de pessoas que se comunicam em ambientes não seguros e anônimos, como *Orkut, Messenger*, *blogs*, *chats*, evitando clicar e abrir imagens, principalmente;
> 8)Denunciar na delegacia de crimes eletrônicos, bem como também em sites especializados, como o www.denunciar.org.br. (PINHEIRO, 2013, p.324).

Todos estão expostos a fraudes eletrônicas, podendo em qualquer instante ter o computador invadido, senhas de bancos e outros arquivos subtraídos. Até mesmo

em sites de compras e vendas, sejam eles de roupas, acessórios, equipamentos informáticos, etc., pode haver criminosos apenas esperando para enganar o usuário desatento.

Portanto os crimes no mundo virtual crescem a cada dia, ainda há inúmeros delitos que não foram citadas. Os usuários estão propensos a passaram por essas situações a cada momento em que se conectarem à rede e tiverem o acesso ao vasto mundo da internet, podendo ter seus dados capturados como no caso das espionagens eletrônicas ou até mesmo ser vítima de fraude na tentativa de uma compra online.

As leis que regem e protegem as vítimas desses criminosos ainda estão em constante mudança e aprimoramento, pois como a criminalidade vem evoluindo o amparo legal também deve desenvolver-se e avançar para o mesmo caminho. Tanto as leis nacionais como as internacionais passam por esse mesmo processo e buscam a solução para a criminalidade na era digital.

3 LEGISLAÇÃO INTERNACIONAL E NACIONAL DO DIREITO DIGITAL

3.1 A RESPONSABILIDADE CIVL NA INTERNET

Nos crimes cometidos no mundo virtual o ato ilícito em si não pode ser caracterizado como o único fato gerador da responsabilidade civil. O que é levado em consideração para se ter um elemento mais construtivo é a ação causadora de determinado dano. Para o ordenamento civil a reparação desse prejuízo é o que realmente interessa. (PAESANI, 2013, p.59).

Aquele agressor que praticou o ato danoso deve responder por sua ação e se sujeitar as consequências que virão dessa atitude repudiosa. Como evidencia Lyra (1977, p.30):

> Quem pratica um ato, ou incorre numa omissão de que resulte dano, deve suportar as consequências do seu procedimento. Trata-se de uma regra elementar de equilíbrio social, na qual se resume, em verdade, o problema da responsabilidade. Vê-se, portanto, que a responsabilidade é um fenômeno social.

A responsabilidade civil busca reparar o dano que a vítima sofreu independentemente de culpa ou dolo, o que resultará sempre em perdas e danos

como o código civil dispõe. Para Paesani (2013, p. 59-60) “Um dos pressupostos da responsabilidade civil é a existência de um nexo causal entre o ato e dano por ele produzido. Sem essa relação de causalidade, não se admite a obrigação de indenizar.”

Essa denominação de responsabilidade vem de um fato histórico, onde somente existia a responsabilização penal envolvendo um comportamento que trouxesse prejuízo, “quem violava normas de comportamento e causava dano a alguém era punido penalmente. Surgiu depois a responsabilidade que não configura um crime e daí o nome responsabilidade civil.” (GLANZ, 2004).

Há duas etapas que auxiliam na identificação da responsabilidade, que vão do fato onde ocorreu o dano até a reparação do mesmo, sendo que para Glanz (2004, p.54) “a) a primeira é indicar o fato gerador da responsabilidade, ou seja, aquilo que dá direito a vítima de obterá reparação. b) a segunda etapa é indicar a pessoa que deve responder pelo dano.”

Portanto a ação criminosa, independente de culpa, mas desde que traga prejuízo a outem deve ser averiguada e o responsável punido, sendo a vítima indenizada e tendo como amparo legislações que façam a justiça vigorar.

A seguir será abordada a legislação de outros países, internacionais e nacionais em relação aos crimes cibernéticos, levando em consideração que o Direito Comparado é de tamanha importância, pois traz situações e exemplos de resoluções desses crimes, como outros países lidam com a criminalidade virtual e julgam os criminosos, buscando sempre amparar a sociedade e julgar de forma correta os delinquentes. Vale ressaltar que será observado a questão dos provedores de internet em relação a todo esse meio virtual, como são responsabilizados e que deveres devem seguir para agirem de forma legal.

3.2 DIREITO COMPARADO

A importância da pesquisa jurídica comparativa abre janela para a evolução do mundo jurídico e seus conhecimentos de forma bastante contributiva e marcante. O direito comparado proporciona até mesmo uma possível junção e aplicação de sistemas que realmente funcionam no mundo da informática. Segundo Ovídio (1984, p.166):

> O Direito Comparado preocupa-se, inicialmente, com a comparação de sistemas jurídicos particulares de diferentes países, destacando os seus pontos comuns ou distintivos, o que constitui a «macrocomparação». Por outro lado, pode limitar a sua atividade a comparação de determinados institutos jurídicos pertencentes a ordens jurídicas distintas, por exemplo, o contrato no Direito Brasileiro e no Direito Italiano, o que, representa a «microcomparação». A atividade juscomparativa foi, paulatinamente, ampliada no sentido de não limitar à comparação de normas jurídicas, mas, também, de ciências jurídicas, procurando captar os diferentes tratamentos conceituais do fenômeno jurídico e as relações existentes entre o Direito e a realidade social subjacente.

Destarte o presente trabalho tem como função apresentar e analisar características das legislações de determinados países levando em consideração pontos positivos que de certo modo poderiam ser aplicados no Direito Brasileiro, ou até mesmo características que são idênticas e amparam a sociedade dos crimes digitais.

3.2.1 Na Itália

Na Itália a Lei 59 de 15 de março de 1997, traz um rol de artigos referenciados ao mundo da informática, focam em grande proporção na segurança de documentos produzidos por meio de computadores.

Segundo Luca e Filho (2001, p.81/82):

> Na Itália, como já mencionado em linhas anteriores, existe um Decreto da Presidência da República dispondo sobre: as definições [art. 1º]; o documento informático [art. 2º]; os requisitos do documento informático [art. 3º]; a forma escrita [art. 4º]; a eficácia probatória do documento informático [art. 5º]; cópia dos atos e documentos [art. 6º]; deposito da chave privada [art. 7º] ; certificação[art. 8º]; obrigações do usuário e do certificar [art. 9º]; assinatura digital [art. 10º]; contratos estipulados com instrumentos informáticos ou pela via telemática [art. 11º]; transmissão do documento [art. 12º]; sigilo da correspondência transmitida vis telemática [art. 13º]; pagamentos informatizados [art. 14º]; livros e escrituração [art. 15º]; assinatura digital autenticada[art. 16º]; chave da codificação da Administração Pública [art. 17º]; documentos informáticos da Administração Pública [art. 18º]; subscrição dos documentos informáticos da Administração Pública [art. 19º]; desenvolvimento dos sistemas informáticos da Administração Pública [art. 20º]; gestão informática do fluxo documental [art. 21º]; e formulários módulos e questionários [art. 22º].

Em relação aos estudos é necessário observar a evolução para Decreto 513 de 10 de novembro de 1997, que é considerado um dos documentos mais importantes

para a Europa, o qual deveria ser referenciado como paradigma na elaboração de muitas outras legislações. (LUCA; FILHO, 2001, p.82).

Mas recentemente, o contrato de forma on-line e as definições de cada documento estão especificados no Decreto 445 de 28 de dezembro de 2000. (ITALIA, 2000).

Em relação a todo o contexto das legislações italianas, buscam guardar sempre todo e qualquer registro de acesso à internet. Os provedores de internet devem, na assinatura do contrato, deixar esclarecido para o cliente que, como forma de proteção, deixarão armazenados os dados de e-mail, nome, localização pelo tempo de 12 meses, conforme a lei determina e liberando o acesso total das informações quando a via judicial solicitar.

Já em relação a direito civil ou penal consegue o usuário livrar-se da responsabilidade de certo ato criminoso se conseguir provar que o conteúdo não é de sua autoria. Agora em relação a publicações no anonimato, que na atualidade se tornou muito fácil, a legislação italiana determina que não há previsão legal, mas sempre há a possibilidade de o indivíduo usar apelidos e no cadastro de contas online usar algum nome ou sobrenome que facilidade a identificação. Em tais situações o provedor de internet deve investigar e identificar a existência do indivíduo e nome verdadeiro usando registro de identidade ou algum cadastro social. (REGULAMENTAÇÃO, 2010).

.3.2.1.1 Convenção de Budapeste

A Convenção de Budapeste conhecida como Convenção sobre o Cibercrime Surgiu na Hungria, em 2001 e entrou em vigor em 2004, criada pelo Conselho Europeu. A Convenção tipifica vários crimes cometidos por meio de equipamentos informáticos. Segundo a tradução do texto da Convenção feita pelo Diário da República (2009, p. 6354/6378) que é o jornal oficial da República Portuguesa:

> Convictos de que a presente Convenção é necessária para impedir os atos praticados contra a confidencialidade, integridade e disponibilidade de sistemas informáticos, de redes e de dados informáticos, bem como a utilização fraudulenta desses sistemas, redes e dados, prevendo a criminalização desses comportamentos, tal como se encontram descritos na presente Convenção, e a criação de competências suficientes para combater eficazmente essas infracções, facilitando a detecção, a investigação e a ação penal relativamente às referidas infracções, tanto ao nível nacional como ao

> nível internacional, e adoptando medidas que visem uma cooperação internacional rápida e fiável;

A Convenção de Budapeste é um dos instrumentos jurídicos que visa, por meio da junção da cooperação internacional, combater os crimes cometidos por meio de equipamentos informáticos e do crime de pornografia infantil, tratando também da segurança dentro da rede de computadores, direitos autorais e de fraude. Entretanto a convenção não foi elaborada somente para tipificar delitos, mas para impor normas de processo penal e conciliar procedimentos internacionais chegando em acordos que englobam a tecnologia atual. (BOITEUX, 2004, p. 170).

Entretanto o Brasil não faz parte dessa Convenção sobre crimes virtuais, mas isso não significa que não tenha capacidade para participar, é uma situação que deva ser analisada e estudada, pois as leis brasileiras são aplicadas de formas bem limitadas, sendo de uso apenas dentro do território brasileiro, enquanto a convenção traz uma grande contribuição internacional eficaz contra os crimes cibernéticos. Como citado por Cidrão, Muniz, Alves (2018, p.78):

> Destaca-se que o Brasil não é signatário da Convenção de Budapeste sobre cibercrimes. Fato este que merece atenção, pois, ainda que se aponte lacunas na respectiva Convenção, vislumbra-se total capacidade técnica e jurídica nacional para recepcionar o Tratado. A importância desta análise para o direito brasileiro refere-se ao fato de que os crimes praticados pela Internet, sejam eles tradicionais ou não, estão em conflito direto com a competência e atuação territorial das autoridades nacionais, uma vez que as leis nacionais têm sua aplicação limitada a um território específico e são totalmente ineficientes no que tange à violação aos direitos humanos e às liberdades individuais. Desse modo, somente um instrumento internacional poderia ter eficácia na luta contra estes crimes. Além da compatibilidade entre o ordenamento brasileiro e a referida convenção, a escassez de leis específicas sobre o tema dentro do Brasil tem dificultado a aplicação da justiça nos casos concretos. Possivelmente, essa realidade seria alterada caso o Brasil se tornasse signatário, já que a cooperação internacional estaria a seu favor.

O Brasil poderia participar da convenção mediante convite do Conselho da Europa segundo o artigo 37º, onde podem “convidar qualquer Estado não membro do Conselho que não tenha participado na elaboração da Convenção a aderir à presente Convenção.” (CONVENÇÃO DE BUDAPESTE, 2001). Enquanto isso a legislação de crimes virtuais no Brasil passa por dificuldade de aplicação. E a escassez de leis para combater esses delitos ainda é muito grande, com a participação e aplicação das normas impostas na convenção a justiça teria mais meios de realmente punir os delinquentes.

3.2.2 Estados Unidos

No mundo da internet os Estados Unidos também se preparam e previnem- se dos delituosos virtuais.

Se preocupam também com documentos digitais, contratos eletrônicos, entre outros meios muito utilizados. Observa-se que em vários Estados do país já legislam sobre essa matéria, como exemplo o Estado de Utah, que tem como o código §§ 46-3-101 a 46-3-504, onde trocaram a assinatura comum por uma totalmente digital, com um certificado que a segure é claro. Mas a Lei do Estado de Utah pode ser considerada uma das mais completas em relação as assinaturas digitais.

Segundo Lucca e Filho (2001, p.77):

> O Título I cuida das normas de interpretação e das definições.
> No que se refere aos objetivos e a interpretação, fica estabelecido que a exegese do capitulo será feita em coerência com o que for considerado razoável em certas circunstancias, tendo em vista os seguintes propósitos:
> 1. Facilitar as transações mediante mensagens eletrônicas confiáveis;
> 2. Reduzir ao mínimo a possibilidade de forjar assinaturas digitais e a ocorrência de fraude nas transações eletrônicas;
> 3. Instrumentalizar juridicamente a incorporação das normas pertinentes, tais como a X.509 da União Internacional de Telecomunicações (antigo comitê Consultor de telégrafos e telefones, o CCITT); e
> 4. Estabelecer, em coordenação com diversos Estados, normas uniformes relativas a autenticação e a confiabilidade das mensagens eletrônicas.

Já em relação ao capítulo das definições observa-se que a Lei apresenta numerosos conceitos explicando minuciosamente cada um, coisa que não estamos acostumados a observar nas legislações brasileiras. Existem, no capitulo 39, definições em relação aos certificados, registros, assinatura digital, sobre usar uma chave privada de segurança, punição adequada para aquele que falsificar uma assinatura digital, sobre verificação de certificado, entre outras. (LUCCA; FILHO, 2001, p. 78).

Em relação aos certificados vejamos as definições da forma exemplificada de Lucca e Filho (2001, p.77):

> Certificado é o registro baseado em computador que: 1. Identifica a autoridade certificadora que o emite; 2. Nomeia ou identifica quem o subscreve; 3. Contém a chave pública de quem o subscreve; 4. Está assinado digitalmente pela autoridade certificadora que o emite. Autoridade certificadora é a pessoa que emite um certificado.

O Título II da lei traz o rol dos cuidados, regularizando as autoridades que são as responsáveis pelos certificados. Já o Título III trata sobre a obrigação dessas autoridades certificadoras, nessa parte são determinadas as regras em relação a emissão dos certificados e também regras de revogação ou suspenção.

Por fim, o Título IV da Lei cuida da assinatura digital e seus efeitos que são quase os mesmos efeitos legais da assinatura em papel físico. (LUCCA; FILHO, 2001, p. 78/79).

Entretanto não somente Utah estabeleceu a lei sobre os usuários da rede de computadores, a Florida no ano de 1978 foi considerada o primeiro Estado a formular leis relacionadas a informática. Na atualidade quase todos os Estados Norte-Americanos possuem suas legislações em relação aos acessos ilícitos, manipulação de dados, e possessão de informações protegidas. Segundo Corrêa (2010, p85):

> Naquele país, as leis relacionadas ao abuso de computadores são divididas em duas categorias: as leis estaduais, responsáveis por cobrir os casos e situações relevantes às preocupações e experiências particulares de cada Estado, e as leis federais, que abrangem crimes com impacto superior, como, por exemplo, o movimento de fundos e materiais ilícitos entre Estados.

A Lei considerada a mais importante do Estados Unidos em relação aos crimes virtuais foi promulgada no ano de 1986 e se chama *Computer Fraud and Abuse Act.* Que significa Lei de Fraudes e Abusos por Computador. O que levou o governo americano a aprovação da referida lei foi a preocupação com a destruição e vandalismo digital nos computadores militares e de acesso do governo. Tanto que a lei tipifica atividades em várias categorias, tendo como finalidade esclarecer ao sujeito que praticou o ato que aquela atividade era ilegal e está passível a receber uma penalização. As categorias são:

> - acessar sistemas sem autorização, com o objetivo de obter informação governamental restrita;
> - acessar sistemas sem autorização, com o objetivo de obter informação financeira restrita;
> - ter a intenção de acessar, sem autorização, qualquer computador do governo, ou qualquer computador utilizado pelo governo;
> - Transmissão de dados através de computador objetivando fins ilícitos. (CORRÊA, 2010, p.86).

É fácil a identificação da supremacia da lei norte-americana, a qual rege os interesses particulares de cada estado, pois cada categoria se preocupa com os computadores que pertencem ao governo. Em contrário a essa nação observa-se o

Reino Unido, o qual impôs que não haverá nenhuma distinção entre lei estadual e federal, sendo que todas as legislações são aplicáveis de forma igual em todo o território, já a Lei de Abuso por Computadores, em inglês pronuncia-se: O Computer Misuse Act. Foi criada pelo Reino Unido e traz 3 definições de situações ilícitas que os criminosos estão suscetíveis a receber:

> Seção 1 – ofensa que envolve o ganho não autorizado de acesso a um computador, ou a uma parte do computador, sobre o qual a pessoa não tenha autoridade. Essa é a mais geral das especificações, podendo ser enquadradas desde *Hackers* até tentativas de localizar informações específicas dentro de determinado sistema.
> Seção 2 – ofensa que envolve o acesso não autorizado a computadores, com a intenção de violar a lei posteriormente, como publicar a informação obtida (para extorsão, por exemplo) ou usar os dados para quebrar a segurança de outros sistemas.
> Seção 3 – ofensa que envolve o acesso não autorizado a computadores, com a intenção de modificar os seus dados, obstando o seu funcionamento ou acesso de usuário autorizado. (CORRÊA, 2010, p.87).

Portando observa-se que os três itens desta lei conseguem abranger vários crimes virtuais, como por exemplo a publicação de material inerente ou protegido por direitos autorais, assim como espalhar vírus e outros ataques tipificados como maléficos.

Em relação aos crimes de pornografia na internet e informações terroristas, o ex-presidente Bill Clinton, dos Estados Unidos, no ano de 1996, promulgou uma lei relacionada aos meios informáticos, onde teve a participação do Senador James Exon do Estado de Nebraska, chamada de "*Communication decency act*", Lei de decência nas comunicações. A qual veio para controlar ataques terroristas e a pornografia dentro do mundo virtual, um problema que foi encontrado pela nação dos Estados Unidos logo após o ataque em Oklahoma. (CORRÊA, 2010, p. 89).

Segundo Corrêa (2010, p.89), "A mídia impressa e televisiva identificou que um grande volume de informações dentro da internet ensinava a fazer bombas caseiras, conduzir campanhas terroristas e disseminar pornografia infantil". Devido à grande enxurrada de material indecente na internet forçou a introdução de severas restrições para essas transmissões, uma delas conhecida como Exon Bill, foi voltada aos provedores de internet que fizessem o monitoramento dos materiais disponíveis na rede e controlassem os arquivos e postagens indecentes. A multa para aqueles que ousassem desobedecer a lei ficou estipulada em 250 milhões de dólares e podendo pegar até 2 anos de prisão. Assim começou uma grande guerra judicial entre o

governo e os provedores de acesso, a discussão era voltada a constitucionalidade de política imposta pelo governo, devido às restrições e penas que foram impostas aos provedores. (CORRÊA, 2010, p.89).

Já os argumentos de defesa dos provedores de acesso eram muito concretos e realistas, afirmavam que o volume de dados que fluía na internet era exorbitante e a verificação de cada material para averiguar a decência era completamente impossível. Não somente isso, debatiam também sobre o direito individual de cada usuário, sendo que os adultos tinham seu direito de escolher o que ver e os menores em relação aos materiais obscenos deveriam ficar a cuidados dos pais para que empunhassem o controle dos materiais impróprios. (CORRÊA, 2010, p.89/90).

Após uma enorme discussão entre os provedores de acesso e o governo com a Exon Bill, a inconstitucionalidade da lei foi declarada por 3 juízes federais. Alegaram que a lei feria o princípio fundamental da nação norte-americana. Onde os juízes proferiram: “(...) por ser a maior forma de expressão já desenvolvida, a Internet merece a maior proteção possível contra a intromissão governamental (...)”. (CORRÊA, 2010, p.89).

Enfim, a decisão da Suprema Corte dos Estados Unidos foi de que os provedores de internet não seriam responsabilizados por qualquer material impróprio ou difamatório que fosse divulgado na esfera virtual.

3.2.3 China

A nação chinesa possui legislação sobre os crimes cometidos na esfera virtual, inclusive o direito Chinês tem uma enorme completude e competência. As autoridades da China até mesmo ironizam dizendo que não se deve a avaliar a sociedade chinesa pelo seu tamanho ocidental. (PAESANI, 2013, p. 26).

O governo tem normas de controle sobre os conteúdos divulgados na internet, alegam que a rede é muito utilizada para filtrar informações danosas e segredos que são de exclusividade do Estado. As regras estabelecidas definem vários crimes, como por exemplo, o estimulo a violência e material pornográfico. A regulamentação ainda prevê penas que não foram especificadas e multas para aqueles que ousarem desobedecer às normas, onde até os provedores de internet estão sujeitos a penalidades. (PAESANI, 2013, p. 26).

O texto de regulamentação contém 25 artigos e foi aprovada pelo Conselho Estadual no dia 12 de dezembro de 1998, porém entrou em vigor somente no dia 30 daquele mês. Para Jesus e Milagre (2016, p.67) houve a divulgação de mais uma Lei no ano de 2011:

> A lei denominada *Computer Information Network and Internet Security, Protection and Management Regulations* foi publicada em dezembro de 2011. Em alguns tipos penais, pode haver até mesmo o cancelamento da conta do usuário junto ao Provedor de Acesso à Internet. Os tipos previstos na legislação criminal chinesa incluem a sabotagem, o acesso indevido, a alteração de dados e o uso de computadores para fraudes, corrupção, criação e propagação de vírus, desvio de fundos públicos, roubo, roubo de segredos do Estado, dentre outros.

Mas voltando a análise do texto legal de 1998, um artigo de forma oportuna foi introduzido, com a determinação de que a internet de forma alguma poderia ser utilizada para dividir o país, levando em consideração os movimentos do Tibete e da região muçulmana que foram caracterizados como separatistas. Outro dispositivo também implantado trata da divulgação de informações do governo central de forma difamatória, pois o número gigantesco de opositores criticava o regime de Pequim por meio das páginas na rede de internet. Para Paesani (2013, p.27):

> Os legisladores alegam que a Internet é um importante instrumento para incrementar as relações culturais e cientificas da China com o resto do mundo, mas acrescentam que ela também tem trazido problemas de segurança e de difusão de informações, prejudiciais à formação do povo. Concluem afirmando que o controle da rede faz parte de uma campanha que o governo promove para acelerar o processo de modernização do país.

Existe um programa de monitoramento na China que é denominado como a *Grande Muralha Corta-Fogo,* este programa filtra redes sociais e outros sites na internet, impedindo os cidadãos Chineses de receberem qualquer notícia e opiniões vindas da linha de política do país, porém com a grande evolução da era cibernética uma grande rede de especialistas encontrou meios de romper com essa barreira e terem o acesso livre a informações como essas do governo.

> Os chamados *hacktivistas* são guerrilheiros eletrônicos com um programa que vai desde a eliminação da censura até a franca sabotagem. Afirmam ter adulterado sites na *web* do governo, derrubando muralhas eletrônicas e desativando um satélite. "*Somos especialistas em informática e, acima disso, gostamos da ideia de liberdade de expressão; estamos destinados a destruir a sistema chinês de censura pela internet, pois acreditamos que o povo*

> *chinês tem o direito de liberdade de expressão"*, disse o editor chinês da VIP *Reference*, uma revista eletrônica com sede em Washington que é enviada por *e-mail* (correio eletrônico) para a China. (PAESANI, 2013, p.27).

Como resultado de todo esse transtorno, Pequim convocou esquadrões da polícia especializada em internet para vigiar o ciberespaço. Porém tudo isso deixou-os mais crente que seria muito mais fácil controlar uma multidão do que ceifar a internet. (PAESANI, 2013, p.27).

Portanto observa-se a grande preocupação da China em relação a censura, buscam de forma extremamente eficaz regular a navegação e acesso dos usuários. Evitando que se espalhe tanto informações do governo, como materiais impróprios e encorajamento a violência.

3.3 LEGISLAÇÃO NACIONAL DOS CRIMES VIRTUAIS

A punição e prevenção dos crimes sempre se concretizará através das leis, elas são essenciais para a organização da sociedade. Independentemente se os delitos forem ocasionados no mundo físico ou virtual. Segundo Corrêa (2010 apud Kelsen, 1991, p.4): "O Direito é uma ordem normativa de conduta humana, ou seja, um sistema de normas que regulam o comportamento humano."

As leis possibilitam a pacificação social, visando a conduta do ser humano dentro de determinados princípios. É por meios como este que as atividades destruidoras e imorais são prevenidas, tornando a sociedade pacífica onde os integrantes podem atuar de forma mais segura, pois se não houvesse limites para se respeitar seria extremamente difícil garantir que a esfera pessoal do outro não fosse invadida. Para Corrêa (2010, p.80): "Especificamente, na Era da Informação, com os consequentes "crimes" digitais, a existência de limites é importantíssima. A capacidade e a tecnologia dos computadores crescem na medida em que se torna difícil regulamentar as implicações advindas desse avanço."

Tanto no Brasil como em outros países, existe legislação que coíbe os crimes cibernéticos. Porém a cada dia que passa surgem condutas criminosas cada vez menos óbvias, e as leis existentes acabam não preenchendo as lacunas de uma maneira totalmente eficaz. Leva-se em consideração que a maioria dos crimes já são pré-existentes no ordenamento jurídico brasileiro, sendo que fraude sempre será uma fraude, o furto de componentes não deixará de ser classificado como um furto. A

questão de lavagem de dinheiro, de certo modo, nunca deixará de ser um crime. Condutas como estas estão previstas, mas não é neste ponto em que as dificuldades residem. Elas estão nos surgimentos dos crimes novos, específicos e mais complexos, onde o controle passa a ser de extrema importância. Como exemplo, a criação de vírus ou de um ataque de hacker, assim como pornografia infantil e outras práticas de vandalismo que culminam na esfera virtual. (CORRÊA, 2010, p.81).

Como exemplo de uma grande dificuldade de punição dos hackers pode-se citar o ocorrido na Agência Espacial Norte-Americana (NASA). Onde brasileiros tentaram romper barreiras de proteção e entrar nos arquivos salvos em computadores da agência, porém não obtiveram total sucesso. Entretanto, a polícia encontra uma grande dificuldade e barreiras invencíveis para concluir a punição, porque mesmo já tendo alguns suspeitos, não poderiam indicia-los devido o crime não estar previsto em lei brasileira. (PAESANI, 2001, p.29).

Em relação ao direito penal e civil na era virtual podemos observar que o Brasil ainda está de fato bem atrasado, pois levando em consideração alguns Projetos de Lei que foram propostas pelo Congresso está efetivamente longe de entender a problemática cibernética e resolver esses conflitos.

> E em se tratado de crimes informáticos, deve-se registrar que as características da Internet não permitiram tão somente o desenvolvimento da comunicação, mas serviram de ambiente para o crescimento de crimes de informática, estes amparados pela sensação de anonimato e pouca possibilidade de punição, considerando que, até recentemente, tudo que o Brasil tinha em termos legislativos no que diz respeito a crimes informáticos era a Lei n. 9.983/2000, que poucos artigos acrescentou ao Código Penal, aplicáveis, via de regra, a funcionários públicos. No mundo, o crime virtual já é o terceiro em prejuízo, apenas atrás das drogas e da falsificação. (JESUS; MILAGRE, 2016, p.71).

No Brasil o Decreto – Lei 2848 de 1940, o Código Penal, faz frente a uma grande quantidade dos crimes cibernéticos. Porém a necessidade de legislação especifica é questionada.

Para Jesus e Milagre (2016, p.71):

> Para muitos autores, o foco do Direito Penal é a proteção de bens jurídicos individuais, não sendo coerente a aplicação penal de interesses supraindividuais. Em tese, a conduta delitiva deveria lesionar bens pessoais e não direitos. Na era digital, porém, acentua-se a tutela penal dos direitos difusos. Passamos a considerar o objetivo da Lei Penal com o escopo de proteger a segurança e possibilitar a vida da sociedade digital. A globalização vai criando ou “inventando” novos riscos, e o Direito Penal segue avançando,

> desconsiderando princípios consagrados, como a intervenção mínima. Pune-se o risco aos bens jurídicos ameaçados pela informática ou pelo uso inadvertido e criminoso desta.

Além disso vários projetos de lei tiveram a sua tramitação dentro do Congresso Nacional, mas apenas alguns tiveram a sua efetividade e outros converteram-se em diferentes leis. As quais serão analisadas dentro deste capitulo.

3.3.1 Lei 12.737 de 2012, conhecida como a “Lei Carolina Dieckmann”.

Tudo se inicia com o projeto de Lei nº 84 do ano de 1999, apresentado pelo Deputado Luiz Piauhylino em 24 de fevereiro. Esse projeto percorreu tramitando por 13 anos recebendo substitutivos e reunindo projetos que tratavam de certos temas semelhantes. (CORRÊA, 2010, p.109).

> Foi também apelidado de “AI-5 digital” e de “Lei Azeredo”, eis que o político brasileiro Eduardo Azeredo foi o relator do Projeto em diversas fases e também
> um dos defensores da sua aprovação. Na justificativa do Projeto, consta: *Não podemos permitir que pela falta de lei, que regule os crimes de informática, pessoas inescrupulosas continuem usando computadores e suas redes para propósitos escusos e criminosos. Daí a necessidade de uma lei que defina os crimes cometidos na rede de informática e suas respectivas penas*. (JESUS; MILAGRE, 2016, p.73).

A referida lei no ano de seu início possuía apenas 18 artigos. Após tramitação legislativa converteu-se na Lei 12.735 de 2012, que continha apenas 4 artigos, que com certeza, trouxe fortes rejeitos e especulações, pois ativistas da época protestavam contra a lei que segundo eles trazia a punição para aquele indivíduo que era apenas internauta. A lei nº84/99 foi de fato desconfigurada e vigorou apenas a lei nº 12.735/2012. (JESUS; MILAGRE, 2016, p.73).

Antes disso, nos anos de 2010 e 2011 enquanto a discussão se estendia em relação ao Projeto de Lei 84/99, os ataques em sites do governo e exposição de dados privados eram constantes, os ciberativistas mostravam suas garras na forma de invasão e indisponibilizando vários serviços informáticos. A partir dali entenderam que o projeto de lei era inviável e nunca seria aprovado, foi então que o Deputado Teixeira propôs um acordo e lançou o projeto de Lei 2.793 no dia 29 de novembro de 2011, que trazia a tipificação dos delitos cometidos na esfera virtual. Tratava de uma

proposta vinda do projeto de Lei 84/99, onde poderia criminalizar certas condutas no mundo da internet.

Para Jesus e Milagre (2016, p. 74):

> Considerou-se também um outro projeto de lei, pois o Projeto de Lei nº 84/99 não poderia mais ser modificado segundo os regimentos do Congresso Nacional. Deixava de lado o projeto de Lei nº2793/2011 qualquer discussão sobre a guarda e logs (registro de conexão e/ou navegação) por parte de provedores de acesso e aplicações de Internet, ponto muito discutido e enfaticamente reprovado por parte da sociedade em inúmeros manifesto. Com isso, propunha-se um projeto mais "suave", sem pontos polêmicos, de menor resistência social, que deveria ser submetido a ampla discussão e audiências públicas.

Entretanto no ano de 2012, no dia 04 de maio, houve um fato envolvendo a atriz Carolina Dieckmann, a mesma teve as suas fotos intimas postadas nas redes sociais, onde na mesma data vários requerimentos de urgência foram impostos em relação ao projeto de Lei. A qual tramitou em tempo recorde e concretamente transformava-se o projeto de Lei 2.793/2011 na Lei 12.737/2012, ficou conhecida como a Lei Carolina Dieckmann, chamada também de Lei dos crimes informáticos.

Segundo a justificação para converter a Lei Jesus e Milagre (2016, p.74) evidenciam:

> [...] com relação ao PL 84/99, nota-se que grande parte dos tipos penais ali propostos apresenta redação significativamente aberta, e muitas vezes sob a forma de tipos de mera conduta, cuja simples prática – independentemente do resultado obtido ou mesmo da específica caracterização da intenção do agente – já corresponderia à consecução da atividade criminosa. Tal estratégia redacional, típica de uma sociedade de risco e de uma lógica de direito penal do inimigo, busca uma antecipação da tutela penal a esferas anteriores ao dano,
> envolvendo a flexibilização das regras de causalidade, a tipificação de condutas tidas como irrelevantes, a ampliação e a desproporcionalidade das penas e a criação de delitos de perigo abstrato, dentre outras características. Exemplo disso é a criação de um capítulo com o objetivo de tutelar juridicamente, como bem jurídico protegido, a "segurança dos sistemas informatizados". Tal estratégia, como já apontado, resulta na possibilidade de punição gravosa a meras condutas que, por sua natureza ou intenção, não mereceriam ensejar a repressão penal – como o acesso não autorizado a sistemas informáticos decorrentes de testes de segurança efetuados sem a prévia anuência dos titulares de sistemas informatizados.

A lei estabelece possibilidades de a polícia estruturar órgãos que tenham a especialidade em crimes virtuais, como ações criminosas em redes de computadores ou sistemas dentro da internet, mas não traz nenhum rol sobre cooperação privada, a qual é muito usada em outros países.

A tipificação mais polêmica que a lei traz é referente a invasão de equipamentos informáticos, crimes que possuem um perigo abstrato, o qual cresce gradativamente conforme o avanço da tecnologia e da informação.

Para Jesus e Milagre (2016, p.88): “na sociedade da informação, cada vez mais buscam-se proteger direitos supraindividuais, em um modelo preventivo do Estado contra os riscos e não contra ameaças concretas de lesão ao bem jurídico protegido.”

A lei em seu artigo 154 – A descreve a conduta e a sua punição:

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.
> § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no **caput.**
> § 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
> § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
> Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.
> § 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidas.
> § 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:
> I - Presidente da República, governadores e prefeitos;
> II - Presidente do Supremo Tribunal Federal;
> III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou
> IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.” (BRASIL, 2012).

Além da Lei 12.737 de 2012, outra lei também é muito usada para combater os criminosos ou pelo menos a única saída para julgar os delinquentes dessa nova era. Como diz Wendt (2011, p.28 apud Santos e Monteiro, 2010) “[...] a segurança global está se tornando mais vulnerável e mais exposta”.

A referida lei é mais atual, vigorou no ano de 2014, conhecida como o Marco Civil da Internet, a qual será explanada a seguir.

3.3.2 Lei Nº 12.965 de 2014, conhecida como o “Marco Civil da Internet”.

A Lei 12.737 de 2012 está muito distante de conseguir resolver todos os problemas relacionados a era virtual no Brasil. A solução, de fato, não é fácil e não será encontrada com diversas edições de leis, é uma situação que envolve educação também, estruturas competentes de investigação e políticas criminais.

A Lei 12.965 de 2014 é considerada a Constituição da Internet, pois garante direitos e deveres a todos os envolvidos com a Internet no Brasil, sejam eles apenas usuários ou provedores de internet, englobando de forma geral todos os usuários. Conhecida também como o Marco Civil da Internet, foi fruto da atuação da Secretaria de Assuntos Legislativos do Ministério da justiça no dia 29 de outubro de 2009, nessa data que o projeto de lei foi lançado. A sua construção foi colaborativa, onde estava disponível para consulta pública no decorrer dos anos de 2009 e 2010, tendo mais de duas mil contribuições. Mas não parou por aí, após toda a fase de participação popular, o projeto ingressou no Congresso em 24 de agosto no ano de 2011, foi transformada na Lei n. 2.126, tendo o Poder Executivo tomado esta medida,

> teve como base o documento do Comitê Gestor da Internet no Brasil (C.G.I. br) e define regras claras para os usuários e determina as diretrizes para a atuação da União dos Estados, do Distrito Federal e dos municípios. (PAESANI, 2013, p. 82).

Sendo ainda apenas um projeto que visava estabelecer direitos e deveres, princípios e garantias para cada usuário da Internet. (JESUS; MILAGRE, 2016, p.182).

No dia 23 de abril de 2014 foi sancionada pelo Presidente da República e tornou-se a Lei 12.965. Sendo considerada uma vitória para a sociedade brasileira.

Para Pinheiro (2013, p.89):

> O Marco Civil será importante para a Sociedade da Informação porque será um sistema complementar às leis já existentes e preencherá lacunas legislativas. A privacidade é um dos princípios a serem discutidos: da mesma forma que existe a proteção constitucional, ela também é garantida na Internet, e é essa proteção de dados pela guarda de logs nos provedores que o anteprojeto discute, e uma das questões mais importantes para a sua aprovação.

Em relação a privacidade dos usuários, a preocupação também esteve presente, pois o Marco Civil da Internet deve ampara-los, pois as informações destes usuários de certa forma viraram moedas na era virtual, onde são usadas como pagamento de serviços que dizer ser gratuitos, mas que capturam informações dos indivíduos e arquivam para sempre, podendo ser usado para qualquer fim.

> Quando se fala no Marco Civil da Internet, seu proposito inicial é garantir a privacidade de dados de consumidores e ter a guarda segura dos mesmos (igualando aos demais países do exterior), complementando o texto Constitucional, o Código de Defesa do Consumidor e o Código Civil. O texto apesentado ao Congresso Nacional está bem claro quanto a garantia de liberdade de expressão, todavia, deveria ter sido tratado melhor no que diz respeito a vedação do anonimato prevista pela Constituição Federal. (PINHEIRO, 2013, p.89/ 90).

Um dos pontos discutidos em relação ao Marco Civil é a questão dos logs de registro de acesso, quanto a sua guarda e identificação. Estabelece que esses logs devem ser guardados durante um ano, podendo ter esse prazo estendido. Mas o acesso deve ser obtido apenas por meio de ordem judicial, e precisa-se de outra ordem autorizando a associação entre o número de IP e o dono do referido número. Neste caso seria necessário comprovar a existência do crime naquele certo horário e que o usuário seja realmente suspeito de ter cometido o delito. (PAESANI, 2013, p. 82).

> A cultura da Internet no Brasil foi bastante difundida e debatida, sendo possível perceber que muitos dos registros de conexão e acesso a terem seu sigilo relativizado por ordem judicial se deram fora do âmbito processual penal. Por isso, não deve o Marco Civil retroceder nesse sentido, delimitando a aplicação da quebra de sigilo dos registros de conexão e acesso somente a processos de natureza criminal, pois há casos em que a competência é da Justiça Comum Cível ou Justiça Federal Trabalhista, as quais merecem a amparo desse recurso para solucionar determinadas lides. (PINHEIRO, 2013, p.90).

Entretanto o texto normativo do Marco Civil impõe que seja “[...] respeitados princípios de liberdade de expressão, pluralidade, diversidade, abertura, colaboração, exercício de cidadania, proteção à privacidade e dados pessoais, livre iniciativa, livre concorrência e defesa do consumidor.” (PAESANI, 2013, p. 82/83).

Portando a Lei 12.737/2012, como já visto, tipifica os crimes virtuais também, porém não traz a estrutura de investigação ou deveres relacionados aos provedores de internet no que concerne a cooperação para com autoridades nas ações de investigações criminais cibernéticas. “A Lei 12.735/2012 (Lei Azeredo). Por sua vez, chega a prever que os órgãos de polícia judiciária poderão estruturar, nos termos de regulamento, setores e equipes especializadas no combate a ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado.” (JESUS; MILAGRE, 2013, p. 183).

Dando seguimento ao mesmo raciocínio, sabe-se que no Brasil há o princípio da legalidade onde mostra que ninguém é obrigado a fazer ou deixar de fazer nada, senão em virtude da lei. Neste mesmo sentido até a criação do Marco Civil no Brasil, não existia nenhuma legislação que trouxesse obrigação aos provedores de internet a registrarem logs de atividades daqueles que usassem a rede de internet. Pois quando alguém se conecta virtualmente, o provedor de internet que o indivíduo possui, atribui um endereço de IP, marcando a data e horário daquele acesso.

Do mesmo modo, diante de um crime virtual como por exemplo, grupos ou páginas que sejam designadas para pornografia infantil, sabe-se que o provedor registrará os dados de acesso à aplicação, porém esses registros não podem ser entregues sem uma ordem judicial, situação que traz os provedores para o meio de toda essa dificuldade de conseguir provas contra os criminosos e também a dúvida em relação a responsabilidade deles para cada fato ocorrido da esfera virtual, situação a qual será esmiuçada no próximo capítulo.

4 A RESPONSABILIDADE DOS PROVEDORES DE INTERNET

Em um primeiro momento é preciso compreender do que se trata a chamada responsabilidade civil, a qual adveio do interesse de ser possível reestabelecer o equilíbrio do binômio econômico-jurídico, uma vez que o dano lhe causou alteração (DIAS, 1984).

Nesse sentido a responsabilidade civil é:

> [...] é a consequência de toda manifestação da atividade humana, e a busca de sua definição conduz ao conceito de obrigação, isto é, de uma prestação que alguém está obrigado a efetuar determinada prestação e, assim, por ela é responsável (SAMPAIO, 1998, p. 11).

Assim, cada cidadão é responsável por seus atos, ainda que seja atos particulares, como contratos de compra e venda, por exemplo, ou até mesmo em atos contra o Estado. É a partir dela, que se torna possível o ressarcimento dos danos causados pelos atos praticados. Esclarecido isso, passa-se a compreensão da responsabilidade civil, no tocante as condutas praticadas na esfera virtual e a responsabilidade dos provedores de internet.

4.1 OS PROVEDORES E A RESPONSABILIDADE CIVIL

Sabe-se que, diariamente, são compartilhadas milhares de informações de maneira livre na internet. É essa liberdade de acesso que permite as mais variadas formas de abuso e violação de direitos por pessoas mal-intencionadas, esperando obter alguma vantagem. Muitas vezes acabam por atingir alguns direitos personalíssimos, como a honra, imagem, vida privada, etc. Segundo Gonçalves (2019), “a facilidade com que a internet penetra nos lares de todas as pessoas determina riscos substanciais de lesões a Direitos como os de intimidade e os de privacidade."

Diante disso, não há como negar que na internet, existe sim a possibilidade de incidência de responsabilidade civil, tornando-se inclusive assunto em evidencia, dado ao fato de ser crescente o mínimo de casos de violação de informações, que ocasionam danos.

Dessa maneira, a teoria da responsabilidade civil na internet, encontra fundamento na teoria do risco, pois vem para solucionar os problemas oriundos dos danos, quando a existência de culpa não se faz indispensável. Isso porque, ao considerar somente a internet, mídia e veículo de comunicação, os danos indiretos são mais visto e possuem um potencial maior que, os danos diretos, ocasionando com isso uma possibilidade de causar prejuízo a outra pessoa, ainda que sem culpa, bem maior (PECK, 2002).

Deste modo,

> o critério da responsabilidade objetiva deve predominar na utilização dos meios eletrônicos com o objetivo de determinar o dever de indenizar do responsável que tenha manejado ou posto em funcionamento o meio eletrônico causador do dano" (LOPES, 1989, p. 36).

De outro lado, tem-se a questão dos crimes praticados na seara virtual, fazendo milhares de vítimas diariamente com furtos de dinheiro, estelionatos, vírus em computadores, tráfico de drogas, dentre outros tantos que vem a ocorrer tanto na *surface* quanto na chamada *deepweb.*

Já em relação aos provedores de acesso, aqueles que fazem a intermediação entre o usuário e a rede, segundo Kazmierczak (2019, p.2):

> Os provedores de acesso não têm capacidade para fiscalizar o teor dos milhares de e-mails que diariamente por trafegam. Sendo assim, é impossível ao provedor de acesso impedir a ação danosa que uma determinada informação transmitida através de um correio eletrônico poderá causar.

Já, no tocante aos provedores de hospedagem, aquele que hospeda os endereços das páginas virtuais, pode haver a responsabilização, quando da publicidade de informações de terceiros, fazendo alusão a teoria do risco. A responsabilidade do provedor de hospedagem é calcada na subjetividade, medindo a culpa, ou seja, só poderá ser responsabilizado por negligência, imperícia ou imprudência (ISAGUIRRE, 2002).

Destarte, pode-se perceber que a responsabilização do provedor de internet pode ocorrer, uma vez que, este pode ter o controle daquilo que terceiros hospedam, vinculando informações que podem vir a ocasionar lesão a outra pessoa, bem como, até o cometimento de crimes.

Entretanto os provedores são sujeitos privados, entidades e empresários que disponibilizam aos usuários a conexão de internet, e de forma eventual oferecem também outros serviços, mediante remuneração ou podendo até ser de forma gratuita.

Segundo Paesani (2013, p.73) “Os provedores são parte da relação contratual de difícil colocação jurídica,” pois observando o contrato do gestor da rede de telecomunicação que oferece uma grande quantidade de linhas para possibilitar o desenvolvimento da atividade, deverá inicialmente gerar uma locação de forma contratual, conforme entende o Código Civil e deve sempre desenvolver uma função social. Tendo o Código incorporado a responsabilidade objetiva, aconselha-se sempre a revisão dos contratos celebrados entre os provedores e seus clientes, de modo que a participação conjunta em processos judiciais seja sempre garantida. Em decorrência das relações de consumo excluídas e responsabilidade sem culpa, os provedores de internet deverão ser responsabilizados diretamente pela forma de uso dos seus clientes, que deixam hospedados os seus sites em seus servidores. (PAESANI, 2013, p.74).

Há uma grande necessidade em estabelecer pontos e hipóteses de limitação ou isenção da responsabilidade em casos que o conteúdo da informação que o fornecedor de internet não consiga controlar no momento da divulgação, salvo quando existir a possibilidade de interceptar a publicação ou informação com base em

suspeitas de utilização de conteúdo ilícito a pedido do ofendido ou por indicação de terceiros.

Observa-se que a limitação da responsabilidade por lei poderia ser reconhecida quando as informações forem fornecidas ou instaladas em outros fornecedores e quando o fornecedor tenha se precavido conforme indicações do código de auto-regulamentação, identificando corretamente cada usuário.

Segundo Paesani (2013, p.77):

> Outra exigência sentida é a de determinar os requisitos na base dos quais um *site* possa ser considerado, e, em consequência, registrado, como *cabeçalho jornalístico* (circunstância indispensável para a aplicação das disposições introduzidas pela lei sobre *Tutela da pessoa e de outros sujeitos quanto ao tratamento dos dados pessoais*), distinguindo assim o que pode ser identificado como cabeçalho de jornal de tudo o mais que não tenha as mesma características (áreas de debates, coleta de textos etc.).

A Lei de imprensa deveria modificar seu texto a fim de estabelecer que os diretores dos jornais telemáticos sejam responsabilizados unicamente por seus conteúdos de redação introduzidos sob seu controle.

Desenvolve-se um grande debate em relação a oportunidade ou não da abstenção do legislador referente a defesa do menor contra pornografia ou violência. Neste campo, a interpretação constitucional autorizaria a aplicação normativa, pois segundo observadores a falta dessa normativa orgânica acaba sempre penalizando a própria rede. (PAESANI, 2013, p.76).

Entretanto, Corrêa (2010, p.123) evidencia que:

> O Ministério Público do Estado da Bahia, embasado no Estatuto da Criança e do Adolescente, ofereceu denúncia contra determinado provedor de acesso utilizado para a disseminação de pornografia infantil por um usuário. Oferecida e acatada a denúncia, foi expedido mandado para apreensão de todos os computadores do provedor.

Não existe dúvidas que houve realmente um crime na situação citada, uma vez que o ECA especifica que fotografar e/ou publicar cena de sexo explícito ou pornografia envolvendo crianças ou adolescente será punido com pena de reclusão de 1 a 4 anos. O delituoso usou a internet como meio para consumar o seu delito, da mesma forma que um assassino possa utilizar um revólver ou faça para alcançar o seu objetivo. Portanto estamos diante de crimes digitais, que são caracterizados pela prática de atividades ilegais, tendo um determinado usuário, agindo pelo anonimato

na internet, disseminando conteúdos pornográficos dentro de comunidades virtuais que não possuem relação alguma com os provedores de acessos. (CORRÊA, p.125).

Os provedores deveriam esclarecer e fixar, contratualmente, a responsabilidade dos seus usuários acerca dos crimes e condutas criminosas que possam vir a ocorrer e ferir o ordenamento jurídico brasileiro, tornando esclarecida o posicionamento perante ações. Afinal, é impossível a tipificação de todas as condutas criminosas possíveis, ao mesmo tempo que a contribuição da tecnologia é essencial para a formação de lacunas jurídicas, também contribui com desenvolvimento jurídico eficaz, criando rápidas respostas para uma sociedade cada vez complicada. (CORRÊA 2010, p. 127).

A seguir será apresentado alguns direitos e deveres que o Marco Civil da internet impõe para os provedores de internet, inclusive a sua responsabilidade perante crimes virtuais e apreensões de equipamentos usados para a prática de crimes.

4.1.1 A Lei 12.965/2014 e a Responsabilidade dos Provedores

Inicialmente vale ressaltar que pode haver a busca e apreensão de equipamentos informáticos quando há indícios de crimes virtuais. Os provedores de acesso, por exemplo, mediante ordem judicial devem fornecer o número de IP do equipamento em que o usuário estaria cometendo um suposto delito, mediante esses números que há a identificação da localidade do delinquente. Diante dessas suspeitas, Jesus e Milagre (2016, p. 192) dispõe que:

> com base nos dados fornecidos pelos provedores ou responsáveis pelos ativos de TI, pode a autoridade requerer uma busca e apreensão na sede ou domicilio do suposto autor do delito, para que as máquinas sejam coletadas adequadamente para a realização de perícia técnica (para a apreensão de instrumentos utilizados na prática de crime ou destinados a fim delituoso).

A busca e apreensão desses equipamentos, segue legalmente a regra do Código de Processo Civil, e a necessidade de os agentes policiais cuidarem da preservação do local até a chegada dos peritos para investigarem o crime que foi cometido com aquela máquina.

Entretanto, essa é apenas umas das medidas que podem ser tomadas pela polícia para identificarem os crimes digitais. Os provedores de internet são

insubstituíveis para cooperarem nesse processo, sem o fornecimento da identificação com o número de IP a localização se tornaria mais demorada e menos eficiente. (JESUS; MILAGRE. 2016, p.190).

Portanto em assuntos de responsabilidades dos provedores de internet observa-se que a própria Anatel disponibiliza em seu site leis, regulamentos e decretos para sanarem as dúvidas dos usuários da rede de internet, dentro desse rol de direitos está disponível o regulamento do Marco Civil, o qual traz uma grande abrangência de direitos e deveres, tanto para usuários como para os provedores de internet.

É importante observar o artigo 18 da Lei supracitada (12.965/2014), que traz claramente o entendimento de que os provedores de internet não poderão ser responsabilizados civilmente por danos que conteúdo de terceiros possam vir a provocar. Ou seja, o ato ilícito cometido por um usuário dentro de suas redes sociais, como Instagram, facebook ou Youtube, não trarão os provedores como responsáveis e sim a responsabilidade total daqueles assinantes que publicaram o conteúdo. (JESUS; MILAGRE. 2016, p.189).

Entretanto, os provedores poderão sim ser responsabilizados por atos de terceiros, como por exemplo um conteúdo abusivo que esteja ferindo a integridade do outro, como fotos intimas ou conteúdo pessoal, conforme o artigo 19 da Lei 12.965 de 2014 dispõe:

> Art. 19. Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário. (BRASIL, 2014).

Deste modo, a seguir serão especificados cada espécie de provedor e sua respectiva responsabilização segundo o direito digital.

4.2 PROVEDORES DE SERVIÇO

Os provedores de serviços são uma das espécies que compõem os provedores de internet, são empresas que possuem servidores que permitem o acesso de seus clientes a rede de internet 24h por dia. Segundo Pinheiro (2002, p.14): “os provedores

de internet são considerados novas modalidades de empresas dentro do segmento de telecomunicações com características mistas.”

Para Colaço (2015, p.3):

> A expressão “provedor de serviços de Internet” designa gênero abrangente de inúmeras categorias ou espécies. Desse modo, pode-se conceituar, de modo conciso, provedor de serviços de Internet como “a pessoa natural ou jurídica que fornece serviços relacionados ao funcionamento da Internet, ou por meio dela.” Diante do conceito formulado, considera-se provedor de Internet todo aquele que viabiliza, de modo direto ou indireto, meios materiais hábeis a manter os indivíduos conectados à rede mundial de computadores. São os provedores de serviço que permitem o estabelecimento da conexão entre os internautas e o meio digital.

Ao contratar um serviço de internet, existe a necessidade de se ter um prestador de serviços de telecomunicação que disponha de todo o suporte necessário, o contratante pode obter o serviço de conexão de internet da própria prestadora que está lhe vendendo a conexão, ou outro que por ela seja habilitado. Segundo a ANATEL (Agência Nacional de Telecomunicações):

> A prestadora de serviço de acesso à internet que exerça a função de provedor serviço de conexão por meio de uma empresa do mesmo grupo deve garantir a gratuidade de tal conexão ao seu cliente. O consumidor continua livre para contratar o provedor de seu interesse, caso não queira o ofertado gratuitamente pela prestadora.

Os provedores de serviço devem ter de forma estruturada tecnologias adequadas para solucionar conflitos no mundo virtual. Caso seja descumprido esse dever é acarretado a chamada responsabilidade direta ou responsabilidade por ato de terceiro, quando o ato ilícito deixar de ser prevenido em razão de falhas ou defeito. Ainda são exigidos que essa espécie viabilize a identificação correta de dados de conexão dos delinquentes, afim de que os dados sejam fornecidos e disponibilizados ao usuário ofendido mediante ordem judicial. (COLAÇO, 2015, p.4).

Portanto, os provedores de internet possuem subdivisões, como provedores de serviço, o qual já foi tratado acima, provedores de acesso e provedores de hospedagens, espécies que serão distinguidas e especificadas a seguir.

4.3 PROVEDORES DE ACESSO

Essa espécie de provedor exerce uma simples atividade de condução, ou seja, conduz a informação entre a rede e o usuário, servindo apenas para conecta-lo ao mundo virtual. Porém, para alguns autores essa espécie de provedor não pode ser responsabilizada civilmente pelas ações de seus usuários. Afirma Filho (2011):

> O provedor de acesso não pode ser responsabilizado, por exemplo, por mensagens enviadas por seus usuários. E na transmissão de mensagens eletrônicas o provedor não exercita controle editorial, portanto, não pode vir a ser responsabilizado como se editor fosse de potenciais mensagens difamatórias.

Os provedores de acesso não possuem gestão sobre os conteúdos disponibilizados na rede, pois apenas prestam um serviço. Portanto não podem impedir nenhuma forma de visualização de informações que despencam na internet, mas mediante ordem judicial possuem o dever de disponibilizar endereços de IP de usuários.

Segundo Colaço (2015, p.8):

> A lógica da responsabilização civil de provedores de acesso em razão de ilícitos praticados por terceiros é inversa à aplicada na responsabilidade por atos próprios. Embora perfeitamente aplicáveis as disposições do Código de Defesa do Consumidor à responsabilização do provedor de acesso por ilícitos cometidos por terceiros, tais regras não autorizam responsabilização objetiva; isso porque esta espécie de provedor apenas age como intermediário do acesso à Internet, não exercendo domínio sobre conteúdo de informações veiculadas na rede e os ilícitos praticados por seus consumidores.

Portanto a situação jurídica do provedor de acesso é o poder de controlar apenas o fluxo de mensagens de uso, situações apenas relacionadas ao acompanhamento de eficiência e funcionamento, mas não possui diretriz para verificar conteúdos que tramitam pela rede. (COLAÇO, 2015, p.8).

A responsabilização dos provedores de acesso só será executada quando não colaborarem para a identificação do autor que causou o crime, deixando de oferecer o número de IP que é extremamente útil para rastrear o usuário. E não interromper o serviço de conexão aquele que utilize essa ferramenta para praticar atos ilegais, concluindo que somente será responsabilizado o provedor de acesso em situações ilícitas de terceiros usuários, quando descumprir um dever geral de conduta.

4.4 PROVEDORES DE HOSPEDAGEM

Provedores de hospedagem, são as pessoas jurídicas que fornecem o armazenamento de dados em servidores de acesso remoto ou podendo ser de natureza própria, dando a possibilidade de que terceiros acessem esse banco de dados. (LEONARDI, 2005, p. 27).

Segundo Leonardi (2005, p.27):

> É importante ressaltar que o jargão informático consagrou, lamentavelmente, a utilização do termo *provedor de hospedagem*, tradução direta da expressão *Housting provider* em inglês. O serviço prestado, no entanto, não guarda qualquer relação com o contrato típico de hospedagem, pois é, em realidade, cessão de espaço em disco rígido de acesso remoto.

Já para Funck e Lacerda (2012 p.8), um provedor de hospedagem consiste:

> em colocar à disposição de um usuário pessoa física ou de um provedor de conteúdo espaço em equipamento de armazenagem, ou servidor, para divulgação das informações que esses usuários ou provedores queiram ver exibidos em seus sites.

Em pauta de usuário e provedor de hospedagem questiona-se a possibilidade de ser configurada como uma relação de consumo, segundo artigos 14 e 20 do CDC, devido falhas que poderão ocorrer na prestação de serviço, como por exemplo um equipamento que não esteja devidamente protegido com antivírus e for invadido por hackers, os quais terão todo o acesso a dados pessoais de clientes, porém, é discutido as excludentes de responsabilidade dos provedores em relação a situações como a citada , onde estão dispostas no artigo 14, parágrafo 2 º do CDC, prevendo que quando o provedor comprovar culpa exclusiva do consumidor em atos ilícitos, levantará a discussão em relação ao enquadramento como uma excludente de responsabilidade. Pois:

> Quanto à responsabilização civil do provedor de hospedagem por ilícitos de terceiros, a priori, não se configura em razão de conteúdo de informações armazenadas em seus servidores, pois a função primordial destes é fornecer suporte técnico para que dados possam ser acessados por demais internautas, nos limites delimitados pelo contratante. Assim, este possui liberdade para criar, modificar ou extinguir material publicado e armazenado pelo provedor de hospedagem. (COLAÇO, 2015, p.11).

Os provedores de hospedagem possuem o acesso aos conteúdos publicados por seus usuários, e mediante mandado judicial são obrigados a remover conteúdos ilícitos e bloquear o serviço prestado ao ofensor. Segundo o artigo 19 da Lei 12.965

de 2014, com a função de resguardar a liberdade de expressão, dispõe que os provedores de hospedagem somente poderão ser responsabilizados civilmente por danos que decorreram de conteúdos ilícitos gerado por terceiros, se não tomarem as providências cabíveis e necessárias para tornar o conteúdo indisponível após a ordem judicial. (COLAÇO, 2015, p.12).

Portanto pode-se compreender que os provedores não poderão selecionar os conteúdos que são publicados, nem os controlar sob pena de censura prévia e acabar ferindo o princípio de liberdade de expressão situada na Lei 5.250 de 9 de fevereiro de 1967. Porém, uma vez notificado do conteúdo ilícito que foi publicado deverá retirá-lo do ar imediatamente através de ordem judicial feita por delegado de polícia, podendo vir a sofrer penalidades caso não cumpra o exigido dentro do prazo estipulado. E para que os provedores possam executar, é necessário que a ordem judicial especifique e indique claramente o conteúdo ofensivo e ilícito que deva ser excluído da rede, podendo até mesmo se tornar nulo o pedido caso não seja claro.

5 CONSIDERAÇÕES FINAIS

A evolução humana se faz presente em todos os aspectos da sociedade, sendo assim, é notório também que os meios de comunicação também sofrem com as transformações do tempo e se moldem as novas eras.

Hoje é impossível deparar-se com um indivíduo que não utiliza a tecnologia de alguma forma no seu cotidiano, mesmo que mínima ela está presente. Desde a criação das redes de computadores por volta dos anos 70 o número de usuários vem aumentando e cada vez mais se moldando as necessidades do mundo a sua volta. Não apenas na forma de conectar os indivíduos, mas também na estrutura de seus matérias. Já que não é mais necessário possuir inúmeros equipamentos, fiações e peças para usufruir do uso da internet.

Fato é que, da mesma forma que a evolução tecnológica aproximou a convivência humana, beneficiando aqueles que querem dispor do contato mesmo que distantes fisicamente do outro, há também aqueles que não sabem lidar com tamanhas evoluções e utilizam o meio virtual com intenções deturbadas, fazendo com que o espaço da internet seja apenas mais uma maneira de disseminar as condutas criminosas.

Assim, por mais dificultoso que seja a localização destes tipos de criminosos, as definições de crimes virtuais (ou cibernéticos) englobam tanto os crimes como as contravenções penais. Esbarrando então na complexidade da causa, que além do anonimato presente na maioria dos crimes virtuais, a territorialidade é assunto delicado nesse tipo de delito. Pois é a internet um ambiente sem fronteiras.

Não há apenas uma maneira de cometimento de delitos no meio virtual, além dos usuários saberem as formas mais complexas de esconder rastros, estes também se utilizam de inúmeras formas para cometer os crimes. Como vimos, desde a espionagem eletrônica contra empresas ou pessoas físicas para obter informações de cunho pessoal a crime como a pornografia virtual.

Considerando assim a evolução destes meios fez-se necessário que o ordenamento jurídico dispusesse de legislação para abarcar esse quesito, pois, independendo do mundo físico ou virtual é dever da legislação regulamentar tais condutas, tanto no meio penal quando no aspecto civil da questão virtual. O Código Penal faz menção a esses crimes, muito embora foi necessário a criação de demais leis com regulamentações bem especificas acerca do tema, apenas algumas tiveram a sua efetividade, tais como a “Lei Carolina Dieckmann”, “Marco Civil da Internet”.

Mais que dispor a regulamentação legal dos crimes virtuais o trabalho apresentado teve o intuito de analisar a reponsabilidade dos provedores de internet. Estes são os que fazem a intermediação entre a rede e o usuário. Deste modo, por serem eles meros intermediadores não possuem a capacidade de fiscalizar cada indivíduo que dela se utiliza. Além de não ser o intuito de seus serviços, é impossível que o provedor evite toda ação danosa que ocorra na rede onde tramita as informações. Enquanto que, no tocante aos provedores de hospedagem, aquele que hospeda os endereços das páginas virtuais, pode haver a responsabilização, quando da publicidade de informações de terceiros, fazendo alusão a teoria do risco. Ou seja, só poderá ser responsabilizado por negligência, imperícia ou imprudência.

Os provedores poderão sim ser responsabilizados por atos de terceiros, como por exemplo um conteúdo abusivo que esteja ferindo a integridade do outro, pode haver a busca e apreensão de equipamentos informáticos quando há indícios de crimes virtuais. Entretanto, é importante frisar que a LEI 12.965/14, a qual regulamenta a questão dos provedores, salienta que os delitos causados pelo uso de redes sociais não incluem a responsabilização destes, pois neste caso serão na integra de seus usuários. Por fim, cada provedor (de serviço, de acesso e de hospedagem), possui

sua própria analise de responsabilização a ser seguida, de acordo com suas peculiaridades.

6 MÉTODO

O método de abordagem empregado para a realização da futura pesquisa apresentada brevemente acima, será o método dedutivo. Visando este uma compreensão da responsabilidade dos provedores quanto a prática dos crimes na internet.

Os métodos de procedimento utilizados nessa pesquisa serão o monográfico, histórico e o comparativo. Visto que se tratará de uma pesquisa que busca entender a aplicação das leis nacionais e internacionais, no tocante aos crimes virtuais.

As técnicas utilizadas no desenvolvimento da pesquisa cuidarão do embasamento teórico, este dado pela pesquisa bibliográfica pautada na consulta de livros, revistas, periódicos e outros meio de veiculação de informação disponibilizados.

REFERÊNCIAS

ANATEL. Provedor. 2015. Disponível em:<https://www.anatel.gov.br/consumidor/banda-larga/direitos/provedor>. Acesso em: 21 out. 2019.

ANATEL. Governo Federal. Disponível em:<https://www.anatel.gov.br/institucional/>. Acesso em: 21 out. 2019.

BOITEUX, Luciana. Crimes informáticos: Reflexões sobre a política criminal inseridas no contexto internacional atual. **Rev. Brasileira de Ciências Criminais**, São Paulo, v. 12, n.47, p. 146-187, 2004.

BRASIL. Lei nº 9.472 de 16 de julho de 1997. Edição Federal, Brasília, 1997. Disponível em:<http://www.planalto.gov.br/ccivil_03/leis/L9472.htm>. Acesso em: 21 de out. 2019.

BRASIL. Lei nº 5.250 de 9 de fevereiro de 1967. Edição Federal, Brasília, 1967. Disponível em:<http://www.planalto.gov.br/ccivil_03/leis/l5250.htm >. Acesso em: 21 out. 2019.

BRASIL, Constituição (1988). **Constituição da República Federativa do Brasil**. Brasília: Senado Federal, 1988.

BRASIL. Lei nº 13.718, de 24 de setembro de 2018. **Lex**: coletânea de legislação: edição federal, Brasília, 2018.

BRASIL, Lei nº 12.965 de 23 de abril de 2014. **Lex:** coletânea de legislação: Edição Federal: Brasília, 2014.

BRASIL, Decreto-lei nº 2838 de dezembro de 1940 (Código Penal). Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm>. Acesso em: 24 de jun. 2019.

BRASIL. Lei nº 12.737 de 30 de novembro de 2012. Edição Federal, Brasília, 2012. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 30 jul. 2019.

BRAGA. Newton, C. **Espionagem e vigilância eletrônica**. 1. Ed. São Paulo: Newton C. Braga, 2015. 274p.

CIDRÃO, Thais Vasconcelos; MUNIZ, Antônio Walber; ALVES, Ana Abigail Costa Vasconcelos. A oportuna e necessária aplicação do Direito Internacional nos ciberespaços: da convenção de Budapeste a legislação brasileira. **Brazilian Journal of Internationl Relation**, Marilia, v.7, n. 1, p.66-82, Jan./abr. 2018. Disponível em:< file:///C:/Users/usuario/Downloads/7069-Texto%20do%20artigo-25459-1-10-20180527.pdf>. Acesso em: 10 jul. 2019.

COLAÇO, Hian Silva. A responsabilidade Civil dos provedores de Internet: dialogo entre a jurisprudência e marco Civil da Internet. Rev. dos Tribunais, v. 957, 2015.

Disponível em:<http://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_servicos_produtos/bibli_boletim/bibli_bol_2006/RTrib_n.957.05.PDF>.Acesso em: 21 out. 2019.

CORRÊA, Gustavo Testa. **Aspectos jurídicos da internet**. 5. Ed. São Paulo: Atlas, 2010. 169p.

CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. São Paulo: Saraiva, 2011. 30p.

DIARIO DA REPUBLICA ELETRÔNICO. Resolução da Assembleia da Republica nº88/2009. Portugal. Serie 1. 15 set. 2009. Acesso em: <https://dre.pt/web/guest/pesquisa/-/search/489698/details/normal?q=Resolu%C3%A7%C3%A3o+da+Assembleia+da+Rep%C3%BAblica+n.%C2%BA%2088%2F2009>. Acesso em: 10 jul. 2019.

DIAS, José Aguiar. **Da responsabilidade civil**. v. II, 4° ed. Rio de janeiro: Forense, 1984.

FELICIANO, Guilherme Guimarães. **Informática e Criminalidade: parte I: Lineamentos e Definições**. Boletim do Instituto Manoel Pedro Pimentel, São Paulo, v. 13, n. 2, p. 35-45, set. 2000.

FILHO, Demócrito Ramos Reinaldo. Responsabilidade do provedor de acesso à internet por mensagens difamatórias transmitidas pelos usuários. Disponível em:<http://www.infojus.com.br>. Acesso em 21 out. 2019.

FUNCK, Rodrigo Gelain; LACERDA, Emanuela Cristina Andrade. Responsabilidade civil dos provedores de hospedagem na Internet. Rev. Eletrônica de Iniciação Científica. Itajaí, Centro de Ciências Sociais e Jurídicas da UNIVALI. v. 3, n.2, p.1283-1300, 2º Trimestre de 2012. Disponível em:<www.univali.br/ricc - ISSN 2236-5044 http://www.rghadvogados.adv.br/upload/files/rodrigo_responsabilidade%20civil%20dos%20provedores%20de%20hospedagem%20na%20internet.pdf>. Acesso em: 21 out. 2019.

GLANZ, Semy. Internet e Responsabilidade Civil. **Rev. Emerj**., Rio de Janeiro, v.7, n.25, p.53, 2004. Disponível em:<http://www.emerj.tjrj.jus.br/revistaemerj_online/edicoes/revista25/revista25_53.pdf>. Acesso em: 04 jul. 2019.

GONÇALVES, Carlos Roberto. **Responsabilidade civil na internet**. Disponível em: <http://www.cahiers.org./new/htm/articoli/goncalves_responsabilidade.htm>. Acesso em mar. 2019.

ISAGUIRRE, Katia Regina. **Internet: responsabilidade das empresas que desenvolvem sites para web-com**. Curitiba, 2002. 161p. (ISBN: 8573948440X). Disponível em:<https://www.lexml.gov.br/urn/urn:lex:br:rede.virtual.bibliotecas:livro:2002;000615189>. Acesso em: 30 set. 2019.

ITALIA. Decreto nº 453, de 28 de dezembro de 2000**. Texto consolidado das disposições legislativas e regulamentares sobre documentação administrativa.** (Texto A). Disponível em: <https://www.normattiva.it/atto/caricaDettaglioAtto?atto.dataPubblicazioneGazzetta=2001-02 20&atto.codiceRedazionale=001G0049&queryString=%3FmeseProvvedimento%3D12%26formType%3Dricerca_semplice%26numeroArticolo%3D%26numeroProvvedimento%3D445%26testo%3D%26annoProvvedimento%3D2000%26giornoProvvedimento%3D28&currentPage=1>. Acesso em: 08 jul. 2019.

JESUS, Damásio de; MILAGRE, José Antonio. **Manual de Crimes Informáticos.** 1. Ed. São Paulo: Saraiva, 2016, 231p.

KAZMIERCZAK, Luiz Fernando. **Responsabilidade civil dos provedores de internet**. Disponível em:<http://www.uj.com.br./publicacoes/doutrinas/3532/responsabilidade_civil_dos_provedores_de_internet>. Acesso em mar. 2019.

LÉVY, Pierre. **Cibercultura**. 1 Ed. São Paulo: 34 Ltda, 1999. 257p.

LYRA, Afranio. **Responsabilidade Civil**, Bahia, 1977.

LOPES, Miguel Maria de Serpa. **Curso de Direito Civil**. v. 5, n. 144. São Paulo: Freitas Bastos, 1989.

LUCCA, Newton de; FILHO, Adalberto Simão. **Direito e internet: aspectos jurídicos relevantes.** São Paulo: Edipro, 2001. 512p.

NIGRI, Deborah Fisch. **Crimes e segurança na internet**. In Verbis, Rio de Janeiro: Instituto dos Magistrados do Brasil, Ano 4, n. 20, p. 34-41, 2000.

OVÍDIO, Francisco. Aspectos do Direito Comparado. Rev. Revista da USP, São Paulo, 1984. Disponível em:<https://www.revistas.usp.br/rfdusp/article/download/67009/69619.>. Acesso em: 05 jul. 2019.

PAESANI, Liliana Mirandi. **Direito e internet:** liberdade de informação, privacidade e responsabilidade civil. 6 ed. São Paulo: Atlas, 2013. 128p.

PECK, Patrícia. **Direito Digital**. São Paulo: Saraiva, 2002.

PENHA, Fabiana Cristhina Almeida da. O sistema de responsabilidade civil aplicável aos provedores de serviços de Internet. Rev. Autônoma de Direito Privado. Curitiba, n.5, p.365-397, jul.-dez. 2008.

PINHEIRO, Patrícia Peck. **Direito digital**. 5. Ed. São Paulo: Saraiva, 2013. 671p.

PINHEIRO, Patrícia Peck. **Direito Digital.** 4°. ed. Revista, atualizada e ampliada. São Paulo: Saraiva, 2º tiragem 2010.

PINHEIRO, Patrícia Peck. **Direito Digital**. São Paulo: Saraiva, 2002, p. 60

RAMALHO TERCEIRO, Cecílio da Fonseca Vieira. **Crimes Virtuais**. 2005. Disponível em:<http://www.advogadocriminalista.com.br>. Acesso em: 20 mar. 2019.

REGULAMENTAÇÃO DA INTERNET NA ITALIA – Contribuição do Itamaraty. Roma. 2010. Disponível em:<http://culturadigital.br/marcocivil/2010/06/10/regulamentacao-da-internet-na-italia-contribuicao-do-itamaraty/>. Acesso em 10 jul. 2019.

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

ROSSINI, Augusto Eduardo de Souza. **Informática, Telemática e Direito Penal**. São Paulo: Memória Jurídica, 2004.

SAMPAIO, Francisco José Marques. **Responsabilidade civil e reparação de danos ao meio ambiente**. 2° ed. Rio de Janeiro: Lumen Juris, 1998.

WENT. Emerson. **Inteligência Cibernética, a (in)segurança virtual no Brasil**. São Paulo: Delfos Editora Digital, 2011. 136p. (ISBN 978-85-64514-15-7). Disponível em: <https://www.academia.edu/9264319/Intelig%C3%AAncia_Cibern%C3%A9tica_livro_>. Acesso em: 30 de jul. 2019.

ZANELLATO, Marco Antônio. **Condutas Ilícitas na sociedade digital**, Caderno Jurídico da Escola Superior do Ministério Público do Estado de São Paulo, Direito e Internet, n. IV, julho de 2002.p. 173.